UBM TechWeb

PROGRAM GUIDE

JULY 21-26, 2012

WWW.BLACKHAT.COM

black hat® USA 2012

SUSTAINING SPONSORS

ACCUVANT LABS IBM Microsoft nCircle paloalto the network security company QUALYS On Demand Security RSA rune Information Security Corporation Pte Ltd

LIEBERMANSOFTWARE

Grow Your BRAIN!

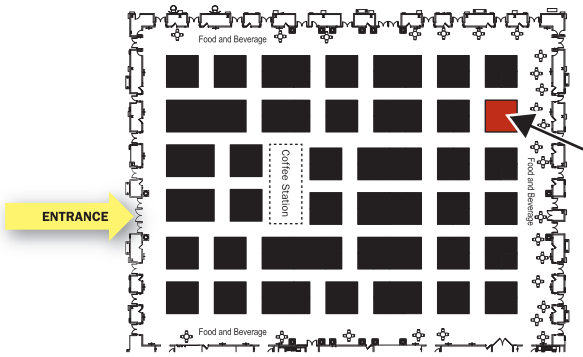
3 WAYS TO WIN Booth #241

Listen, Learn & Win

1 TOP OF THE HOUR (:00) —
Attend a **PRIVILEGED IDENTITY MANAGEMENT** presentation for a chance to win a $50 Amex gift card

2 BOTTOM OF THE HOUR (:30) —
Attend a **WINDOWS SECURITY MANAGEMENT** presentation for a chance to win a $50 Amex gift card

3 DAILY DRAWING —
Enter to win a Parrot AR.Drone 2.0 Quadricopter



Parrot AR.Drone Quadricopter

www.liebsoft.com | sales@liebsoft.com
(310) 550-8575 | (800) 829-6263

© 2012 Lieberman Software Corporation. All Rights Reserved.
All trademarks are the property of their respective owners.

LIEBERMANSOFTWARE

WELCOME

Welcome to Las Vegas, and thank you for your participation in the growing Black Hat community. As we celebrate our 15th anniversary, we believe that the event continues to bring you timely and action packed briefings from some of the top security researchers in the world.

Security saw action on almost every imaginable front in 2012. The year started with a massive online protest that beat back US-based Internet blacklist legislation including SOPA and PIPA, echoed by worldwide protests against adopting ACTA in the European Union. Attackers showed no signs of slowing as Flame replaced Stuxnet and Duqu as the most sophisticated malware yet detected. The Web Hacking Incident Database (WHID) has added LinkedIn, Global Payments, eHarmony and Zappos.com while Anonymous and other politically motivated groups have made their presence known in dozens of attacks.

No matter which incidents you examine—or which ones your enterprise must respond to—one thing is clear: security is not getting easier. The industry relies upon the Black Hat community to continue our research and education, and seeks our guidance in developing solutions to manage these threats.

Black Hat USA 2012 features nine tracks and fourty-nine live, onstage demonstrations presented by over one hundred of the community's best and brightest. We're particularly excited about this year's keynote speakers, Shawn Henry, former FBI Executive Assistant Director (EAD) and the current President of CrowdStrike Services; and Neal Stephenson, one of the world's foremost historical and science fiction authors. Shawn will take the stage to offer new insights on how a hostile cyber environment has rendered traditional security obsolete while Neal will take the stage for an interactive interview.

The Arsenal returns for its third year, offering researchers and the open source community a platform to demonstrate tools they develop and use in their daily professions.

I would like to ask for your help with two items:

- Keep your eye open for the review board members, and give them a hearty thank-you. This team spent countless hours reviewing over 500 submissions; their guidance ensures that the show remains connected to its roots.
- Please fill out your surveys! Black Hat is the most important security event of the year, and our ethos remains focused on the community. We need to hear from you!

Whether it's your first Black Hat or your fifteenth, I want to encourage all attendees reach out and connect. This event offers unique opportunities for professional growth, while providing access to a very niche population—nowhere else on earth will you have this kind of access to researchers, technology experts and Black Hat sponsors. We hope you enjoy this year's show!

Trey Ford

General Manager
Black Hat

TABLE OF CONTENTS

Schedule 4-7
Briefings 8-24
Workshops 21
Turbo Talks 23
Speakers 25-39
Keynote Bio 25
Floorplan 40-41
Arsenal 42-51
Special Events 52-53
Stay Connected + More 54
Sponsors 55

UPCOMING EVENTS:

- **Black Hat Training: HALO Summit 2012**
  San Diego, CA October 29-November 2
- **Black Hat UAE 2012**
  Abu Dhabi, United Arab Emirates December 10-13
- **Black Hat EU 2013**
  Amsterdam, The Netherlands March 11-14
- **Black Hat USA 2013**
  Las Vegas, Nevada July 27-August 1

STAY CONNECTED

- **Twitter:** Twitter.com/Black HatEvents
- **Facebook:** Facebook.com/Black Hat
- **LINKED.IN:** search for "Black Hat" on LinkedIN Groups

SCHEDULE / WED, JULY 25

Time	Track 1	Track 2	Track 3	Track 4
Track	Defining the Scope	Upper Layers	Lower Layers	Mobile *Track Chair: Vincenzo Iozzo*
ROOM	Augustus III + IV	Augustus I + II	Augustus V + VI	Palace I
08:00-12:00	**REGISTRATION: Emperiors Ballroom**			
08:00-08:50	**BREAKFAST: Octavius Ballroom**—*Sponsored by* LOOKINGGLASS			
08:50-09:00	**Jeff Moss: Welcome & Introduction to Black Hat USA 2012: Augustus Ballroom**			
09:00-10:00	**Keynote Speaker: Shawn Henry: Augustus Ballroom**			
10:00-10:15	**Break**			
10:15-11:15	Smashing the Future for Fun and Profit *with Jeff Moss, Adam Shostack, Marcus Ranum, Bruce Schneier* *Moderated by Jennifer Granick*			Advanced ARM Exploitation *by Stephen Ridley + Stephen Lawler*
11:15-11:45	**Coffee Service**—*Sponsored by* RSA			
11:45-12:45	Black Ops *by Dan Kaminsky*	Google Native Client: Analysis Of A Secure Browser Plugin Sandbox *by Chris Rohlf*	How The Analysis of Electrical Current Consumption of Embedded Systems Could Lead to Code Reversing? *by Yann Allain + Julien Moinard*	Scaling Up Baseband Attacks: More (unexpected) Attack Surface *by Ralf-Philipp Weinmann*
12:45-14:15	**Lunch: Forum Ballroom**—*Sponsored by* QUALYS			
14:15-15:15	CuteCats.exe and The Arab Spring *by Morgan Marquis-Boire* The Last Gasp of the Industrial Air-Gap... *by Eireann Leverett* STIX: The Structured Threat Information eXpression *by Sean Barnum*	ModSecurity as Universal Cross-platform Web Protection Tool *by Greg Wroblewski + Ryan Barnett* HTExploit bypassing htaccess restrictions *by Maximiliano Soler + Matias Katz* libinjection: A C library for SQLi detection and generation through lexical analysis of real world attacksTurbo *by Nick Galbreath*	Looking Into the Eye of The Meter *by Don C. Weber*	Don't Stand So Close To Me: An Analysis of the NFC Attack Surface *by Charlie Miller*
15:15-15:30	**Break / Booksigning with the authors of "iOS Hacker's Handbook": Palace Pre-Function**			
15:30-16:30	Errata Hits Puberty: 13 Years of Chagrin *by Jericho*	PRNG: Pwning Random Number Generators (in PHP applications) *by George Argyros + Aggelos Kiaylas*	Windows 8 Heap Intervals *by Chris Valasek + Tarjei Mandt*	Probing Mobile Operator Networks *by Collin Mulliner*
16:30-17:00	**Coffee Service**—*Sponsored by* CISCO			
17:00-18:00	The Myth of Twelve More Bytes: Security on the Post-Scarcity Internet *by Alex Stamos + Tom Ritter*	Owning Bad Guys {and Mafia} with Javascript Botnets *by Chema Alonso*	Ghost is in the Air(traffic) *by Andrei Costin*	Adventures in Bouncer Land *by Nicholas Percoco + Sean Schulte*
18:00-19:30	**Reception: Octavius Ballroom**—*Sponsored by our Diamond, Platinum, Gold Sponsors*			
18:15-19:30	**PWNIE awards: Augustus III + IV**			

Track 5	Track 6	Track 7	Track 8	Track 9
Defense *Track Chair: Shawn Moyer*	Breaking Things *Track Chair: Chris Rohlf*	Gnarly Problems	Applied Workshop I	Applied Workshop II
Palace II	Palace III	Romans I-IV	Florentine	Pompeian
SexyDefense: Maximizing the Home-Field Advantage *by Iftach Ian Amit*	A Stitch in Time Saves Nine: A Case of Multiple Operating System Vulnerability *by Rafal Wojtczuk*	File Disinfection Framework: Striking Back at Polymorphic Viruses *by Mario Vuksan + Tomislav Pericin*	<GHZ or Bust: Black Hat *by Atlas*	Advanced Chrome Extension Exploitation: Leveraging API Powers for The Better Evil *by Kyle Osborn + Krzysztof Kotowicz*
The Defense RESTs: Automation and APIs for Improving Security *by David Mortmon*	Expoiting The Jemalloc Memory Allocator: Owning Firefox's Heap *by Patroklos Argyroudis + Chariton Karamitas*	Confessions of a WAF Developer: Protocol-Level Evasion of Web Application Firewalls *by Ivan Ristic*	<GHZ or Bust: Black Hat *cont.*	Advanced Chrome Extension Exploitation: Leveraging API Powers for The Better Evil *cont.*
Control-Alt-Hack(TM): White Hat Hacking for Fun & Profit (A Computer Security Card Game) *by Tadayoshi Kohno + Tamara Denning + Adam Shostack*	The Info Leak Era on Software Exploitation *by Fermin J. Serna*	Torturing OpenSSL *by Valeria Bertacco*	Code Reviewing Web Application Framework Based Applications (Struts 2, Spring MVC, Ruby on Rails (Groovy on Grails), .NET MVC) *by Abraham Kang*	Linux Interactive Exploit Development with GDB and PEDA *by Long Le*
Intrusion Detection Along the Kill Chain: Why your Detection System Sucks and What to Do About it *by John Flynn*	Are You My Type?-Breaking.net Sandboxes Through Serialization *by James Forshaw*	WebTracking For You *by Gregory Fleischer*	Code Reviewing Web Application Framework Based Applications (Struts 2, Spring MVC, Ruby on Rails (Groovy on Grails), .NET MVC) *cont.*	Linux Interactive Exploit Development with GDB and PEDA *cont.*
Exploit Mitigation Improvements in Windows 8 *by Matt Miller + Ken Johnson*	PinPadPwn *by Nils + Rafael Dominguez Vega*	Here Be Backdoors: A Journey Into the Secrets of Industrial Firmware *by Ruben Santamarta*	Code Reviewing Web Application Framework Based Applications (Struts 2, Spring MVC, Ruby on Rails (Groovy on Grails), .NET MVC) *cont.*	From the Iriscode to the Iris: A New Vulnerability of Iris Recognition Systems *by Javier Galbally*

SCHEDULE / THU, JULY 26

Time	Track 1	Track 2	Track 3	Track 4
Track	Big Picture	Web Apps *Track Chair: Nathan Hamiel*	Malware *Track Chair: Stefano Zanero*	Enterprise Intrigue
ROOM	Augustus III + IV	Augustus I + II	Augustus V + VI	Palace I
08:00-11:00	**REGISTRATION: Emperiors Ballroom**			
08:00-08:50	**BREAKFAST: Octavius Ballroom**—*Sponsored by* Accuvant LABS			
09:00-10:00	**Keynote Speaker: Neal Stephenson: Augustus Ballroom**			
10:00-10:15	**Break / Booksigning with Neal Stephenson: Palace Pre-Function**			
10:15-11:15	Trust, Security, and Society *by Bruce Schneier*	HTML5 Top 10 Threats: Stealth Attacks and Silent Exploits *by Shreeraj Shah*	A Scientific (but not academic) Study of Malware Employs Anti-Debugging, Anti-disassemly, and Anti-virtualization Technologies *by Rodrigo Branco*	Catching Insider Data Theft With Stochastic Forensics *by Jonathan Grier*
11:15-11:45	**Coffee Service**—*Sponsored by* LogRhythm / **Booksigning with Bruce Schneier: Palace Pre-Function**			
11:45-12:45	The Christopher Columbus Rule and DHS *by Mark Weatherford*	AMF Testing Made Easy *by Luca Carettoni*	De Mysteriis Dom Jobsivs: Mac Efi Rootkits *by Loukas K*	Find Me in Your Database: An Examination of Index Security *by David Litchfield*
12:45-14:15	**Lunch: Forum Ballroom**—*Sponsored by* Microsoft			
14:15-15:15	Legal Aspects of Cyberspace Operations *by Robert Clark*	Hacking with WebSockets *by Sergey Shekyan + Vaagan Toukharian*	Dex Education: Practicing Safe Dex *by Timothy Strazzere*	Passive Bluetooth Monitoring in Scapy *by Ryan Holeman* SYNful Deceit, Stateful Subterfuge *by Tom Steele + Chris Patten* Stamp Out Hash Corruption, Crack All The Things *by Ryan Reynolds + Jonathan Claudius*
15:15-15:30	**Break**			
15:30-16:30	Targeted Intrusion Remediation: Lessons From The Front Lines *by Jim Aldridge*	Blended Threats and JavaScript: A Plan for Permanent Network Compromise *by Phil Purviance + Joshua Brashars*	Hardware Backdooring is Practical *by Jonathan Brossard*	Clonewise: Automated Package Clone Detection *by Silvio Cesare*
16:30-17:00	**Coffee Service**—*Sponsored by* Symantec.			
17:00-18:00	Hacking the Corporate Mind: Using Social Engineering Tactics to Improve Organizational Security Acceptance *by James Philput*	State of Web Exploit Toolkits *by Jason Jones*	Flowers for Automated Malware Analysis *by Chengyu Song + Paul Royal*	SSRF VS. Business Critical Applications *by Alexander Polyakov + Dmitry Chastuhin*

Track 5	Track 6	Track 7	Track 8	Track 9
92.2% Market Share	Over the Air and In the Device	Mass Effect	Applied Workshop I	Applied Workshop II
Palace II	Palace III	Romans I-IV	Florentine	Pompeian
Exploitation of Windows 8 Metro Style Apps *by Sung-ting Tsai + Ming-chieh Pan*	iOS Security *by Dallas De Atley*	Still Passing the Hash 15 Years Later? Using the Keys to the Kingdom to Access all Your Data *by Alva Duckwall + Christopher Campbell*	Lessons of Binary Analysis *by Chrstien Rioux*	The Dark Art of IOS Application Hacking *by Jonathan Zdziarski*
We have you by the Gadgets *by Mickey Shkatov + Toby Kohlenberg*	iOS Kernel Heap Armageddon Revisited *by Stefan Esser*	Recent Java Exploitation Trends and Malware *by Jeong Wook Oh*	Lessons of Binary Analysis *cont.*	The Dark Art of IOS Application Hacking *cont.*
Exchanging Demands *by Peter Hannay*	When Security Gets in the Way: Tools for PenTesting Mobile Apps That Use Certificate Pinning *by Alban Diquet + Justine Osborne* Embedded Device Firmware Vulnerability Hunting Using FRAK *by Ang Cui* Mapping and Evolution of Android Permissions *by Andrew Reiter + Zach Lanier*	Digging Deep Into The Flash Sandboxes *by Paul Sabanal + Mark Vincent Yason*	SNSCat: What You Don't Know About Sometimes Hurts the Most *by Dan Gunter + Solomon Sonya*	Ruby for Pentesters: The Workshop *by Cory Scott + Michael Tracy + Timur Duehr*
Windows Phone 7 Internals and Exploitability *by Tsukasa Oi*	iOS Application Security Assessment and Automation: Introducing SIRA *by Justin Engler + Seth Law + Joshua Dubik + David Vo*	SQL Injection to MIPS Overflows: Rooting SOHO Routers *by Zachary Cutlip*	Mobile Network Forensics *with Eric Fulton*	Ruby for Pentesters: The Workshop *cont.*
Easy Local Windows Kernel Exploitations *by Cesar Cerrudo*	How Many Bricks does it take to crack a microcell? *by Mathew Rowley*	Hookin' Ain't Easy: BeEF Injection with MITM *by Steve Ocepek + Ryan Linn*	Mobile Network Forensics *cont.*	Ruby for Pentesters: The Workshop *cont.*

KEYNOTES

CHANGING THE SECURITY PARADIGM…TAKING BACK YOUR NETWORK AND BRINGING PAIN TO THE ADVERSARY

Shawn Henry

JULY 25 / 09:00 / AUGUSTUS BALLROOM

The threat to our networks is increasing at an unprecedented rate. The hostile environment we operate in has rendered traditional security strategies obsolete. Adversary advances require changes in the way we operate, and "offense" changes the game. Former FBI Executive Assistant Director Shawn Henry explores the state of the industry from his perspective as the man who led all cyber programs for the FBI.

AN INTERVIEW WITH NEAL STEPHENSON

Neal Stephenson

JULY 26 / 09:00 / AUGUSTUS BALLROOM

Black Hat USA 2012 is proud to welcome one of the world's foremost Historical and Science Fiction authors to our keynote stage. Get your questions ready! Attendees will get the chance to ask Mr. Stephenson about his life, processes, and works… But you may want to keep your latest Cryptonomicon conspiracy theories to yourself…as of course, we can neither confirm nor deny their validity. Join us!

BRIEFINGS

A SCIENTIFIC (BUT NON ACADEMIC) STUDY OF HOW MALWARE EMPLOYS ANTI-DEBUGGING, ANTI-DISASSEMBLY, AND ANTI-VIRTUALIZATION TECHNOLOGIES.

Rodrigo Branco

JULY 26 / 10:15 / AUGUSTUS V+VI

Malware is widely acknowledged as a growing threat with hundreds of thousands of new samples reported each week. Analysis of these malware samples has to deal with this significant quantity but also with the defensive capabilities built into malware; Malware authors use a range of evasion techniques to harden their creations against accurate analysis. The evasion techniques aim to disrupt attempts of disassembly, debugging or analyse in a virtualized environment.

This talk catalogs the common evasion techniques malware authors employ, applying over 50 different static detections, combined with a few dynamic ones for completeness. We validate our catalog by running these detections against a database of 3 million samples (the system is constantly running and the numbers will be updated for the presentation), enabling us to present an analysis on the real state of evasion techniques in use by malware today. The resulting data will help security companies and researchers around the world to focus their attention on making their tools and processes more efficient to rapidly avoid the malware authors' countermeasures.

This first of its kind, comprehensive catalog of countermeasures was compiled by the paper's authors by researching each of the known techniques employed by malware, and in the process new detections were proposed and developed. The underlying malware sample database has an open architecture that allows researchers not only to see the results of the analysis, but also to develop and plug-in new analysis capabilities. The system will be made available in beta at Black Hat, with the purpose of serving as a basis for innovative community research.

A STITCH IN TIME SAVES NINE: A CASE OF MULTIPLE OPERATING SYSTEM VULNERABILITY

Rafal Wojtczuk

JULY 25 / 10:15 / PALACE III

Six years ago Linux kernel developers fixed a vulnerability that was caused by using the "sysret" privileged Intel CPU instruction in an unsafe manner. Apparently, nobody realized (or cared enough to let others know) the full impact and how widespread and reliably exploitable the problem is: in 2012, four other popular operating systems were found to be vulnerable to user-to-kernel privilege escalation resulting from the same root cause.

The presentation will explain the subtleties of the relevant Intel CPU instructions and the variety of ways they can be reliably exploited on unpatched systems. Exploits for a few affected operating systems will be demonstrated.

Attendees are expected to have basic understanding of Intel CPUs architecture.

ADVANCED ARM EXPLOITATION

Stephen Ridley
Stephen Lawler

JULY 25 / 10:15 / PALACE I

Hardware Hacking is all the rage. Early last year (2011) we at DontStuffBeansUpYourNose.com debuted a talk entitled "Hardware Hacking for Software People" *(see: http://bit.ly/pGAGlO)*. The talk was a collection of experiences and simple techniques we as laymen had discovered/used over the years to perform very simple hardware penetration testing. We covered a range of topics from hardware eavesdropping and bus tapping to simple integrated circuit interfacing and debugging. The popularity of the talk, paper/slides, and video was surprising. People were really hungry for this stuff.

Although that talk did conclude with demonstration of a real-world bug in a home cable modem, it did not dive into the gritty details of exploitation on embedded processors. Late last year (2011) we developed and privately delivered 5 day courses that taught Advanced software exploitation on ARM microprocessors (used in iPhones, appliances, iPads, Androids, Blackberries, et al.) We opened that course to the public for CanSecWest 2012 and Black Hat 2012 *(see http://bit.ly/wKHKsG)* The response to that too has been very surprising. The purpose of the talk is to reach a broader audience and share the more interesting bits of the research that went into developing the Practical ARM Exploitation course that we are giving at Black Hat 2012. We discuss reliably defeating XN, ASLR, stack cookies, etc. using nuances of the ARM architecture on Linux (in embedded applications and mobile devices). We will also demonstrate these techniques and discuss how we were able to discover them using several ARM hardware development platforms that we custom built *(see: http://bit.ly/zaKZYH)*. We will also share some anecdotal "hardware hacking" experiences we had exploiting similar bugs on embedded devices running on other platforms *(see: http://bit.ly/pGAGlO)*

ADVENTURES IN BOUNCERLAND

Nicholas Percoco
Sean Schulte

JULY 25 / 17:00 / PALACE I

Meet <REDACTED>*. He is a single function app that wanted to be much more. He always looked up those elite malware and botnet apps but now that the Google's Bouncer moved into town his hopes and dreams appeared to be shattered. This was until he was handed text file while strolling along a shady part of the Internet (AKA Pastebin). The title of this txt file was "Bypassing Google's Bouncer in 7 steps for Fun and Profit". Upon reading this, our little app began to glow with excitement. He routed himself all the way to the gates of Google Play and began his journey from a simple benign app that <REDACTED>*, to a full-fledged info stealing botnet warrior. In this presentation will tell the story of how our little app beat the Bouncer and got the girl (well, at least all her personal information, and a few naughty pics).

**Our little buddy is still having fun in the market and we don't want anyone playing around with him right now, even you CFP reviewers.*

AMF TESTING MADE EASY

Luca Carettoni

JULY 26 / 11:45 / AUGUSTUS I+II

Since its introduction in 2002, Action Message Format (AMF) has attracted the interest of developers and bug-hunters. Techniques and extensions for traditional web security tools have been developed to support this binary protocol. In spite of that, bug hunting on AMF-based applications is still a manual and time-consuming activity. Moreover, several new features of the latest specification, such as externalizable objects and variable length encoding schemes, limit the existing tools. During this talk, I will introduce a new testing approach and toolchain, reshaping the concept of AMF fuzzing. Our automated gray-box testing technique allows security researchers to build custom AMF messages, dynamically generating objects from method signatures. The approach has been implemented in a Burp Suite plugin named Blazer. This tool consents to improve the coverage and the effectiveness of fuzzing efforts targeting complex applications. Real-world vulnerabilities

discovered using Blazer will be presented as well as a generic methodology to make AMF testing easier and more robust. Adobe BlazeDS, a well-known Java remoting technology, will be used as our server-side reference implementation.

ARE YOU MY TYPE? BREAKING .NET SANDBOXES THOUGH SERIALIZATION

James Forshaw

JULY 25 / 15:30 / PALACE III

In May, Microsoft issued a security update for .NET due to a number of serious issues I found. This release was the biggest update in the product's history, it aimed to correct a number of specific issues due to unsafe serialization usage as well as changing some of the core functionality to mitigate anything which could not be easily fixed without significant compatibility issues.

This presentation will cover the process through which I identified these vulnerabilities and provide information on how they can be used to attack .NET applications, both locally and remotely, as well as demonstrating breaking out of the partial trust sandboxes used in technologies such as ClickOnce and XAML Browser Applications.

BLENDED THREATS AND JAVASCRIPT: A PLAN FOR PERMANENT NETWORK COMPROMISE

Phil Purviance
Joshua Brashars

JULY 26 / 15:30 / AUGUSTUS I+II

During Black Hat 2006, it was shown how common Web browser attacks could be leveraged bypass perimeter firewalls and "Hack Intranet Websites from the Outside." In the years since, the fundamental problems were never addressed and the Intranet remains wide open, probably because the attack techniques described had important limitations. These limitations prevented mass scale and persistent compromise of network connected devices, which include but are not limited to home broadband routers. Now in 2012, with the help of new research and next-generation technologies like HTML5, browser-based Intranet attacks have overcome many of the old limitations and improved to a new degree of scary.

This presentation will cover state-of-the-art Web browser blended threats launched with JavaScript, using zero to minimal user interaction and complete every step of the exploit attack cycle. Starting with enumeration and discovery, escalating the attack further upstream and into embedded network devices, and ultimately mass-scale permanent compromise.

BLACK OPS

Dan Kaminsky

JULY 25 / 11:45 / AUGUSTUS III-IV

If there's one thing we know, it's that we're doing it wrong. Sacred cows make the best hamburgers, so in this year's talk I'm going to play with some techniques that are obviously wrong and evil and naive. There will also be a lot of very interesting code, spanning the range from high speed network stacks to random number engines to a much deeper analysis of non-neutral networks. Finally, we will revisit DNSSEC, both in code, and in what it can mean to change the battleground in your favor.

CATCHING INSIDER DATA THEFT WITH STOCHASTIC FORENSICS

Jonathan Grier

JULY 26 / 10:15 / PALACE I

A stochastic process is, by definition, something unpredictable, but unpredictable in a precise way. Think of the molecules in a gas: we can't predict how any individual molecule will move and shake; but by accepting that randomness and describing it mathematically, we can use the laws of statistics to accurately predict the gas's overall behavior.

What's this have to do with data theft? Insider data theft often leaves no artifacts or broken windows, making it invisible to traditional forensics. But copying large amounts of data will always affect the file system, and when we look through stochastic lenses, copying sticks out like a sore thumb. Stochastic forensics is a new technique which uses these patterns to detect insider data theft, despite its lack of artifacts.

I've used these techniques to catch data theft months after its occurrence. I'll show you the statistical patterns present on a typical filesystem, the distinct patterns induced by copying, and the mathematical technique which highlights the difference. You'll learn how to spot otherwise invisible data theft.

CLONEWISE: AUTOMATED PACKAGE CLONE DETECTION

Silvio Cesare

JULY 26 / 15:30 / PALACE I

Developers sometimes statically link libraries from other projects, maintain an internal copy of other software or fork development of an existing project. This practice can lead to software vulnerabilities when the embedded code is not kept up to date with upstream sources. As a result, manual techniques have been applied by Linux vendors to track embedded code and identify vulnerabilities. We propose an automated solution to identify embedded packages, which we call package clones, without any prior knowledge of these relationships. Our approach identifies similar source files based on file names and content to identify elationships between packages. We extract these and other features to perform statistical classification using machine learning. We evaluated our automated system named Clonewise against Debian's manually created database.

Clonewise had a 68% true positive rate and a false positive rate of less than 1%. Additionally, our system detected many package clones not previously known or tracked. Our results are now starting to be used by Linux vendors such as Debian and Redhat to track embedded packages. Redhat started to track clones in a new wiki, and Debian are planning to integrate Clonewise into the operating procedures used by their security team. Based on our work, over 30 unknown package clone vulnerabilities have been identified and patched.

CONFESSIONS OF A WAF DEVELOPER: PROTOCOL-LEVEL EVASION OF WEB APPLICATION FIREWALLS

Ivan Ristic

JULY 25 / 11:45 / ROMANS I-IV

Most discussions of WAF evasion focus on bypassing detection via attack payload obfuscation. These techniques target how WAFs detect specific attack classes, and that's fine. Protocol-level evasion techniques target a lower processing layer, which is designed to parse HTTP streams into meaningful data. A successful evasion at this layer makes the WAF see a request that is different from that seen

by the victim application. Through evasion, attacks become virtually invisible. The technique can be used with any class of attack.

Especially vulnerable to this type of attack are virtual patches, which are, somewhat ironically, the most successful use case for WAFs today. I will show how, through the combination of WAF design and implementation issues, inadequate documentation and inadequate user interfaces, many virtual patches can be trivially bypassed.

In this talk I will share the lessons learned from 10 years of web application firewall development. The focus will be on demonstrating the problems that exist today, including a previously unknown flaw in ModSecurity that remained undetected for many years. In addition, I will discuss many evasion techniques that are countered in ModSecurity, but which may be effective against other tools.

As part of this talk, I will release a catalogue of protocol-level evasion techniques and a complete testing suite.

CONTROL-ALT-HACK(TM): WHITE HAT HACKING FOR FUN AND PROFIT (A COMPUTER SECURITY CARD GAME)

Tadayoshi Kohno
Tamara Denning
Adam Shostack

JULY 25 / 14:15 / PALACE II

You and your fellow players work for Hackers, Inc.: a small, elite computer security company of ethical, white hat hackers that perform security audits and provide consultation services. Their Motto: You Pay Us to Hack You.

In 1992, Steve Jackson Games published the game Hacker, satirizing the Secret Service raid that seized drafts of GURPS Cyberpunk. The Hacker game manual helpfully states, “Important Notice To Secret Service! This Is Only A Game! These Are Not Real Hacking Instructions! You Cannot Hack Into Real Computers By Rolling Little Dice!” Now, 20 years later, we wish to announce a new card game that’s fun, yes, but also designed to illustrate important aspects of computer security. We licensed our game mechanics (Ninja Burger) from none other than Steve Jackson Games, then created all-new content—complete with illustrations and graphic design—to deal with computer security topics.

Each person plays as a white hat hacker at a company that performs security audits and provides consulting services. Your job is centered around Missions—tasks that require you to apply your hacker skills (Hardware Hacking, Software Wizardry, Network Ninja, Social Engineering, Cryptanalysis, Forensics, and more) and a bit of luck in order to succeed. You gain Hacker Cred by successfully completing Missions (“Disinformation Debacle,” “Mr. Botneto”, “e-Theft Auto”) and you lose Hacker Cred when you fail. Entropy cards help you along the way with advantages that you can purchase (“Superlative Visualization Software”) and unexpected obstacles that you can use to thwart other players (“Failed to Document”). Gain enough Hacker Cred, and you win fame and fortune as the CEO of your very own consulting company.

Why a game? Entertainment provides an engaging medium with which to raise awareness of the diversity of technologies impacted by security breaches and the creativity of techniques employed by attackers. In this talk, we will describe our goals in creating the game, discuss trials involved in the game design process, and discuss the potential applications of security-themed games. Come observe a game demo, look for a free copy to give away

DE MYSTERIIS DOM JOBSIVS: MAC EFI ROOTKITS

Loukas K

JULY 26 / 11:45 / AUGUSTUS V+VI

The EFI firmware used in Intel Macs and other modern systems presents some interesting possibilities for rootkit developers. This presentation will provide a full account of how an EFI-based rootkit might work. We will begin with some background on the EFI architecture—what it does, how it works, and how we can leverage EFI to inject code into the Mac OS X kernel or attack the user directly. We will then detail how a kernel payload might work, employing a number of rootkit techniques that can be used within the XNU kernel. Finally, we will discuss the possibilities for rootkit persistence that are presented by EFI. This presentation will not require a detailed understanding of EFI, and will leave the audience with an understanding of the ways in which EFI can be used in a modern Mac OS X rootkit.

DEX EDUCATION: PRACTICING SAFE DEX

Timothy Strazzere

JULY 26 / 14:15 / AUGUSTUS V+VI

In an ecosystem full of potentially malicious apps, you need to be careful about the tools you use to analyze them. Without a full understanding of how the Android Dalvik VM or dex file interpreters actually work, it’s easy for things to slip through the cracks. Based on learnings from the evolution of PC-based malware, it’s clear that someone, somewhere will someday attempt to break the most commonly used tools for static and dynamic analysis of mobile malware. So we set out to see who was already breaking them and how, then, how we could break them more.

We’ve taken a deep dive into Android’s dex file format that has yielded interesting results related to detection of post-compilation file modification. After deconstructing some of the intricacies of the dex file format, we turned our attention to dex file analysis tools themselves, analyzing how they parse and manage the dex format. Along the way we observed a number of easily exploitable functionality, documenting specifically why they fail and how to fix them. From this output we’ve developed a proof of concept tool—APKfuscator—that shows how to exploit these flaws. It’s our hope that it can be a tool that helps everyone practice safe dex.

DIGGING DEEP INTO THE FLASH SANDBOXES

Paul Sabanal
Mark Vincent Yason

JULY 26 / 14:15 / ROMANS I-IV

Lately we have seen how sandboxing technology is positively altering the software security landscape. From the Chrome browser, to Adobe Reader, to Mac and iOS applications, sandboxing has become one of the main exploit mitigation technologies that software has come to rely on. As with all critical security technologies, they need to be understood and scrutinized, mainly to see how effective they are, or at the very least, to satisfy one’s curiosity. The sandbox implementations for Adobe’s Flash Player certainly piqued ours.

Our talk will explore the internals of three sandbox implementations for Flash: Protected Mode Flash for Chrome, Protected Mode Flash for Firefox, and Pepper Flash. And of course, we will show that an exhaustive exploration of the Flash sandboxes will eventually yield gold as we discuss and demonstrate some Flash sandbox escape vulnerabilities we found along the way.

We start with a look at the high level architecture of each sandbox implementation. Here we will define the role of each process and the connections between them. In the second part, we will dive deep into the internal sandbox mechanisms at work such as the sandbox restrictions, the different IPC protocols in use, the services exposed by higher-privileged processes, and more. In the third part of our talk we will take a look at each sandbox’s security and talk

about the current limitations and weaknesses of each implementation. We will then discuss possible avenues to achieve a sandbox bypass or escape. Throughout all this we will be pointing out the various differences between these implementations.

DON'T STAND SO CLOSE TO ME: AN ANALYSIS OF THE NFC ATTACK SURFACE

Charlie Miller

JULY 25 / 14:15 / PALACE I

Near Field Communication (NFC) has been used in mobile devices in some countries for a while and is now emerging on devices in use in the United States. This technology allows NFC enabled devices to communicate with each other within close range, typically a few centimeters. It is being rolled out as a way to make payments, by using the mobile device to communicate credit card information to an NFC enabled terminal. It is a new, cool, technology. But as with the introduction of any new technology, the question must be asked what kind of impact the inclusion of this new functionality has on the attack surface of mobile devices. In this paper, we explore this question by introducing NFC and its associated protocols.

Next we describe how to fuzz the NFC protocol stack for two devices as well as our results. Then we see for these devices what software is built on top of the NFC stack. It turns out that through NFC, using technologies like Android Beam or NDEF content sharing, one can make some phones parse images, videos, contacts, office documents, even open up web pages in the browser, all without user interaction. In some cases, it is even possible to completely take over control of the phone via NFC, including stealing photos, contacts, even sending text messages and making phone calls. So next time you present your phone to pay for your cab, be aware you might have just gotten owned.

EASY LOCAL WINDOWS KERNEL EXPLOITATION

Cesar Cerrudo

JULY 26 / 17:00 / PALACE II

For some common local Kernel vulnerabilities there is no general, multi-version and reliable way to exploit them. There have been interesting techniques published but they are not simple and/or neither they work across different Windows versions most of the time. This presentation will show some easy, reliable and cross platform techniques for exploiting some common local Windows kernel vulnerabilities. These new techniques allow even to exploit vulnerabilities that have been considered difficult or almost impossible to exploit in the past.

ERRATA HITS PUBERTY: 13 YEARS OF CHAGRIN

Jericho

JULY 25 / 15:30 / AUGUSTUS III-IV

The attrition.org Errata project has documented the shortcomings, hypocrisy, and disgraces of the information technology and security industries. For 13 years, we have acted as a watchdog and reminder that industries who sell integrity should have it as well. The public face of Errata is very different than the process that leads to it.

This presentation will give a unique insight into the history, process, and blowback that are cornerstones of the project. This will include statistics, how Errata has fallen short, how it can be improved, and where the project is going. Most importantly, it will cover how the industry can better help the project, both in staying off the pages on attrition.org, as well as contributing to it.

EXCHANGING DEMANDS

Peter Hannay

JULY 26 / 14:15 / PALACE II

Smart phones and other portable devices are increasingly used with Microsoft Exchange to allow people to check their corporate emails or sync their calendars remotely. Exchange has an interesting relationship with its mobile clients. It demands a certain level of control over the devices, enforcing policy such as password complexity, screen timeouts, remote lock out and remote wipe functionality. This behavior is usually accepted by the user via a prompt when they first connect to Exchange. However, the protocol for updating these policies provides very little in the way of security and is quickly accepted by the device, often with no user interaction required.

In this talk we will focus on the remote wipe functionality and how a potential attacker could abuse this functionality to remotely wipe devices that are connected to Exchange. By impersonating an Exchange server and sending appropriate policy updates through a simple script we are able to erase all data on devices remotely without any need for authentication. The presentation will explain how this can be accomplished and show proof of concept code for Android & iOS devices.

EXPLOIT MITIGATION IMPROVEMENTS IN WIN 8

Matt Miller
Ken Johnson

JULY 25 / 17:00 / PALACE II

Over the past decade, Microsoft has added security features to the Windows platform that help to mitigate risk by making it difficult and costly for attackers to develop reliable exploits for memory safety vulnerabilities. Some examples of these features include Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), and Visual C++'s code generation security (GS) protection for stack-based buffer overruns. In Windows 8, Microsoft has made a number of substantial improvements that are designed to break known exploitation techniques and in some cases prevent entire classes of vulnerabilities from being exploited. This presentation will provide a detailed technical walkthrough of the improvements that have been made along with an evaluation of their expected impact. In closing, this presentation will look beyond Windows 8 by providing a glimpse into some of the future directions in exploit mitigation research that are currently being explored by Microsoft.

EXPLOITATION OF WINDOWS 8 METRO STYLE

Sung-ting Tsai
Ming-chieh Pan

JULY 26 / 10:15 / PALACE II

Windows 8 introduces lots of security improvements, one of the most interesting feature is the Metro-style app. It not only provides fancy user interface, but also a solid application sandbox environment.

All Metro-style application run in AppContainer, and the AppContainer sandbox isolates the execution of each application. It can make sure that an App does not have access to capabilities that it hasn't declared and been granted by the user.

This presentation will introduce the design of Metro-style app as well as AppContainer sandbox. We will dive into details of the architecture and see how it works, how does it protect from a malicious App attack. After reviewing the design, we will discuss some logic flaws that we have discovered, and demonstrate how do we bypass AppContainer to access files, launch program, connect to Internet. And also we will introduce how do we implement exploit/shellcode in Metro-style app by demonstrating a memory corruption vulnerability in a Broker process.

EXPLOITING THE JEMALLOC MEMORY ALLOCATOR: OWNING FIREFOX'S HEAP

Patroklos Argyroudis
Chariton Karamitas

JULY 25 / 11:45 / PALACE III

Jemalloc is a userland memory allocator that is being increasingly adopted by software projects as a high performance heap manager. It is used in Mozilla Firefox for the Windows, Mac OS X and Linux platforms, and as the default system allocator on the FreeBSD

Able To Leap Tall Buildings...

...and find the right people to strengthen your organization.

- *Building Organizations*
- *Securing Relationships*
- *Developing Leaders*

For 26 years Alta Associates has been an integral and trusted member of the Information Security, IT Risk Management and GRC community offering the most sought after, respected team of recruiters led by a CEO named, "one of the 25 most influential women in information security" by *Information Security* Magazine.

The industry's most trusted recruiting partner

Alta ASSOCIATES
specialists in executive recruiting

To learn more about Alta Associates, please visit **www.altaassociates.com**

EWF
October 2-4, 2012
Hyatt Regency at Gainey Ranch
Scottsdale, AZ

To continue promoting diversity and investing in the creation of future leaders, Alta Associates–once again–proudly hosts the Executive Women's Forum on Information Security, Privacy & Risk Management; the annual Women of Influence Awards; and EWF Scholarship program.

Register now for the 10th Annual EWF National Conference:

Managing Current & Future Risks Globally

Gain a Security, Privacy, Risk and Leadership perspective on latest trends, challenges, and game changing solutions for an increasingly mobile workforce.

www.ewf-usa.com

and NetBSD operating systems. Facebook also uses jemalloc in various components to handle the load of its web services. However, despite such widespread use, there is no work on the exploitation of jemalloc.

Our research addresses this. We will begin by examining the architecture of the jemalloc heap manager and its internal concepts, while focusing on identifying possible attack vectors. jemalloc does not utilize concepts such as 'unlinking' or 'frontlinking' that have been used extensively in the past to undermine the security of other allocators. Therefore, we will develop novel exploitation approaches and primitives that can be used to attack jemalloc heap corruption vulnerabilities. As a case study, we will investigate Mozilla Firefox and demonstrate the impact of our developed exploitation primitives on the browser's heap. In order to aid the researchers willing to continue our work, we will also release our jemalloc debugging tool belt.

FILE DISINFECTION FRAMEWORK: STRIKING BACK AT POLYMORPHIC VIRUSES

Mario Vuksan
Tomislav Pericin

JULY 25 / 10:15 / ROMANS I-IV

"Invincibility lies in the defense; the possibility of victory in the attack." – Sun Tzu

Polymorphic viruses make up an ever-increasing percentage of daily malware collections. The sophistication of these attacks significantly exceeds the capabilities of existing classification and handling solutions. The situation goes from bad to worse when we attempt the most complicated part of incident response, file disinfection and remediation.

To combat this problem we've created a new open source project, the File Disinfection Framework (FDF), built on top of a new generation of TitanEngine and tailored specifically to aid in solving these hard problems. FDF combines both static analysis and emulation to enable users to rapidly switch between modes of operation to use the best features of each approach. Highly advanced static functions are hidden behind a simple and easy-to-use program interface that enables the broad range of capabilities that are required for decryption, decompression and disinfection. Their complement is a set of functions that enable quick and very customizable emulation. For the first time, analysts will have the ability to truly see and control everything that happens inside the emulated environment. They can run high level code inside the context of the emulated process to influence objects and files and direct the execution flow.

File disinfection framework features:

Static analysis functionality that has the ability to view, modify and build on-the-fly PE32/PE32+ files, fields and tables. A large number of embedded decompression routines is included along with systems that dynamically define static structures and build polymorphic decrypters.

Highly advanced PE32/PE32+ file validation and repair functionality that completely solves the issues brought up by our last year's Black Hat presentation titled "Constant insecurity: Things you didn't know about PE file format". These functions accurately detect and identify all purposely-malformed PE files that break current security tools or evade detection. In addition, if the file is damaged (as usually happens during virus infections) and deemed repairable, it is automatically repaired to maximize the number of remediated files.

Integrated hash database functionality that helps to resolved the otherwise unsolvable problem of reverting function name hashes back to their original names. This custom database is easily extended to add even more libraries and functions to its known hash lists.

A truly unique x86 emulator written from scratch that supports the following Windows features:

- Multiple processes in parallel each in a separate emulated OS
- Vital Windows structures: PEB, TEB (with multiple threads) and SEH
- x86 assembly code execution with support for FPU and MMX instructions
- Windows objects such as handles, mutexes and environment variables
- Hundreds of standard Windows APIs that can easily be extended by the user
- Dynamically build libraries that mirror the application requirements
- The entire file system with customizable drives
- Interface which matches the standard Windows debug API
- Use of emulated APIs which are directly exposed to user

User can call standard Windows APIs inside the context of an emulated process. For example the user can dynamically create a new DLL file inside the virtual file system and load it into the context of an emulated process by calling LoadLibrary equivalent. Every emulated API is exposed to the user and therefore usable with the option of hooking any API one or more times.

Advanced breakpoint logic which includes breakpoints on specific instruction groups and specific instruction behavior such as read or write to a specific part of the memory

Seamless switching between emulation and static analysis

Specific functionally designed to disinfect files infected with polymorphic viruses such as Virut and Sality with examples that show its use.

Tools to aid in writing disinfection routines such as automatic binary profiling with search for the presence and location of the virus stub.

File disinfection framework has been developed under the cyber fast track program run by DARPA and built on top of the new generation of TitanEngine. It's an open source cross platform x86-x64 library that enables its user to unpack, disinfect and build PE32/PE32+ files. These and all Emulation components of the new major release of this framework have been designed to be presented as a Black Hat exclusive. This talk will be followed by the public release of the source code along with whitepapers that outline possible use case scenario for this technology.

FIND ME IN YOUR DATABASE: AN EXAMINATION OF INDEX SECURITY

David Litchfield

JULY 26 / 11:45 / PALACE I

This talk will look at the Oracle indexing architecture and examine some new flaws, with demonstration exploits. We'll also discuss how to find such issues in custom applications as well as an examination of the forensic aspects.

FLOWERS FOR AUTOMATED MALWARE ANALYSIS

Chengyu Song
Paul Royal

JULY 26 / 17:00 / AUGUSTUS V+VI

Malware, as the centerpiece of threats to the Internet, has increased exponentially. To handle the large volume of malware samples collected each day, numerous automated malware analysis techniques have been developed. In response, malware authors have made analysis environment detections increasingly popular and commoditized. In turn, security practitioners have created systems that make an analysis environment appear like a normal system (e.g., baremetal malware analysis). Thus far, neither side has claimed a definitive advantage.

In this presentation, we demonstrate techniques that, if widely adopted by the criminal underground, would permanently disadvantage automated malware analysis by making it ineffective and unscalable. To do so, we turn the problem of analysis environment detection on its head. That is, instead of trying to design techniques that detect specific analysis environments, we instead propose malware that will fail to execute correctly on any environment other than the one originally infected.

To achieve this goal, we developed two obfuscation techniques that make the successful execution of a malware sample dependent on the unique properties of the original infected host. To reinforce the potential for malware authors to leverage this type of analysis resistance, we discuss the Flashback botnet's use of a similar technique to prevent the automated analysis of its samples.

FROM THE IRISCODE TO THE IRIS: A NEW VULNERABILITY OF IRIS RECOGNITION SYSTEMS

Javier Galbally

JULY 25 / 17:00 / POMPEIAN

A binary iriscode is a very compact representation of an iris image, and, for a long time, it has been assumed that it did not contain enough information to allow the reconstruction of the original iris. The present work proposes a novel probabilistic approach to reconstruct iris images from binary templates and analyzes to what extent the reconstructed samples are similar to the original ones (that is, those from which the templates were extracted). The performance of the reconstruction technique is assessed by estimating the success chances of

an attack carried out with the synthetic iris patterns against a commercial iris recognition system. The experimental results show that the reconstructed images are very realistic and that, even though a human expert would not be easily deceived by them, there is a high chance that they can break into an iris recognition system.

GHOST IS IN THE AIR (TRAFFIC): ON SECURITY ASPECTS OF ADS-B AND OTHER "FLYING" TECHNOLOGY

Andrei Costin

JULY 25 / 17:00 / AUGUSTUS V-VI

Air-related technologies are on the verge of tehnological upgrade and advance in approximately the same manner the mobile communication networks and smartphones were 5-10 years.

As noticed in practice, these technological advances open opportunities for performance and innovation, but at the same time open great opportunity for security exploitation.

In this talk and whitepaper, we will approach the ADS-B (in)security from the practical angle, presenting the feasibility and techniques of how potential attackers could play with generated/injected airtraffic and as such potentially opening new attack surfaces onto AirTrafficControl systems.

GOOGLE NATIVE CLIENT: ANALYSIS OF A SECURE BROWSER PLUGIN SANDBOX

Chris Rohlf

JULY 25 / 11:45 / AUGUSTUS I-II

Native Client is Google's attempt at bringing millions of lines of existing C/C++ code to the Chrome web browser in a secure sandbox through a combination of software fault isolation, a custom compiler toolchain and a secure plugin architecture. Sound challenging? It is! Native Client isn't a typical browser extension and it certainly isn't ActiveX. Native Client allows for all sorts of applications to run inside in your browser, everything from games to PDF readers. In this talk I will cover the basics of the Native Client sandbox and general security relevant architecture including PPAPI (the replacement for NPAPI), vulnerabilities I discovered via source review in the PPAPI interface and finally a tool that dynamically generates code to fuzz the Native Client PPAPI interfaces based on the IDL (Interface Description Language) files found in the Chrome source tree.

HACKING THE CORPORATE MIND: USING SOCIAL ENGINEERING TACTICS TO IMPROVE ORGANIZATIONAL SECURITY ACCEPTANCE

James Philput

JULY 26 / 17:00 / AUGUSTUS III+IV

Network defenders face a wide variety of problems on a daily basis. Unfortunately, the biggest of those problems come from the very organizations that we are trying to protect. Departmental and organizational concerns are often at odds with good security practices. As information security professionals, we are good at designing solutions to protect our networks, and the data housed on them. That said, we are awful at communicating the need for these controls in a way that the users will either understand or listen to. In this presentation, I will discuss using social engineering techniques against your organization's users. Through the application of social engineering tactics, I will show how to bridge the gulf between the user and the information security team. Allowing for better security awareness, better adherence to information security policy, and fewer difficulties in user acceptance.

HACKING THE CORPORATE MIND: HACKING WITH WEBSOCKETS

Sergey Shekyan
Vaagn Toukharian

JULY 26 / 14:15 / AUGUSTUS I+II

HTML5 isn't just for watching videos on your iPad. Its features may be the target of a security attack as much as they may be used to improve an attack. Vulnerabilities like XSS have been around since the web's beginning, but exploiting them has become increasingly sophisticated. HTML5 features like WebSockets are part of the framework for controlling browsers compromised by XSS.

This presentation provides an overview of WebSockets. How they might increase the attack surface of a web site, their implications for privacy, and the potential security problems with protocols tunneled over them. Then it demonstrates how WebSockets can be used as an effective part of a hacking framework.

It closes with recommendations for deploying WebSockets securely, applying security principles to web app design, and providing a tool for exploring WebSockets security.

HARDWARE BACKDOORING IS PRACTICAL

Jonathan Brossard

JULY 26 / 15:30 / AUGUSTUS V+VI

This presentation will demonstrate that permanent backdooring of hardware is practical. We have built a generic proof of concept malware for the intel architecture, Rakshasa, capable of infecting more than a hundred of different motherboards. The first net effect of Rakshasa is to disable NX permanently and remove SMM related fixes from the BIOS, resulting in permanent lowering of the security of the backdoored computer, even after complete earasing of hard disks and reinstallation of a new operating system. We shall also demonstrate that preexisting work on MBR subvertions such as bootkiting and preboot authentication software bruteforce can be embedded in Rakshasa with little effort. More over, Rakshasa is built on top of free software, including the Coreboot project, meaning that most of its source code is already public. This presentation will take a deep dive into Coreboot and hardware components such as the BIOS, CMOS and PIC embedded on the motherboard, before detailing the inner workings of Rakshasa and demo its capabilities. It is hoped to raise awareness of the security community regarding the dangers associated with non open source firmwares shipped with any computer and question their integrity. This shall also result in upgrading the best practices for forensics and post intrusion analysis by including the afore mentioned firmwares as part of their scope of work.

HERE BE BACKDOORS: A JOURNEY INTO THE SECRETS OF INDUSTRIAL FIRMWARE

Ruben Santamarta

JULY 25 / 17:00 / ROMANS I-IV

PLCs, Smart Meters, SCADA, Industrial Control Systems…nowadays all those terms are well known for the security industry. When critical Infrastructures come into play, the security of all those systems and devices that control refineries, Water treatment or nuclear plants pose a significant attack vector.

For years, the isolation of that world provided the best 'defense' but things are changing and that scenario is no longer valid. Is it feasible to attack a power plant without ever visiting one? Is is possible to hack into a Smart meter…without having that Smart Meter? Yes, it is. This talk discusses the approach followed to do so, mixing theory and practice.

This presentation pivots around the analysis of firmware through reverse engineering in order to discover additional scenarios such as backdoors, confidential documentation or software, vulnerabilities... Everything explained will be based on real cases, unveiling curious 'features' found in industrial devices and finally disclosing some previously unknown details of an interesting case: a backdoor discovered in a family of Smart Meters. We will navigate through the dark waters of Industrial Control Systems, where the security by obscurity has ruled for years. Join us into this journey, here be backdoors…

HOOKIN' AIN'T EASY: BEEF INJECTION WITH MITM

Steve Ocepek
Ryan Linn

JULY 26 / 17:00 / ROMANS I-IV

Kiddies gotta make the money, and it don't come easy when those mean users don't click our links. And if there aren't any ports open, what's a PenTest John to do?? If you are curious about hooking browsers without yucky social engineering or XSS, getting the goods through proxy hosts, or even if you're just BeEF-curious, this is the one you've been waiting for.

This talk is about, that's right, BEEF INJECTION: a completely unabashed love story between MITM and the BeEF Framework. Through demos and new code, we'll show you how to hook up with browsers using old pickup lines like ARP Poisoning and Karma Attacks, and once you get their digits, we'll even show you how to maintain that relationship, and use it to get even more connections you never dreamed of. Featuring in-depth BeEF tips by Ryan Linn, author of "Coding for Penetration Testers", and Steve Ocepek, creator of thicknet and the seminal favorite, "How to Get a Date Using Unshielded Twisted Pair and a Hot Glue Gun", you too can get in on the Pro Tips and up your IEEE 802 dating game.

HOW MANY BRICKS DOES IT TAKE TO CRACK A MICROCELL?

Mathew Rowley

JULY 26 / 17:00 / PALACE III

This is a tale of a journey that tested almost every security related skill I have acquired over the past six years. It is a story of a software hackers trip through a hardware hackers world; a story of successes, failures, logic flaws and learning.

This talk is my adventure through reverse engineering a 3G microcell. It will cover topics from hardware hacking, kernel reversing, firmware extraction and manipulation, software reversing, networking, memory forensics, social engineering, and more. I have gained a wealth of knowledge going through the process of completely pulling apart this device and want to share my trial and errors. The talk covers such a broad spectrum of topics with differential depths that anyone attending should obtain some knowledge they previously did not have.

HOW THE ANLYSIS OF ELECTICAL CURRENT CONSUMPTION OF EMBEDDED SYSTEMS COULD LEAD TO CODE REVERSING?

Yann Allain
Julien Moinard

JULY 25 / 11:45 / AUGUSTUS V-VI

A practical approach of Power Analysis dedicated to reverse Engineering

This submission presents an experimental protocol developed to extract (part of) the code that runs on an embedded system using its power consumption

Experimental content (no math!), proof of concept, tools, limits, protections and prospective

The purpose of our study is to try to show how the analysis of electrical consumption of an embedded system enables us to find parts of the codes that it executes; this is done by presenting an operating mode, tools, a solid analysis, results, counter-measures and future research axes. It is all about trying to find another approach to the audit system. This approach aims at acquiring the code (reverse engineering) without having a physical access to the internal system components.

Our submission content will consist in making a quick presentation of the physical phenomenon at the origin of this type of information leak, confirming whether a sequence of instructions (opcode and data) can be found (reversed) by the analysis of electrical current used by the embedded system during the execution of a program, assessing then overcoming the technical difficulties in its achievement (Signal Acquisition, treatment and analysis, limitsÉ), presenting a proof of concept and possible countermeasures to limit the risks.

HTML5 TOP 10 THREATS: STEALTH ATTACKS AND SILENT EXPLOITS

Shreeraj Shah

JULY 26 / 10:15 / AUGUSTUS I+II

HTML5 is an emerging stack for next generation applications. HTML5 is enhancing browser capabilities and able to execute Rich Internet Applications in the context of modern browser architecture. Interestingly HTML5 can run on mobile devices as well and it makes even more complicated. HTML5 is not a single technology stack but combination of various components like XMLHttpRequest (XHR), Document Object model (DOM), Cross Origin Resource Sharing (CORS) and enhanced HTML/Browser rendering. It brings several new technologies to the browser which were not seen before like localstorage, webSQL, websocket, webworkers, enhanced XHR, DOM based XPATH to name a few. It has enhanced attack surface and point of exploitations for attacker and malicious agents. By leveraging these vectors one can craft stealth attacks and silent exploits, it is hard to detect and easy to compromise. In this paper and talk we are going to walk through these new architectures, attack surface and possible threats. Here is the top 10 threats which we are going to cover in detail with real life examples and demos.

- A1—CORS Attacks & CSRF
- A2—ClickJacking, CORJacking and UI exploits
- A3—XSS with HTML5 tags, attributes and events
- A4—Web Storage and DOM information extraction
- A5—SQLi & Blind Enumeration
- A6—Web Messaging and Web Workers injections
- A7—DOM based XSS with HTML5 & Messaging
- A8—Third party/Offline HTML Widgets and Gadgets
- A9—Web Sockets and Attacks
- A10—Protocol/Schema/APIs attacks with HTML5

Above attack vectors and understanding will give more idea about HTML5 security concerns and required defense. It is imperative to focus on these new attack vectors and start addressing in today's environment before attackers start leveraging these features to their advantage. We are going to see new tricks for HTML5 vulnerabilities scanning and tools.

INTRUSION DETECTION ALONG THE KILL CHAIN: WHY YOUR DETECTION SYSTEM SUCKS AND WHAT TO DO ABOUT IT

John Flynn

JULY 25 / 15:30 / PALACE II

The field of intrusion detection is a complete failure. Vendor products at best address a narrow part of the problem and more typically are completely worthless at detecting sophisticated attacks. This talk discusses the fundamental problems in the field and why the state of the art isn't good enough. We then introduce the concept of the attacker plane and the kill chain how to use them to make a much more sophisticated intrusion detection system. Finally we cover ways of putting them into action. Even veterans of the field will find something new here.

IOS APPLICATION SECURITY ASSESSMENT AND AUTOMATION: INTRODUCTING SIRA

Justin Engler
Seth Law
Joshua Dubick
David Vo

JULY 26 / 15:30 / PALACE III

Apple's AppStore continues to grow in popularity, and iOS devices continue to have a high perception of security from both users and experts. However, applications on the AppStore often have security or privacy flaws that are not apparent, even to sophisticated users. Security experts can find these flaws via manual tests, but the enormity of the AppStore ensures that only a small minority of apps could ever be manually tested.

This presentation will demonstrate a new tool and methodology to perform automated or semi-automated assessment of iOS applications and assist with manual testing. In addition, our findings about the prevalence of different types of security issues in iOS applications will be discussed, giving a window into the risks of trusting your data to products on the AppStore.

IOS KERNAL HEAP ARMAGEDDON REVISTED

Stefan Esser

JULY 26 / 11:45 / PALACE III

Previous work on kernel heap exploitation for iOS or Mac OS X has only covered attacking the freelist of the kernel heap zone allocator. It was however never discussed before what other kernel heap memory allocators exist or what kernel heap allocation functions wrap these allocators. Attacks against further heap meta data or attacking kernel application data has not been discussed before.

This talk will introduce the audience to the big picture of memory allocators in the iOS kernel heap. It will be shown how attacks can be carried out against other meta data stored by other allocators or wrappers. It will be shown how memory allocated into different zones or allocated by different allocators is positioned to each other and if cross attacks are possible. It will be shown how overwriting C++ objects inside the kernel can result in arbitrary code execution. Finally this talk will leverage this to present a generic technique that allows to control the iOS kernel heap in a similar fashion as JavaScript is used in today's browser exploits to control the user space heap.

IOS SECURITY

Dallas De Atley

JULY 26 / 10:15 / PALACE III

Apple designed the iOS platform with security at its core. In this talk, Dallas De Atley, manager of the Platform Security team at Apple, will discuss key security technologies in iOS.

LEGAL ASPECTS OF CYBERSPACE OPERATIONS

Robert Clark

JULY 26 / 14:15 / AUGUSTUS III+IV

This presentation examines the legal regime surrounding cyberspace operations. The analysis looks at the legal underpinnings of computer network security; defense; exploitation; and, attack. After covering the laws and policies related to these topics, we will examine several of the recent incidents and intrusions that have occurred and discuss why none of them have been classified as "attacks" by those who could do so. Attendees will get an understanding of the hot legal topics in computer network operations. Past presentations have shown much of what is taken away is audience driven in response to their questions and the subsequent discussion. And, as always, I try to impress upon computer security professionals the importance of working closely with their legal counsel early and often, and explaining the technical aspects of computer security to their attorneys at a third grade level so my profession can understand it and then turn around and explain it to a judge or jury at a first grade level. (All material is unclassified and available in the public domain.)

LOOKING INTO THE EYE OF THE METER

Don C. Weber

JULY 25 / 14:15 / AUGUSTUS V-VI

When you look at a Smart Meter, it practically winks at you. Their Optical Port calls to you. It calls to criminals as well. But how do criminals interact with it? We will show you how they look into the eye of the meter. More specifically, this presentation will show how criminals gather information from meters to do their dirty work. From quick memory acquisition techniques to more complex hardware bus sniffing, the techniques outlined in this presentation will show how authentication credentials are acquired. Finally, a method for interacting with a meter's IR port will be introduced to show that vendor specific software is not necessary to poke a meter in the eye.

This IS the talk that was not presented at ShmooCon 2012 in response to requests from a Smart Grid vendor and the concerns of several utilities. We have worked with them. They should be okay with this.....should.....

MY ARDUINO CAN BEAT UP YOUR HOTEL ROOM LOCK

Cody Brocious

JULY 24 / PALACE III

Nearly ten million Onity locks are installed in hotels worldwide, representing 1/3 of hotels and about 50% of hotel locks. Chances are good that you've stayed in dozens of such hotels in your life and you may even be staying in one tonight. This presentation will show, in detail, how they're designed and implemented. Then we will take a look at how they are insecure by design and release a number of critical, unpatchable vulnerabilities.

You will never see locks the same way again.

OWNING BAD GUYS {AND MAFIA} WITH JAVASCRIPT BOTNENTS

Chema Alonso

JULY 25 / 17:00 / AUGUSTUS I-II

Man in the middle attacks are still one of the most powerful techniques for owning machines. In this talk mitm schemas in anonymous services are going to be discussed. Then attendees will see how easily a botnet using javascript can be created to analyze that kind of connections and some of the actions of bad people, mafia, scammers, etc... behind those services are doing... in real. It promises to be funny

PINPADPWN

Nils

Rafael Dominguez Vega

JULY 25 / 17:00 / PALACE III

Pin Pads or Payment Terminals are widely used to accept payments from customers. These devices run Payment Applications on top of the device specific firmware. It shouldn't come as no surprise to anyone that these applications and operating systems are just as vulnerable as any other systems when it comes to handling user input.

As the use of Chip and Pin continues to replace the fairly basic magnetic stripe cards, these devices are handling more and more complex information from untrusted sources; namely the EMV protocol spoken by all major payment smart-cards. On top of this many of these terminals are connected through Ethernet, GPRS, WiFi or phone lines, which add to the overall

attack surface.

We will demonstrate that memory corruption vulnerabilities in payment terminals and applications are a reality and that they can be used to gain code execution on the terminals. Furthermore we will demonstrate and discuss potential payloads and how these can profit an attacker.

PRNG: PWNING RANDOM NUMBER GENERATIONS (IN PHP APPLICATIONS)

George Argyrous
Aggelos Kiayias

JULY 25 / 15:30 / AUGUSTUS I-II

We present a number of novel, practical, techniques for exploiting randomness vulnerabilities in PHP applications. We focus on the predictability of password reset tokens and demonstrate how an attacker can take over user accounts in a web application via predicting the PHP core randomness generators.

Our suite of new techniques and tools go far beyond previously known attacks (e.g. Kamkar and Esser) and can be used to mount attacks against all PRNG of the PHP core system even when it is hardened with the Suhosin extension. Using them we demonstrate how to create practical attacks for a number of very popular PHP applications (including Mediawiki, Gallery, osCommerce and Joomla) that result in the complete take over of arbitrary user accounts.

While our techniques are designed for the PHP language, the principles behind]them are independent of PHP and readily apply to any system that utilizes weak randomness generators or low entropy sources.

We will also release tools that assist in the exploitation of randomness vulnerabilities and exploits for some vulnerable applications.

PROBING MOBILE OPERATOR NETWORKS

Collin Mulliner

JULY 25 / 15:30 / PALACE I

Cellular networks do not only host mobile and smart phones but a wide variety of other devices. We investigated what kind of devices currently sit on cellular networks. In this talk we provide a walk through on how to probe cellular networks from start to end. Finally we show some of our results from our effort and discuss the security implications of our findings.

RECENT JAVA EXPLOITATION TRENDS AND MALWARE

Jeong Wook Oh

JULY 26 / 11:45 / ROMANS I-IV

We are seeing more and more Java vulnerabilities exploited in the wild. While it might surprise many users, and even some people in the industry, to hear that Java is currently a major vector for malware propagation, attackers haven't forgotten that it is still installed and used on a huge number of systems and devices, including those running Microsoft Windows, Mac OSX and different flavors of Unix. Since Java supports multiple platforms, one Java vulnerability can sometimes lead to exploitation on multiple platforms.

Java vulnerabilities are often about evading the sandbox. With sandbox evasion vulnerabilities, the exploitation is much easier and multi-platform attacks are feasible—all those security measures against memory corruption issues won't help. The widely-exploited CVE-2012-0507 vulnerability, for example, was a sandbox breach. We saw active Mac OSX system breaches using this vulnerability, and before that, the vulnerability was used for widespread infection of Windows systems. The cost of writing multi-platform exploits is relatively low and the success rate of exploitation is high.

As we can see, Java vulnerabilities have become more and more popular. However, there is a lack of knowledge on how exploitation of these vulnerabilities actually works. Many Java vulnerabilities result in a sandbox breach, but the way the breach happens is quite a complex process. In this presentation, we will look at some recent Java vulnerabilities and show where these vulnerabilities occur. We will also show you how the exploitation happens and how the bad guys adapt them to use in their arsenal. Of course, Java exploits and malware are written in Java. That opens up an easy way for the attackers to obfuscate and hide their exploits inside complicated logic and code. On the other hand, it means a hard life for security researchers. We are also going to show you an example of an exploit that was obfuscated and modified in a way that made analysis and detection difficult. We share Java debugging techniques and our experience in dealing with these problems.

SCALING UP BASEBAND ATTACKS: MORE (UNEXPECTED) ATTACK SURFACE

Ralf-Phillip Weinmann

JULY 25 / 11:45 / PALACE I

Baseband processors are the components of your mobile phone that communicate with the cellular network. In 2010 I demonstrated the first vulnerabilities in baseband stacks that were remotely exploitable using a fake base station.

Subsequently, people assumed that baseband attacks are attack vectors requiring some physical proximity of the attacker to the target. In this talk we will uproot this narrow definition and show an unexpected attack vector that allows an attacker to remotely exploit bugs in a certain component of the baseband stack over an IP connection. Depending on the configuration of certain components in the carrier network, a large population of smartphones may be simultaneously attacked without even needing to set up your own base station.

SEXYDEFENSE-MAXIMIZING THE HOME-FIELD ADVANTAGE

Iftach Ian Amit

JULY 25 / 10:15 / PALACE II

Offensive talks are easy, I know. But the goal of offensive security at the end of the day is to make us better defenders. And that's hard. Usually after the pentesters (or worst—red team) leaves, there's a whole lot of mess of vulnerabilities, exposures, threats, risks and wounded egos. Now comes the money time—can you fix this so your security posture will actually be better the next time these guys come around?

This talk focuses mainly on what should be done (note—no what should be BOUGHT—you probably have most of what you need already in place and you just don't know it yet).

The talk will show how to expand the spectrum of defenders from a reactive one to a proactive one, will discuss ways of performing intelligence gathering on your opponents, and modeling that would assist in focusing on an effective defense rather than a "best practice" one. Methodically, defensively, decisively. Just like the red-team can play ball cross-court, so should you!

SMASHING THE FUTURE FOR FUN AND PROFIT

Jeff Moss
Bruce Schneier
Adam Shostack
Marcus Ranum
Jennifer Granick

JULY 25 / 10:15 / AUGUSTUS I-VI

Has it really been 15 years? Time really flies when keeping up with Moore's law is the measure. In 1997, Jeff Moss held the very first Black Hat. He gathered together some of the best hackers and security minds of the time to discuss the current state of the hack. A unique and neutral field was created in which the security community—private, public, and independent practitioners alike—could come together and exchange research, theories, and experiences with no vendor influences. That idea seems to have caught on. Jeff knew that Black Hat could serve the community best if it concentrated on finding research by some of the brightest minds of the day, and he had an uncanny knack for finding them.

Please join Black Hat for this very special session, as we bring the 5 of the original 1997 speakers: Jeff Moss, Bruce Schneier, Marcus Ranum, Adam Shostack, and Jennifer Granick to share their vision of Security over the next 15 years. One of Black Hat's core values is its focus on cutting edge research and emergent technologies. So there will be no war stories in this session. This is no panel either. Each speaker will have the opportunity to deliver his or her own view. Based on the track records…. take good notes.

SNSCAT: WHAT YOU DON'T KNOW ABOUT SOMETIMES HURTS THE MOST

Dan Gunter
Solomon Sonya

JULY 26 / 14:15 / FLORENTINE

A vulnerability exists through the use of Social Networking Sites that could allow the exfiltration / infiltration of data on "secured networks". SNSCat provides a simple to use post-penetration data

exfiltration/infiltration and C2 (Command and Control) platform using images and documents on social media sites (Facebook, Google Apps, twitter, imgur, etc). The first part of our presentation will focus on case studies demonstrating the risks assumed by allowing social media sites on business networks both by malicious insiders and outsiders. After coverage of preliminary terms and concepts, we will introduce our tool and show how one can easily move files in and out of a network using social media sites. We will next demonstrate how one can use SNSCat along with the implants we have created to establish full command and control between the controller and the listening agents. Automation of commands is vital in establishing a robust botnet covertly communicating and responding to instructions from the controller. Anonymity is also essential which keeps the attacker and victim networks from ever touching each other. SNSCat is built to provide these very functions! Finally, we will introduce how one can plug in their own home-brewed steganography and cryptology modules as well as how one can build connectors for additional sites into our framework. In a 60 minute presentation, we will show you how to bypass network security equipment via social networking sites to mask data infiltration/exfiltration and C2 from any network with access to social networking sites.

SQL INJECTION TO MIPS OVERFLOWS: ROOTING SOHO ROUTERS

Zachary Cutlip

JULY 26 / 15:30 / ROMANS I-IV

This presentation details an approach by which SQL injection is used to exploit unexposed buffer overflows, yielding remote, root-level access to Netgear wireless routers. Additionally, the same SQL injection can be used to extract arbitrary files, including plain-text passwords, from the file systems of the routers. This presentation guides the audience through the vulnerability discovery and exploitation process, concluding with a live demonstration. In the course of describing several vulnerabilities, I present effective investigation and exploitation techniques of interest to anyone analyzing SOHO routers and other embedded devices.

SSRF VS. BUSINESS CRITICAL APPLICATIONS

Alexander Polyakov
Dmirtry Chastuhin

JULY 26 / 17:00 / PALACE I

Typical business critical applications have many vulnerabilities because of their complexity, customizable options and lack of awareness. Most countermeasures are designed to secure system using firewalls and DMZ's so that, for example, to enter technology network from the Internet, attacker has to bypass 3 or more lines of defense. It looks ok until somebody finds a way to attack secured system through trusted sources. With the help of SSRF and one of its implementations Ð XXE Tunneling Ð it is possible to root a system within one request which will be from trusted source and will bypass all restrictions.

SSRF, as in Server Side Request Forgery. A great concept of the attack which was discussed in 2008 with very little information about theory and practical examples. We have decided to change it and conducted a deep research in this area. As we deal with ERP security, we take SAP as the example for practicing SSRF attacks. The idea is to find victim

Copyright © 2012, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. 81712

server interfaces that will allow sending packets initiated by victim's server to the localhost interface of the victim server or to another server secured by firewall from outside. Ideally this interface must allow us to send any packet to any host and any port. And this interface must be accessed remotely without authentication or at least with minimum rights. Looks like a dream but this is possible. Why this attack is especially dangerous to SAP? Because many restrictions preventing the exploitation of previously found vulnerabilities, for example in RFC and Message Server or Oracle auth, prevent only attacks from external sources but not from localhost!

We have found various SSRF vulnerabilities which allow internal network port scanning, sending any HTTP requests from server, bruteforcing backed and more but the most powerful technique was XXE Tunneling. We made a deep research of the XXE vulnerability and most of the popular XML parsers and found that it can be used not only for file reading and hash stealing but even for getting shell or sending any packet to any host (0-day). What does it mean for business critical systems? Actually XML interfaces are normally used for data transfer between Portal's, ERP's, BI's, DCS's, SCADA's and other systems. Using an XXE vulnerability you can bypass firewalls and other security restrictions. What about practice? To show a real threat we took the most popular business application platform Ð SAP NetWeaver and its various XML parsers. We found that it is possible to bypass almost all security restrictions in SAP systems. Using XXE Tunneling it is possible to reopen many old attacks and conduct new ones which were impossible before.

A tool called XXEScanner which will help to gain critical information from server, make scans and execute attacks on victim host or backend will be released as part of the OWASP-EAS project.

STATE OF WEB EXPLOIT TOOLKITS

Jason Jones

JULY 26 / 17:00 / AUGUSTUS I+II

Web exploit toolkits have become the most popular method for cybercriminals to compromise hosts and to leverage those hosts for various methods of profit. This talk will give a deep dive on some of the most popular exploit kits available today including Blackhole and Phoenix and also take a look at some of the newer players that have appeared from Asia. An overview of how each kit is constructed, analysis of its observed shellcodes, obfuscations, and exploits will be presented to give a better understanding of the differences and similarities between these kits, ways that we have developed to harvest data from them and any trends that may be present.

STILL PASSING THE HASH 15 YEARS LATER? USING THE KEYS TO THE KINGDOM TO ACCESS ALL YOUR DATA

Alva Duckwall
Christopher Campbell

JULY 26 / 10:15 / ROMANS I-IV

Kerberos is the cornerstone of Windows domain authentication, but NTLM is still used to accomplish everyday tasks. These tasks include checking email, sharing files, browsing websites and are all accomplished through the use of a password hash. Skip and Chris will utilize several tools that have been ÒenhancedÓ to connect to Exchange, MSSQL, SharePoint and file servers using hashes instead of passwords. This demonstrates the "so what" of losing control of the domain hashes on your domain controller: all of your data can be compromised.

TARGETING INTRUSION REMEDIATION: LESSONS FROM THE FRONT LINES

Jim Aldridge

JULY 26 / 15:30 / AUGUSTUS III+IV

Successfully remediating a targeted, persistent intrusion generally requires a different approach from that applied to non-targeted threats. Regardless of the remediation actions enacted by victim organizations, experience has shown that such threats will continue to target certain organizations. In order to be successful against these types of threats, organizations must change the way they think about remediation. This presentation outlines a model to guide tactical and strategic security planning by focusing efforts on the following three goals:

- Inhibit attacker's activities.
- Enhance visibility to detect indicators of compromise.
- Enhance the security team's ability to effectively and rapidly respond to intrusions

THE CHRISTOPHER COLUMBUS RULE AND DHS

Mark Weatherford

JULY 26 / 11:45 / AUGUSTUS III+IV

"Never fail to distinguish what's new, from what's new to you." This rule applies to a lot people when they think about innovation and technology in the government. At the U.S. Department of Homeland Security, in addition to running the National Cybersecurity and Communication Integration Center (NCCIC), the US-CERT and the ICS-CERT, they work daily with companies from across the globe to share critical threat and vulnerability information. DHS also supports and provides funding for a broad range of cutting-edge cybersecurity research initiatives, from the development and implementation of DNSSEC to sponsoring the use of open source technologies and from development of new cyber forensics tools to testing technologies that protect the nation's industrial control systems and critical infrastructures. This is not your grandfather's Buick! Come hear Deputy Under Secretary for Cybersecurity Mark Weatherford talk about research and training opportunities, the growing number of cybersecurity competitions sponsored by DHS, and how they are always looking to hire a few good men and women.

THE DEFENSE RESTS: AUTOMATION AND APIS FOR IMPROVING SECURITY

David Mortman

JULY 25 / 11:45 / PALACE II

Want to get better at security? Improve your ops and improve your dev. Most of the security tools you need aren't from security vendors, they don't even need to be commercial. You need tools like chef & puppet, jenkins, logstash + elasticsearch & splunk or even hadoop to name but a few. The key is to centralize management, automate and test. Testing is especially key, like Jeremiah says "Hack Yourself First". So many vulnerabilities can be detected automatically. Let the machines do that work and find the basic XSS, CSRF and SQLi flaws, not to mention buffer overflows, Save the manual effort for the more complex versions of the above attacks and for business logic flaws. This is one of those spaces that dedicated security tools are a must. Leverage APIs (and protect API endpoints), be evidence driven. Counter intuitively, deploy more often, with smaller change sets. Prepare for fail and fail fast but recover faster. Not just theory, will include real examples with real code including open protocols like netconf and open source software like dasein-cloud. There will be no discussion of APT, DevOps vs NoOps, BYOD or Cloud Security concerns, there will however be baked goods.

THE INFO LEAK ERA ON SOFTWARE EXPLOITATION

Fermin J. Serna

JULY 25 / 14:15 / PALACE III

Previously, and mainly due to application compatibility. ASLR has not been as effective as it has been expected. Nowadays, once some of the problems to fully deploy ASLR has been solved, it has become the key mitigation preventing reliable exploitation of software vulnerabilities. Defeating ASLR is a hot topic in the exploitation world.

During this talk, it will be presented why other mitigations without ASLR are not strong ones and why if you defeat ASLR you mainly defeat the rest of them. Methods to defeat ASLR had been fixed lately and the current way for this is using information leak vulnerabilities.

During this talk it will be presented several techniques that could be applied to convert vulnerabilities into information leaks:

- Creating an info leak from a partial stack overflow
- Creating an info leak from a heap overflow with heap massaging
- Creating an info leak from an object though non virtual calls
- Member variables with function pointers
- Write4 pointers
- Freeing the wrong object
- Application specific info leaks: CVE-2012-0769, the case of the perfect info leak
- Converting an info leak into an UXSS

THE MYTH OF TWELVE MORE BYTES: SECURITY ON THE POST-SCARCITY INTERNET

Alex Stamos
Tom Ritter

JULY 25 / 17:00 / AUGUSTUS III-IV

In what may be the greatest technical shift the Internet has seen, three of the network's major foundations are being overhauled simultaneously: IPv6, DNSSEC and the creation of hundreds of new top-level domains. Two of these technologies are direct responses to the artificial scarcity of names and addresses on the Internet, and one is meant to address the lack of trust we have in the Internet's fundamental architecture. Unfortunately the unexpected secondary effects of these changes have not been appropriately explored, and enterprise IT and risk teams need to come to grips with the fact that the products and processes they have honed over the last decade will not serve them well in the next.

This talk will provide a quick background of these technologies and the direct security impacts faced by network administrators today, even if you're "not using that yet". (Hint: You probably are, you just don't know it.) A great deal of modern fraud, spam and brand abuse infrastructure is based upon assumptions from the IPv4/old gTLD world, and we will explore which of these protections are completely useless and which can be retrofitted to provide some value. We will then explore the indirect impacts on monitoring, compliance, intrusion detection and prevention, and the future of enterprise architecture and defense.

TORTURING OPENSSL

Valeria Bertacco

JULY 25 / 14:15 / ROMANS I-IV

For any computing system to be secure, both hardware and software have to be trusted. If the hardware layer in a secure system is compromised, not only it is possible to extract secret information about the software, but it is also extremely difficult for the software to detect that an attack is underway.

This talk will detail a complete end-to-end security attack to on a microprocessor system and will demonstrate how hardware vulnerabilities can be exploited to target systems that are software-secure. Specifically, we present a side-channel attack to the RSA signature algorithm by leveraging transient hardware faults at the server. Faults may be induced via voltage-supply variation, temperature variation, injection of single-event faults, etc. When affected by faults, the server produces erroneous RSA signatures, which it returns to the client. Once a sufficient number of erroneously signed messages is collected at the client end, we filter those that can leak private key information and we use them to extract the private key. We developed an algorithm to extract the private RSA key from messages affected by single-bit faults in the multiplication during Fixed Window Exponentiation (FWE), that is, the standard exponentiation algorithm used in OpenSSL during RSA signing. Our algorithm was inspired by a solution developed by Boneh, et al. for the Chinese Remainder Theorem (CRT) [D. Boneh, R. DeMillo, and R. Lipton. On the importance of eliminating errors in cryptographic computations. Journal of Cryptology, Dec 2001], an algorithm particularly prone to attacks. Depending of the window size used in the encryption algorithm, it is possible to extract 4-6 bits of the private key from an erroneously signed message.

Our attack is perpetrated using a FPGA platform implementing a SPARC-based microprocessor running unmodified Linux and the OpenSSL authentication library. The server provides 1024-bits RSA authentication to a client we control via Ethernet connection. Faults are injected by inducing variations in the supply voltage on the FPGA platform or by subjecting the server to high temperatures. Our client collects a few thousands signed messages, which we transfer to an 80-machines computing pool to compute the private RSA key in less than 100 hours.

Note that our attack does not require access to the victim system's internal components, but simply proximity to it. Moreover, it is conceivable that an attack leveraging solely high temperatures can be carried out on machines in a remote poorly-conditioned server room. Finally, the attack does not leave any trail of the attack in the victim machine, and thus it cannot be detected.

The presentation includes a live demo of the attack on an FPGA platform implementing a SPARC system. The system is powered via a voltage controller, used to induce variations in the supply voltage. The server is simplified to use a 128-bits private key so that the attack can be perpetrated during the briefing.

TRUST, SECURITY AND SOCIETY

Bruce Schneier

JULY 26 / 10:15 / AUGUSTUS III+IV

Human societies run on trust. Every day, we all trust millions of people, organizations, and systems—and we do it so easily that we barely notice. But in any system of trust, there is an alternative, parasitic, strategy that involves abusing that trust. Making sure those defectors don't destroy the very cooperative systems they're abusing is an age-old problem, and we've developed a variety of societal pressures to induce cooperation: moral systems, reputational systems, institutional systems, and security systems. Understanding how these different societal pressures work—and fail—is essential to understanding the problems we face in today's increasingly technological and interconnected world.

WE HAVE YOU BY THE GADGETS

Mickey Shkatov
Toby Kohlenberg

JULY 26 / 11:45 / PALACE II

Why send someone an executable when you can just send them a sidebar gadget?

We will be talking about the windows gadget platform and what the nastiness that can be done with it, how are gadgets made, how are they distributed and more importantly their weaknesses. Gadgets are comprised of JS, CSS and HTML and are application that the Windows operating system has embedded by default. As a result there are a number of interesting attack vectors that are interesting to explore and take advantage of.

We will be talking about our research into creating malicious gadgets, misappropriating legitimate gadgets and the sorts of flaws we have found in published gadgets.

WEB TRACKING FOR YOU

Gregory Fleischer

JULY 25 / 15:30 / ROMANS I-IV

There has been a lot of conversation recently around the privacy degrading techniques used by shady online advertisers, faceless megacorps, and social network overlords to track users across the web. But, after all the recriminations and fancy infographics about the supposed loss of privacy, where does that leave people who need to implement tracking of website visitors? People seem so distracted with "punch the monkey" advertising cookies that they have lost a sense of the need to legitimately track and identify potential bad actors.

This talk is a technical examination of the tracking techniques that can be implemented to identify and track users via their web browsers. The key concepts of active and passive fingerprinting, tracking, and user unmasking are discussed in detail. From the humble browser cookie to more advanced techniques to sidestep private browsing modes, the most effective approaches are discussed in relation to the various web browsers across operating systems and desktop and mobile environments.

At the conclusion of the presentation, an open source tracking server will be released that implements the techniques covered in the talk. Additionally, several utilities to facilitate injection of tracking content and correlation of collected data will also be made available. These tools will be suitable to deploy on your network to track web users or on your local machine in a standalone "Track Yourself" mode.

WINDOWS PHONE 7 INTERNALS AND EXPLOITABILITY

Tsukasa Oi

JULY 26 / 15:30 / PALACE II

Windows Phone 7 is a modern mobile operating system developed by Microsoft. This operating system—based on Windows CE 6—protects the system and the user by modern sandbox and secure application model. These security models are veiled and were difficult to uncover but we succeeded to analyze and inspect not well-known Windows Phone 7 security internals by comprehensive reverse engineering.

This operating system is properly implemented which makes exploitation and privilege escalation extremely difficult. However, it does not mean exploitation is impossible. Even the sandbox can be breached on some latest Windows Phone 7.5 devices.

The first topic is Windows Phone 7 security

analysis. In this presentation, I will talk how we analyzed the system and how Windows Phone 7 looks secure/unsecure along with examples.

The second topic is customizations by thirt-party vendors. Windows Phone 7-based devices by some vendors have special interfaces for system applications. Some interfaces however makes subverting sandbox easier because of various design/implementation issues such as directory traversal and improper privileged operations. I will talk about this kind of vulnerability along with its countermeasure.

WINDOWS 8 HEAP INTERNALS

Chris Valasek
Tarjei Mandt

JULY 25 / 15:30 / AUGUSTUS V-VI

Windows 8 developer preview was released in September 2011. While many focused on the Metro UI of the operating system, we decided to investigate the memory manager. Although generic heap exploitation has been dead for quite some time, intricate knowledge of both the application and underlying operating system's memory manager have continued to prove that reliable heap exploitation is still achievable. This presentation will focus on the transition of heap exploitation mitigations from Windows 7 to Windows 8 (Consumer Preview) from both a user-land and kernel-land perspective. We will be examining the inner workings of the Windows memory manager for allocations, de-allocations and all additional heap-related security features implemented in Windows 8. Also, additional tips and tricks will be covered providing the attendees the proper knowledge to achieve the highest possible levels of heap determinism.

WORKSHOPS

<GHZ OR BUST: BLACK HAT

Atlas

JULY 25 / 10:15 / FLORENTINE

Wifi is cool and so is cellular, but the real fun stuff happens below the GHz line. medical systems, mfg plant/industrial systems, cell phones, power systems, it's all in there!

Atlas and some friends set out to turn pink girltech toys into power-systems-attack tools. through through several turns and changes, the cc1111usb project was born, specifically to make attacking these systems easier for all of you. with a $50 usb dongle, the world of ISM sub-GHz is literally at your fingertips.

New and improved! if you missed it at shmoocon, here's your chance to see the intro to this fun new world. if you caught it at shmoo, come to the talk and prove your <ghz prowess and wirelessly hack a special pink girl's toy target!

ADVANCED CHROME EXTENSION EXPLOITATION-LEVERAGING API POWERS FOR THE BETTER EVIL

Kyle Osborn
Krzysztof Kotowicz

JULY 25 / 10:15 / POMPEIAN

Browser exploitation can seem to be a nearly unachievable task these days. ASLR, DEP, segregated processes and sandboxes have proven to be effective in abating exploits by attackers. Our expectation of browser security is so high, that in addition to bug bounty programs, competitions such as Pwn2Own and Pwnium have been formed around the core concept of weeding out dangerous bugs.

But even with all the current protections, there is still attack surface not being exploited. We are, of course, talking about Chrome Extensions security bugs. These bugs can lead to extremely powerful attacks, which can effectively allow an attacker to take over your browser. In our workshop, we will demonstrate the power given to an attacker in a presence of a vulnerable extension, and present a tool which will assist in their practical exploitation.

CODE REVIEWING WEB APPLICATION FRAMEWORK BASED APPLICATIONS (STRUTS 2, SPRING MVC, RUBY ON RAILS,(GROOVY ON GRAILS), .NET MVC)

Abraham Kang

JULY 25 / 14:15 / FLORENTINE

This workshop will give participants an opportunity to practically review Web Application Framework based applications for security vulnerabilities. The material in this workshop provides the hands-on experience that one would need to quickly understand each web application framework (Struts 2, Spring MVC, Ruby on Rails (Groovy on Grails), .NET MVC, Zend PHP, and Scala Play) and identify vulnerabilities in applications using those frameworks. Sample applications are provided with guided tasks to ease participants into understanding the nuances of each framework and the overall steps a code reviewer should follow to identify vulnerabilities.

LESSONS OF BINARY ANALYSIS

Christien Rioux

JULY 26 / 10:15 / FLORENTINE

Ever wanted to know more about how static binary analysis works? It's complicated. Ever want to know how C++ language elements are automatically transformed? The high-level overview of how machines analyze code for security flaws is just the beginning. In this talk we'll be delving into the gritty details of the modeling process.

LINUX INTERACTIVE EXPLOIT DEVELOPMENT WITH GDB AND PEDA

Long Le

JULY 25 / 14:15 / POMPEIAN

Exploit development requires a lot of interactive works with debugger, automating time consuming tasks will help speed up that process. People is familiar with GDB (GNU Debugger) on Linux/Unix, unfortunately GDB lacks of commands specific to exploit development. Since version 7.0, GDB added support for Python scripting, this brings opportunities to improve the situation. PEDA—Python Exploit Development Assistance for GDB—is a wrapper for Python GDB that comes as a gdbinit script with many handy commands to ease exploit development tasks. PEDA is the first script in its class with notable features:

Debugging helpers: smart context display with detail memory references; function calls tracing with detail arguments; specific instructions tracing; stepping until specific instruction; bypass/deactive undesired functions (e.g ptrace); execution statistics with profiling; process snapshoting.

Advanced memory operations: fast, convenient memory searching for regex/value/reference/address/pointer; display, dump, load, compare, XOR memory content.

Exploit helpers: cyclic pattern create and search; ELF headers and symbols retrieval; simple ASM instructions and ROP gadgets search; common shellcodes and ROP payloads generation (ret2plt data transfer, ret2dlresolve); exploit skeleton generation; in memory fuzzer; crashdump logging.

PEDA's commands and wrapper API can also be reused to write custom automation scripts easily, hence makes GDB become a powerful exploit development toolkit.

During this hands-on workshop, attendees will learn how to use PEDA interactive commands, write python automation scripts through various exploit exercises, wargame/CTF challenges and real world exploits.

Binging your laptop with an Ubuntu Live to play with and get a special copy of PEDA.

MOBILE NETWORK FORENSICS

Eric Fulton

JULY 26 / 15:30 / FLORENTINE

Intentionally or not, your phone leaks data to the world. What can you—or your enemies—uncover from mobile network traffic? Dig through real-life Android packet captures to uncover GPS coordinates, usernames and accounts, social networking data, and more. Dissect a traffic dump of Android malware and analyze phone data as it is exfiltrated to third-party servers. The second half of this workshop is a mobile network forensics contest. Each attendee will be given a mysterious USB drive and a note with a challenge. Students must use the skills they've gained in class to unravel the mystery. You are the forensics investigator. Can you solve the puzzle in time?

To participate, workshop attendees must bring a laptop with at least 2GB of RAM, a DVD drive. and VMWare Workstation or Player preinstalled and licensed (evaluation licenses are available from VMWare's web site).

RUBY FOR PENTESTERS: THE WORKSHOP

Cory Scott
Michael Tracy
Timur Duehr

JULY 26 / 14:15 / POMPEIAN

Having a great set of test tools could be the difference between a successful engagement and utter catastrophe. Being able to create tools on the fly to solve intractable test or research problems is a challenge we face every day.

In this workshop we'll lead off by demonstrating the power and flexibility of Ruby. Then we'll teach you how to use your new superpowers to rapidly prototype solutions for real-world problems including:

- The fast path to binary and protocol reversing tools
- Rapidly prototyped network clients using our 'bag of tricks' approach
- Dealing with Java using JRuby
- Extending Burp Suite using Buby
- Building scriptable debuggers and hit tracers with Ragweed
- Hooking into native code with FFI
- Adding Redis in the mix to manage test cases and results from within your Ruby code

Participants will be given a virtual test environment to use that includes a toolchain and sample applications to test—they just need to bring a laptop. The toolchain will also be available on the conference DVD and for download.

Quick demonstrations leading into hands-on hacking on real apps will keep the workshop fast-paced and fun.

THE DARK ART OF IOS APPLICATION HACKING

Jonathan Zdziarski

JULY 26 / 10:15 / POMPEIAN

This talk demonstrates how modern day financial applications, password and credit card managers, and other applications handling sensitive data are attacked on the iOS platform, and sometimes all too easily breached in as little as seconds. Attendees will learn how iOS applications are infected, how low-level classes and objects are manipulated and abused, logic checks bypassed, and other dark techniques used to steal data.

The electronic information age has made the theft of data a very lucrative occupation. Criminals stand to greatly benefit from electronic crimes, making their investment well worth the risk. The chances that your applications will be vulnerable to attack are very high. Due to a number of common vulnerabilities in the iOS monoculture, attackers can easily reverse engineer, trace, and manipulation applications in ways that even most iOS developers aren't aware of. Even many encryption implementations are weak, and a good hacker can penetrate these and other layers that, so many times, present only a false sense of security to the application's developers.

This talk is designed to demonstrate many of the techniques black hats use to steal data and manipulate software, so that developers will better know the fight they're up against, and hopefully how to avoid many all-too common mistakes that leave your applications exposed to easy attacks. These attacks are not necessarily limited to just the theft of data from the device, but can sometimes even lead to much more nefarious attacks. The audience will also learn about some techniques to better secure applications, such as counter debugging techniques, attack response, implementing better encryption, etc.

In this talk, the audience will see an example of how some credit card payment processing applications have been breached, allowing a criminal not only to expose the credit card data stored on the device, but also to manipulate the application to grant him huge credit card refunds for purchases that he didn't make, paid straight from the merchant's stolen account. You'll see many more examples, too, of exploits that put data at risk, such as password and credit card managers, and other applications. Attendees will gain a basic understanding of how these attacks are executed, and many examples and demonstrations of how to code more securely in ways that won't leave applications exposed to such attacks.

TURBO TALKS

CUTECATS.EXE AND THE ARAB SPRING

Morgan Marquis-Boire

JULY 25 / 14:15 / AUGUSTUS III-IV

There has been significant discussion regarding the impact of the internet, social media, and smart phones on the uprisings in the Middle East. Accompanying the digitisation of dissent and the growth of an increasingly connected online community has been the rise in malware targeting activists in the region.

From backdoored anti-censorship software to malicious PDFs promising details on revolutionary high councils, this talk will detail specific examples and provide analysis of malware which has been seen to target dissidents in Libya, Syria and other countries over the past 18 months. The distribution of these attacks across forums specialising in regional issues, social media and spear phishing will also be discussed.

EMBEDDED DEVICE FIRMWARE VULNERABILITY HUNTING USING FRAK

Ang Cui

JULY 26 / 14:35 / PALACE III

We present FRAK**, the firmware reverse analysis konsole. FRAK is a framework for unpacking, analyzing, modifying and repacking the firmware images of proprietary embedded devices. The FRAK framework provides a programmatic environment for the analysis of arbitrary embedded device firmware as well as an interactive environment for the disassembly, manipulation and re-assembly of such binary images. We demonstrate the automated analysis of Cisco IOS, Cisco IP phone and HP LaserJet printer firmware images. We show how FRAK can integrate with existing vulnerability analysis tools to automate bug hunting for embedded devices. We also demonstrate how FRAK can be used to inject experimental host-based defenses into proprietary devices like Cisco routers and HP printers.

HTEXPLOIT BYPASSING HTACCESS RESTRICTIONS

Maximiliano Soler
Matias Katz

JULY 25 / 14:35 / AUGUSTUS I-II

HTExploit is an open-source tool written in Python that exploits a weakness in the way that htaccess files can be configured to protect a web directory with an authentication process. By using this tool anyone would be able to list the contents of a directory protected this way, bypassing the authentication process.

LIBINJECTION: A C LIBRARY FOR SQLI DETECTION AND GENERATION THROUGH LEXICAL ANALYSIS OF REAL WORLD ATTACKS

Nick Galbreath

JULY 25 / 14:55 / AUGUSTUS I-II

SQLi and other injection attacks remain the top OWASP and CERT vulnerability. Current detection attempts frequently involve a myriad of regular expressions which are not only brittle and error prone but also proven by Hanson and Patterson at Black Hat 2005 to never be a complete solution. libinjection is a new open source C library that detects SQLi using lexical analysis. With little upfront knowledge of what SQLi is, the algorithm has been trained on tens of thousands of real SQLi attacks and hundreds of millions of user inputs taken from a Top 50 website for high precision and accuracy. In addition, the algorithm categorizes SQLi attacks and provides templates for new attacks or new fuzzing algorithms. libinjection is available now on github for integration into applications, web application firewalls, or porting to other programming languages.

MAPPING EVOLUTION OF ANDROID PERMISSIONS

Andrew Reiter
Zach Lanier

JULY 26 / 14:55 / PALACE III

The Android Open Source Project provides a software stack for mobile devices. The provided API enforces restrictions on specific operations a process is allowed to perform through a permissions mechanism. Due to the fine-grained nature of the model (and lack of a map), it is non-obvious which calls require which permission(s) for an API of over 2400 classes. Also, due to the on-going development of the AOSP and API, these required permissions have changed. Both of these provide headaches for application security testers and application developers. We first discuss our methodology for building a Android API permission map, including active and passive discovery tools. We then present the evolution of the map as the Android API has transformed through releases. This work is significant because of the need for an understanding of the API permission requirements in application security testing and the current lack of clarity in this ever-growing environment.

MODSECURITY AS UNIVERSAL CROSS-PLATFORM WEB PROTECTION TOOL

Greg Wroblewski
Ryan Barnett

JULY 25 / 14:15 / AUGUSTUS I-II

For many years ModSecurity was a number one free open source web application firewall for the Apache web server. At this year's Black Hat we would like to announce that right now ModSecurity is also available for IIS and nginx servers, making it a first free cross-platform WAF for on-line services. Using MSRC response process and CVE-2011-3414 as an example, we will show how ModSecurity can be used in early detection of attacks and mitigation of vulnerabilities affecting web infrastructure. We will also show how OWASP ModSecurity Core Rule Set can be used as a base for detection of 0-day attacks on Apache, IIS and nginx servers.

PASSIVE BLUETOOH MONITORING IN SCAPY

Ryan Holeman

JULY 26 / 14:15 / PALACE I

Recognizing a need to support passive bluetooth monitoring in Scapy, Python's interactive monitoring framework, a project was launched to produce this functionality. Through this functionality, a new means for interactively observing bluetooth was created along with Python APIs to assist in the development of bluetooth auditing, pentesting and exploitation tools.

The project supplements the work of Michael Ossman et al by providing Python extensions and Scapy modules which interact with an Ubertooth dongle. The project also provides support for other passive bluetooth techniques not present in the current Ubertooth core software such as NAP identification, vendor lookup, extended logging and more.

In conjunction with this presentation, the source for this project will be released along with distribution packages for easy installation.

STAMP OUT HASH CORRUPTION, CRACK ALL THE THINGS

Ryan Reynolds
Jonathan Clauduis

JULY 26 / 14:55 / PALACE I

The precursor to cracking any password is getting the right hash. In this talk we are going to cover how we discovered that Cain and Able, Creddump, Metasploit and other hash extraction tools regularly yield corrupt hashes that cannot be cracked. We will take a deep dive into password extraction mechanics, the birth of a viral logic flaw that started it all and how to prevent corrupt hashes. At the conclusion of this talk we will release patches that prevent hash corruption in these tools that many security professionals use every day.

STIX: THE STRUCTURED THREAT INFORMATION EXPRESSION

Sean Barnum

JULY 25 / 14:55 / AUGUSTUS III-IV

This Turbo Talk will give a brief introduction and overview of an ongoing effort to define a standardized integrated information architecture for representing structured cyber threat information.

The effort known as the Structured Threat Information eXpression (STIX) is a work in progress among a broad community of industry, government, academic and international experts. This representation, as a whole or in parts, is actively being

pursued as a basis for automation and information sharing within several active communities.

SYNFUL DECEIT, STATEFUL SUBTERFUGE

Tom Steele
Chris Patten

JULY 26 / 14:35 / PALACE I

Successful network reconnaissance and attacks are almost always predicated by effectively identify listening application services. However, the task can be daunting with various deployments of SYN Flood protections that can mask legitimate results. Furthermore, misconceptions are plenty and suggestions are elusive regarding how to truly detect the actual available services from the false positives. This presentation will delve into techniques used for SYN Flood protection and how to defeat various open-source and commercial vendor implementations.

The presentation will consist of IPv4 packet level details. As a result, a solid understanding of TCP/IP and the IPv4 connection process is highly advised prior to attending this presentation. Further understanding of typical port scanning techniques, such as SYN and ACK scans, will be useful, as well. Finally, a tool will be released so attendees can continue to explore the concepts and techniques within their own networks.

THE LAST GASP OF THE INDUSTRIAL AIR-GAP

Eireann Leverett

JULY 25 / 14:35 / AUGUSTUS III-IV

Industrial Systems are widely believed to be air-gapped. At previous Black Hat conferences, people have demonstrated individual utilities control systems directly connected to the internet. However, this is not an isolated incident of failure, but rather a disturbing trend. By visualising results from SHODAN over a 2 1/2 year period, we can see that there are thousands of exposed systems around the world. By using some goelocation, and vulnerability pattern matching to service banners we can see their rough physical location and the numbers of standard vulnerabilities they are exposed to.

This allows us to look at some statistics about the industrial system security posture of whole nations and regions. During the process of this project I worked with ICS-CERT to inform asset-owners of their exposure and other CERT teams around the world. The project has reached out to 63 countries, and sparked discussion of convergence towards the public internet of many insecure protocols and devices.

WHEN SECURITY GETS IN THE WAY: PENTESTING MOBILE APPS THAT USE CERTIFICATE PINNING

Alban Diquet
Justine Osborne

JULY 26 / 14:15 / PALACE III

More and more mobile applications such as the Chrome, Twitter and card.io apps have started relying on SSL certificate pinning to further improve the security of the application's network communications. Certificate pinning allows the application to authenticate the application's servers without relying on the device trust store. Instead, a white-list of certificates known to be used by the servers is directly stored in the application, effectively restricting the set of certificates the application will accept when connecting to those servers.

While improving the security of end users, not using the device trust store to validate the servers' identity also makes black-box testing of such apps much more challenging. Without access to the application's source code to manually disable certificate validation, the tester is left with no simple options to intercept the application's SSL traffic.

We've been working on a set of tools for both Android and iOS to make it easy to defeat certificate pinning when performing black-box testing of mobile apps.

On iOS, a Mobile Subtrate "tweak" has been developed in order to hook at run-time specific SSL functions performing certificate validation. Using Cydia, the "tweak" can easily be deployed on a jailbroken device, allowing the tester to disable certificate validation for any app running on that device in a matter of minutes.

For Android applications, a custom JDWP debugger has been built to perform API hooking tasks. This tool can be easily used on any Android device or emulator that allows USB debugging and application debugging.

This presentation will discuss the techniques we used to create those iOS and Android API hooking tools, common use case scenarios, and demonstrations of the tools in action.

EVENT AUDIO & VIDEO

THE SOURCE OF KNOWLEDGE

Palace Ballroom Foyer

JULY 25-26

Did you miss a session? The Source of Knowledge is onsite to sell audio and video recordings of the Briefings sessions. Media, including iPad ready presentations, may be purchased onsite at a substantial discount.

KEYNOTES

SHAWN HENRY *CrowdStrike*

Shawn retired as FBI Executive Assistant Director (EAD) in March 2012, with responsibility for all criminal and cyber programs and investigations worldwide, as well as international operations and the FBI's critical incident response. During his career as a Special Agent, Shawn served in three FBI Field Offices and at FBI Headquarters, where he held a wide range of operational and leadership positions, including Assistant Director in Charge of the Washington Field Office.

Having served in multiple positions relating to cyber intrusions since 1999, Shawn has been the Bureau's outspoken top agent on cybersecurity issues, and is credited with boosting the FBI's computer crime and cybersecurity investigative capabilities. In addition to his last position as EAD of the Criminal, Cyber, Response and Services Branch, he served as both Deputy Assistant Director and Assistant Director of the Cyber Division at FBI Headquarters; Supervisor of the FBI Cyber Crime squad in Baltimore; and Chief of the Computer Investigations Unit within the FBI-led National Infrastructure Protection Center.

During his tenure, Shawn oversaw major computer crime and cyber investigations spanning the globe, from denial-of-service attacks, to major bank and corporate breaches, to nation-state sponsored intrusions. Shawn led the establishment of the National Cyber Investigative Joint Task Force (NCIJTF), a multi-agency center led by the FBI, which coordinates and shares information about cyber threat investigations. He also forged partnerships domestically and internationally within governments and the private sector, and posted FBI cyber experts in police agencies around the world, including Amsterdam, Romania, Ukraine, and Estonia. Early in his cyber career, Shawn served on the U.S. delegation to the G8 as a member of the High-Tech Crimes Subgroup.

Shawn was an original member of the National Cyber Study Group, under the direction of the Office of the Director of National Intelligence. This organization developed the Comprehensive National Cybersecurity Initiative (CNCI), the U.S. government's national strategy to mitigate threats and secure cyberspace, to which Shawn was a key contributor.

Shawn has been a keynote speaker on a multitude of cyber issues in venues around the world. He has been sought out by the media for his cyber expertise, and has been featured on television and radio, including 60 Minutes; CBS Evening News; Good Morning America; The Today Show; Dateline; Rock Center with Brian Williams and C-SPAN. He has also conducted interviews with numerous print and online publications, including Forbes Magazine, Business Week, The Wall Street Journal, The Associated Press, The New York Times, and USA Today.

Shawn has been professionally recognized during his career. In 2009, he received the Presidential Rank Award for Meritorious Executive for his leadership in enhancing the FBI's cyber capabilities, and was recognized by SC Magazine as one of the top industry pioneers who shaped the information security industry. In 2010, he was named one of the most influential people in security by Security Magazine; received the Federal 100 Award as a government leader who played a pivotal role in the federal government IT community; and was selected as cybercrime fighter of the year by McAfee Inc.

Shawn earned a Bachelor of Business Administration from Hofstra University and a Master of Science in Criminal Justice Administration from Virginia Commonwealth University. He is a graduate of the Homeland Security Executive Leaders Program of the Naval Postgraduate School's Center for Homeland Defense and Security. As President of CrowdStrike Services, Shawn leads a world-class team of cybersecurity professionals who respond to computer network intrusions to mitigate Advanced Persistent Threats (APT).

NEAL STEPHENSON

Neal Stephenson is the author of the three-volume historical epic "The Baroque Cycle" (Quicksilver, The Confusion, and The System of the World) and the novels Cryptonomicon,The Diamond Age, Snow Crash, and Zodiac. He lives in Seattle, Washington.

BRIEFINGS

JIM ALDRIDGE *Mandiant*

Jim Aldridge is a Manager in Mandiant's Washington, D.C. office and is responsible for Mandiant's incident remediation services. His areas of expertise include security incident response, penetration testing, security strategy, and secure systems and network design. Jim has significant experience working with the defense industrial base, technology, and industrial products sectors.

CHEMA ALONSO *Informatica64*

Chema Alonso is a Security Consultant with Informatica64, a Madrid-based security firm. Chema holds respective Computer Science and System Engineering degrees from Rey Juan Carlos University and Universidad Politacnica de Madrid. During his more than six years as a security professional, he has consistently been recognized as a Microsoft Most Valuable Professional (MVP). Chema is a frequent speaker at industry events (Microsoft Technet / Security Tour, AseguraIT) and has been invited to present at information security conferences worldwide including Black Hat Briefings, DEF CON, Ekoparty and RootedCon. He is a frequent contributor on several technical magazines in Spain, where he is involved with state-of-the-art attack and defense mechanisms, web security, general ethical hacking techniques and FOCA, the meta-data extraction tool which he co-authors.

YANN ALLAIN *Opale Security*

Yann ALLAIN, founder and current director of the OPALE SECURITY company (www.opale-security.eu). He graduated from a computer and electronic engineering school (Polytech -UniversitŽ Pierre et Marie Curie). After a time in the electronic industry as an engineer in embedded system conception, he made a career move towards IT. He started as a production manager for a company in the financial sector (Private Banking), and evolved towards IT security when he became part of the ACCOR group. He was in charge of applicative security for the group. He has an 18-year experience, 14 of which dedicated to IT system and embedded system security. OPALE SECURITY deals with research projects linked, amongst other things to the security of embedded systems (*http://www.opale-security.eu/innovation-information-systems-security.html*)

IFTACH IAN AMIT *IOActive*

With over a decade of experience in the information security industry, Iftach Ian Amit brings a mixture of software development, OS, network and Web security expertise as Director of Services to the top-tier security consulting firm IOActive. Prior to IOActive, Ian was the VP consulting for Security Art, Ian also held Director of Security Research positions with Aladdin and Finjan, leading their security research while positioning them as leaders in the Web security market. Ian has also held leadership roles as founder and CTO of a security startup in the IDS/IPS arena, developing new techniques for attack interception, and a director at Datavantage, responsible for software development and information security, as well as designing and building a financial datacenter. Prior to Datavantage, he managed the Internet Applications as well as the UNIX departments at the security consulting firm Comsec.

Ian is also the founder of the local DEF CON group in Tel-Aviv DC9723, as well as one of the founding members of the PTES (Penetration Testing Execution Standard), and the IL-CERT.

GEORGE ARGYROS

University Of Athens / Census, Inc.

George Argyros is an undergraduate student at University Of Athens in Greece but he is about to start a Ph.D. at Columbia University in September. He also works as an intern at Census inc. His research interests include cryptography, software testing, source code auditing and anything else related to computer security seems interesting.

PATROKLOS ARGYROUDIS *Census Inc*

Patroklos Argyroudis is a computer security researcher at Census Inc, a company that builds on strong research foundations to offer specialized IT security services to customers worldwide. Patroklos holds a PhD in Computer Security from the University of Dublin, Trinity College, where he has also worked as a postdoctoral researcher on applied cryptography. His current focus is on vulnerability research, exploit development, reverse engineering, source

code auditing and malware analysis. Patroklos has presented research at several international security conferences on topics such as kernel exploitation, kernel mitigation technologies, and electronic payments.

VALERIA BERTACCO

University of Michigan

Valeria Bertacco is an Associate Professor of Electrical Engineering and Computer Science at the University of Michigan. She is currently spending her sabbatical at the Addis Ababa Institute of Technology. Her research interests are in the area of design correctness, with emphasis on full design validation, digital system reliability and hardware security assurance. Valeria joined the faculty at Michigan after being in the Advanced Technology Group of Synopsys for four years as a lead developer of Vera and Magellan, two popular verification tools.

Valeria serves in several conference program committees, including DATE and DAC and she the author of three books on design errors and validation. She received her M.S. and Ph.D. degrees in Electrical Engineering from Stanford University in 1998 and 2003, respectively; and a Computer Engineering degree ("Dottore in Ingegneria") summa cum laude from the University of Padova, Italy in 1995. Valeria is the recipient of the IEEE CEDA Early Career Award, an IBM faculty award, an NSF CAREER award, and the Air Force Office of Scientific Research's Young Investigator award.

RODRIGO BRANCO ***Qualys***

Rodrigo Rubira Branco (BSDaemon) is the Director of Vulnerability & Malware Research at Qualys. In 2011 he was honored as one of the top contributors to Adobe Vulnerabilities in the past 12 months. Previously, as the Chief Security Research at Check Point he founded the Vulnerability Discovery Team (VDT) and released dozens of vulnerabilities in many important software. Previous to that, he worked as Senior Vulnerability Researcher in COSEINC, as Principal Security Researcher at Scanit and as Staff Software Engineer in the IBM Advanced Linux Response Team (ALRT) also working in the IBM Toolchain (Debugging) Team for PowerPC Architecture. He is a member of the RISE Security Group and is the organizer of Hackers to Hackers Conference (H2HC), the oldest security research conference in Latin America.

JOSHUA BRASHARS ***AppSec Consulting***

Joshua Brashars is a senior penetration tester at AppSec Consulting. He specializes in network, application, and the mobile security testing. In his spare time, he enjoys playing around with old telephone systems. Joshua has presented at several industry-recognized conferences and has contributed to several books by Syngress Publishing.

CODY BROCIOUS ***Mozilla***

Cody Brocious is a hacker for the Mozilla Corporation with over 8 years of experience as a computer security researcher, reverse engineer, and developer. Prior to this, he worked for Matasano Security as a senior security consultant. His reverse engineering and hardware analysis work, written about in Forbes and Ars Technica, includes early key research in hardware jailbreaking (including an ARM decompiler), reversing projects that led to the first Linux compatibility for the Apple iTunes Music Store, and Linux compatibility for Windows games.

JONATHAN BROSSARD

Toucan System Security Company

Jonathan is a security research engineer. Born in France, he's been living in Brazil and India, before currently working in Australia. With about 15 years of practice of assembly, he is specialised in low level security, from raw sockets to cryptography and memory corruption bugs. He is currently working as CEO and security consultant at the Toucan System security company. His clients count some of the biggest Defense and Financial Institutions worldwide. Jonathan is also the co-organiser of the Hackito Ergo Sum conference (HES2011) in France.

CHRISTOPHER CAMPBELL

Northrop Grumman

Works for Northrop Grumman as a full-scope penetration tester for several years. He holds many industry certifications and a Master of Science in IA from Capitol College. Chris served over ten years in the Army with most of that time as a Signal Officer.

LUCA CARETTONI

Matasano Security

Luca Carettoni is a senior security consultant for Matasano Security with over 7 years experience as a computer security researcher. His professional expertise includes black box security testing, web application security, vulnerability research and source code analysis. Prior to Matasano, Luca worked at The Royal Bank of Scotland as a penetration testing specialist where he performed security audits against several online banking systems worldwide. In the past years, Luca has been an active participant in the security community and a member of the Open Web Application Security Project (OWASP). Luca holds a Master's Degree in Computer Engineering from the Politecnico di Milano university.

CESAR CERRUDO ***IOActive Labs***

Cesar Cerrudo is CTO at IOActive Labs where he leads the team in producing ongoing cutting edge research in the areas of SCADA, mobile device, application security and more. Formerly the founder and CEO of Argeniss Consulting, acquired by IOActive, Cesar is a world renown security researcher and specialist in application security.

Throughout his career, Cesar is credited with discovering and helping to eliminate dozens of vulnerabilities in leading applications including Microsoft SQL Server, Oracle database server, IBM DB2, Microsoft BizTalk Server, Microsoft Commerce

Server, Microsoft Windows, Yahoo! Messenger, etc. In addition, Cesar has authored several white papers on database, application security, attacks and exploitation techniques and he has been invited to present at a variety of companies and conferences including Microsoft, Black Hat, Bellua, CanSecWest, EuSecWest, WebSec, HITB, Microsoft BlueHat, EkoParty, FRHACK, H2HC, DEF CON, Infiltrate, etc. Cesar collaborates with and is regularly quoted in print and online publications including eWeek, ComputerWorld, and other leading journals.

SILVIO CESARE ***Deakin University***

Silvio Cesare is a PhD student at Deakin University. His research is supported by a full scholarship under a Deakin University Postgraduate Research Award. His research interests include malware detection and automated vulnerability discovery using static analysis of executable binaries. He has previously spoken at industry conferences including Black Hat, Cansecwest, Ruxcon, and has published in academic journals such as IEEE Transactions on Computers. He is also author of the book Software Similarity and Classification, published by Springer. He has worked in industry within Australia, France and the United States. This work includes time as the scanner architect of Qualys – now the world's largest vulnerability assessment company. In 2008 he was awarded $5000 USD tied 3rd prize for the highest impact vulnerability reported to security intelligence company IDefense for an implementation specific IDS evasion bug in the widely deployed Snort software. He has a Bachelor of Information Technology and a Master of Informatics by research from CQUniversity where he was awarded with two academic prizes during his undergraduate degree, and a University Postgraduate Research Award full scholarship during his Masters degree.

DMITRY CHASTUHIN
St. Petersburg State Polytechnic University

The student of St. Petersburg State Polytechnic University, computer science department, he works upon SAP security, particularly upon Web applications and JAVA systems. He has official acknowledgements from SAP for the vulnerabilities found.

Dmitriy is also a WEB 2.0 and social network security geek who found several critical bugs in Yandex services (Russian largest search engine), Google, Vkontakte (vk.com), the Russian largest social network. He is a contributor to the OWASP-EAS project. He spoke at the following conferences: Hack in the Box and BruCON.

Actively participates in the life of the Russian DEF CON Group.

ROBERT CLARK
U.S. Army Cyber Command

Robert Clark is currently the operational attorney for the U.S. Army Cyber Command. He is the former Cybersecurity Information Oversight & Compliance Officer with the Office of Cybersecurity and Communications, Department of Homeland Security and former legal advisor to the Navy CIO; United States Computer Emergency Readiness Team; and, the Army's Computer Emergency Response Team. In these positions he has provided advice on all aspect of computer network operations. He interacts regularly with many government agencies and is a past lecture at Black Hat; DEF CON; Stanford Center for Internet and Society and the Berkman Center for Internet & Society at Harvard University -Four TED-TECH Talks 2011; SOURCE Boston 2010; the iapp; and, the DoD's Cybercrimes Conference.

JONATHAN CLAUDUIS ***Trustwave***

Jonathan Claudius is a Security Researcher at Trustwave. He is a member of Trustwave's SpiderLabs—the advanced security team focused on penetration testing, incident response, and application security. He has eleven years of experience in the IT industry with the last nine years specializing in Security. At Trustwave, Jonathan works in the SpiderLabs Research Division where he focuses on vulnerability research, network exploitation and is the creator of the BNAT-Suite. Before joining SpiderLabs, Jonathan ran Trustwave's Global Security Operations Center.

Before joining Trustwave, Jonathan was a Network Penetration Tester for a Top 10 Consulting and Accounting firm and worked for a US Department of Defense contractor in their Communications Electronics Warfare Division. Jonathan holds a Bachelor of Science in Applied Networking and System Administration from the Rochester Institute of Technology and is a Certified Information Systems Security Professional (CISSP).

ANDREI COSTIN ***Eurecom***

Born and grown-up in Moldova, Andrei is a Computer Science graduate of the Politechnic University of Bucharest where he did his thesis work in Biometrics and Image Processing. While starting out his IT-career in the Computer Games industry, he has worked in the Telecom field and also was a senior developer at a specialized firm programming various GSM/UMTS/GPS sub-systems. He is the author of the MiFare Classic Universal toolKit (MFCUK), the first publically available (FOSS) card-only key cracking tool for the MiFare Classic RFID card family and is known as the "printer guy" for his "Hacking MFPs" and "Hacking PostScript" series of hacks & talks at various international conferences. He is passionate about security in a holistic fashion. Currently he is a PhD candidate with EURECOM in the field of "Security of embedded devices".

ZACHARY CUTLIP
Tactical Network Solutions

Zachary Cutlip is a security researcher with Tactical Network Solutions, in Columbia, MD. At TNS, Zach develops exploitation techniques targeting embedded systems and network infrastructure. Since 2003, Zach has worked either directly for or with the National Security Agency in various capacities. Before embracing a lifestyle of ripped jeans and untucked shirts, he spent six years in the US Air Force, parting ways at the rank of Captain. Zach holds an undergraduate degree from Texas A&M University and a master's degree from Johns Hopkins University.

DALLAS DE ATLEY ***Apple***

Dallas De Atley, Manager of the Platform Security Team, Apple

TAMARA DENNING
University of Washington

Tamara Denning is a fifth year PhD student at the University of Washington working with Tadayoshi Kohno in the Security and Privacy Research Lab. She received her B.S. in Computer Science from the University of California, San Diego in 2007 and her Master's degree from the University of Washington in 2009. Her main area of focus is the intersection of humans and computer security with a focus on emerging technologies.

JOSHUA DUBICK ***FishNet Security***

Joshua Dubik is a Security Consultant for FishNet Security's Application Security practice. His focus is on the security of web, mobile and desktop applications. Previously, Joshua worked as a developer for several organizations including the United States Coast Guard. Joshua is currently working on the iOS Application Assessment Tool.

ALVA DUCKWALL ***Northrop Grumman***

Alva "Skip" Duckwall has been using Linux back before there was a 1.0 kernel and has since moved into the information security arena doing anything from computer/network auditing, to vulnerability assessments and penetration testing. Skip currently works for a group doing full-scope penetration testing. Skip currently holds the following certs:GSE, CISSP, CISA, and RHCE. Skip currently works for Northrop Grumman as a Sr. Cyber Something or other.

JUSTIN ENGLER ***FishNet Security***

Justin Engler is a Senior Security Consultant for FishNet Security's Application Security practice. His focus is on the security of web applications, mobile devices, web-backed thick clients, databases, and industrial control systems. Justin has previously spoken at Black Hat USA and DEF CON.

STEFAN ESSER ***SektionEins GmbH***

Stefan Esser is best known in the security community as the PHP security guy. Since he became a PHP core developer in 2002 he devoted a lot of time to PHP and PHP application vulnerability research. However in his early days he released lots of advisories about vulnerabilities in software like CVS, Samba, OpenBSD or Internet Explorer. In 2003 he was the first to boot Linux directly from the hard disk of an unmodified XBOX through a buffer overflow in the XBOX font loader. In 2004 he founded the Hardened-PHP Project to develop a more secure version of PHP, known as Hardened-PHP, which evolved into the Suhosin PHP Security System in 2006. Since 2007 he works as head of research and development for the German web application company SektionEins GmbH that he cofounded.

GREGORY FLEISCHER ***FishNet Security***

Gregory is a Senior Security Consultant in the Application Security practice at FishNet Security where he conducts security assessments against a wide variety of web and mobile applications. In his spare time, he likes to find and exploit vulnerabilities in web browsers and client-side technologies such as Java and Flash as well as working on open source security tools. He has an interest in privacy and anonymity and has worked with The Tor Project to identify potential issues. Gregory has previously spoken at the Black Hat USA and DEF CON security conferences.

JOHN FLYNN ***Facebook***

John "Four" Flynn is an expert in Information Security with over 10 years of experience in the field. At Google, he was the founder and lead architect of Google's innovative Intrusion Detection group which led to the successful detection of the Aurora attack in December 2009. Four also led Google's Security Operations team where he pioneered innovative approaches to Enterprise IT Security. He is a technical advisor to both a prominent political campaign and a top tier Venture Capital firm. Four holds a Masters in Computer Science and Information Assurance from George Washington University as well as a Bachelors in Computer Engineering from the University of Minnesota. Currently he works as a Security Engineer at Facebook and maintains a blog at SecInt.org.

When it comes to cybersecurity, being out of the loop is a dangerous place.

Shared Knowledge. Shared Security.

Developing and Connecting Cybersecurity Leaders Globally

Your Membership Will Provide You With:

- Peer-to-Peer Networking
- Continued Education & Training
- Career Development, Growth and Opportunities

Join ISSA Now and get a $20 Membership Discount for Black Hat Attendees.*

Stop by Black Hat Booth **TT2** to sign up and take advantage of the Black Hat Discount for General Membership or visit **www.issa.org** now and use the promo code "BlackHat".

ISSA

Information Systems Security Association

**Hurry, this offer is for new members only and expires September 30, 2012.*

JAMES FORSHAW
Context Information Security

James is a principal consultant for Context Information Security in the UK, with a keen focus on novel security research. He has been involved with computer hardware and software security for almost 10 years with a skill set which covers the bread and butter of the security industry such as application testing, through to more bespoke product assessment, vulnerability analysis and exploitation.

He has spoken at a number of security conferences in the past, on a range of different topics such as Sony Playstation Portable hacking at Chaos Computer Congress, WebGL exploitation at Ruxcon and Citrix network exploitation at Black Hat Europe. He is also the developer of CANAPE networking tool presented at that conference.

JAVIER GALBALLY
Universidad Autonoma de Madrid

Javier Galbally received the MSc in electrical engineering in 2005 from the Universidad de Cantabria, and the PhD degree in electrical engineering in 2009, from Universidad Autonoma de Madrid, Spain. Since 2006 he is with Universidad Autonoma de Madrid, where he is currently working as an assistant researcher. He has carried out different research internships in worldwide leading groups in biometric recognition such as BioLab from Universita di Bologna Italy, IDIAP Research Institute in Switzerland, or the Scribens Laboratory at the Ìcole Polytechnique de Montreal in Canada. His research interests are mainly focused on the security evaluation of biometric systems, but also include pattern and biometric recogniton, and synthetic generation of biometric traits. He is actively involved in European projects focused on vulnerability assessment of biometrics (e.g, STREP Tabula Rasa) and is the recipient of a number of distinctions, including:IBM Best Student Paper Award at ICPR 2008, and finalist of the EBF European Biometric Research Award.

JENNIFER GRANICK ***Stanford***

Jennifer Stisa Granick started as the Stanford Law School Center for Internet and Society's (CIS) Director of Civil Liberties in June of 2012. Jennifer returns to Stanford after stints as General Counsel of entertainment company Worldstar Hip Hop and as counsel with the internet boutique firm of Zwillgen PLLC. Before that, she was the Civil Liberties Director at the Electronic Frontier Foundation. Jennifer practices, speaks and writes about computer crime and security, electronic surveillance, consumer privacy, data protection, copyright, trademark and the Digital Millennium Copyright Act. From 2001 to 2007, Jennifer was Executive Director of CIS and taught Cyberlaw, Computer Crime Law, Internet intermediary liability, and Internet law and policy. Before teaching at Stanford, Jennifer spent almost a decade practicing criminal defense law in California. She was selected by Information Security magazine in 2003 as one of 20 "Women of Vision" in the computer security field. She earned her law degree from University of California, Hastings College of the Law and her undergraduate degree from the New College of the University of South Florida.

JONATHAN GRIER

Jonathan Grier has been an independent security consultant and researcher for over a decade. He has conducted forensic investigations, performed security audits, trained programmers in secure application development, and advised clients on data security. He has forensically investigated employee dishonesty, network break-ins, data theft and industrial espionage. Jonathan has consulted for clients in health care, telecommunications, construction, and professional services, and taught classes sponsored by the US Department of Defense Cyber Crime Center.

An active researcher, Jonathan has developed new methods used in forensics and application security. Microsoft Press, the Journal of Digital Investigation, Digital Forensics Magazine, Symantec, Information Week and the US Department of Defense have all featured his work.

DAN GUNTER

Dan brings a depth and breadth of experience for both the technical and business development side of information security. He has worked and consulted across the commercial, non-profit, academic and government sectors and recognizes the unique needs and constraints within each setting. He has served in roles ranging from proposal development and customer need analysis for high value information security contracts to designing and coding solutions to solve unique and challenging problems in settings with anywhere from a few users to hundreds of thousands of users. Dan holds an Undergraduate Degree in Computer Science and will finish his Masters in Computer Science soon.

PETER HANNAY ***Edith Cowan University***

Peter Hannay is a PhD student, researcher and lecturer based at Edith Cowan University in Perth Western Australia. His PhD research is focused on the acquisition and analysis of data from small and embedded devices. In addition to this he is involved in smart grid & network security research and other projects under the banner of the SECAU research organisation.

Peter is an accomplished academic, with more than 20 publications in peer reviewed conferences and journals, in addition he is a regular speaker at the Ruxcon and Kiwicon hacker conferences taking place in Australia and New Zealand respectively.

JERICHO

Jericho has been poking about the hacker/security scene for over 19 years (for real), building valuable skills such as skepticism and anger management. As a hacker-turned-security whore, he has a great perspective to offer unsolicited opinion on just about any security topic. A long-time advocate of advancing the field, sometimes by any means necessary, he thinks the idea of 'forward thinking' is quaint; we're supposed to be thinking that way all the time. No degree, no certifications, just the willingness to say things many in this dismal industry are thinking but unwilling to say themselves. He remains a champion of security industry integrity and small misunderstood creatures.

KEN JOHNSON ***Microsoft***

Ken Johnson works on the Security Science team within the Microsoft's Security Engineering Center (MSEC), where he primarily focuses on researching, developing, and implementing exploitation mitigation techniques. Ken's prior contributions to the field have included the development of an Address Space Layout (ASLR) implementation for Windows earlier than Vista. He is known for a number of prior articles on security-related, Windows internals, debugging, and reverse engineering topics (often contributed to the Uninformed Journal). Prior to joining Microsoft, Ken developed a number of advanced debugging tools for Windows on his own time, including the first accelerated kernel debugger transport for Windows VMware VMs (VMKD), and a debugger extension capable of importing data from IDA into WinDbg (SDbgExt). He has continued this tradition in recent times, contributing Hyper-V VM debugging support and self-consistent physical machine memory snapshot support to the Sysinternals LiveKd debugging too.

JASON JONES ***HP DVLabs***

I am a security researcher at HP DVLabs and lead for the ASI team that specializes in applied security research, malware analysis, and is responsible for our IP Reputation product. I have done research on Webkit instrumentation, web exploit toolkits, honeypots, and reverse engineering malware.

LOUKAS K aka SNARE ***Assurance***

Once upon a time, snare was a code-monkey, cranking out everything from pre-press automation apps to firmware for Big F***ing Laser Machines. Upon discovering that "information security" was actually a somewhat legitimate industry, and not just hacking stuff for fun, he got himself a job as a penetration tester. He now works as the Principal Consultant for Assurance in Melbourne, Australia.

Having been a Mac fanboy since around 1987, snare spends most of his free time messing with Mac OS X -from firmware to kernel rootkits to writing actual useful applications. When he's not playing with computers he enjoys hoppy pale ales, guitars, metal \m/, and building robots.

DAN KAMINSKY

Dan Kaminsky has been a noted security researcher for over a decade, and has spent his career advising Fortune 500 companies such as Cisco, Avaya, and Microsoft. Dan spent three years working with Microsoft on their Vista, Server 2008, and Windows 7 releases.

Dan is best known for his work finding a critical flaw

in the Internet's Domain Name System (DNS), and for leading what became the largest synchronized fix to the Internet's infrastructure of all time. Of the seven Recovery Key Shareholders who possess the ability to restore the DNS root keys, Dan is the American representative. Dan is presently developing systems to reduce the cost and complexity of securing critical infrastructure.

CHARITON KARAMITAS *Census Inc*

Chariton is an undergraduate student at the engineering school and works as an intern at Census Inc. His research interests include compilers, static analysis, reverse engineering and source code auditing. He enjoys spending his free time studying maths and coding stuff.

TOBY KOHLENBERG *Infosec*

Toby is a senior information security technologist for a Fortune 50 company and has been working in infosec since 1999. He has worked on a large number of different technologies in the information security space. His primary job is new technology evaluation, penetration, and defense. Recently he has been focusing on cloud and virtualization security.

TADAYOSHI KOHNO

University of Washington

Tadayoshi Kohno is an Associate Professor of Computer Science and Engineering at the University of Washington. His work focuses on finding vulnerabilities in insecure systems, and building secure systems. In 2003 he was part of the team that conducted the first security review of the Diebold electronic voting machine software, and he also conducted the first public experimental security analysis of a modern implantable cardiac device (2008) and a complete automobile (2010 and 2011). His group also framed a networked printer for copyright infringement, with the printer receiving a DMCA takedown notice for illegally downloading Iron Man. Prior to academia, Kohno worked as a cryptographer and security consultant at Counterpane Systems and Cigital. Kohno is the co-author of Cryptography Engineering, with Niels Ferguson and Bruce Schneier, and is chairing the 2012 USENIX Security Symposium.

SETH LAW *FishNet Security*

Seth Law is a Principal Consultant for FishNet Security in Application Security. He spends the majority of his time breaking web and mobile applications, but has been known to code when the need arises. Seth is currently involved in multiple open source projects (including RAFT) and is working with others to advance the state of mobile security testing tools. He has spoken previously at Black Hat, DEF CON, and other security conferences.

STEPHEN LAWLER

Stephen Lawler is the Founder and President of a small computer software and security consulting firm. Mr. Lawler has been actively working in information security for over 7 years, primarily in reverse engineering, malware analysis, and exploit development. While working at Mandiant he was a principal malware analyst for high-profile computer intrusions affecting several Fortune 100 companies.

Prior to this, as a founding member of ManTech International's Security and Mission Assurance (SMA) division he discovered numerous "0-day" vulnerabilities in COTS software and pioneered several exploitation techniques that have only been recently published.

Prior to his work at ManTech, Stephen Lawler was the lead developer for the AWESIM sonar simulator as part of the US Navy SMMTT program.

Stephen is also the technical editor of the book "Practical Malware Analysis" published by No Starch Press.

RYAN LINN *Trustwave*

Ryan Linn is a Senior Consultant with Trustwave's SpiderLabs -the advanced security team focused on penetration testing, incident response, and application security. Ryan is a penetration tester, an author, a developer,and an educator. He comes from a systems administration and Web application development background, with many years of IT security experience. Ryan currently works as a full-time penetration tester and is a regular contributor to open source projects including Metasploit and BeEF, the Browser Exploitation Framework.

DAVID LITCHFIELD

David Litchfield is recognized as one of the world's leading authorities on database security. He is the author of "Oracle Forensics", the "Oracle Hacker's Handbook", the "Database Hacker's Handbook and SQL Server Security" and is the co-author of the "Shellcoder's Handbook"and "Special Ops". He is a regular speaker at a number of computer security conferences and has delivered lectures to the National Security Agency, the UK's Security Service, GCHQ and the Bundesamt für Sicherheit in der Informationstechnik in Germany.

TARJEI MANDT *Azimuth Security*

Tarjei Mandt is a senior vulnerability researcher at Azimuth Security. He holds a Master's degree in Information Security and has previously spoken at security conferences such as Black Hat USA, INFILTRATE, SyScan, H2HC, and Hackito Ergo Sum. In his free time, he enjoys spending countless hours challenging security mechanisms and researching intricate issues in low-level system components. Recently, he has done extensive research on modern kernel pool exploitation and discovered several vulnerabilities in Windows kernel components.

CHARLIE MILLER *Accuvant Labs*

Charlie Miller is Principal Research Consultant at Accuvant Labs. He was the first with a public remote exploit for both the iPhone and the G1 Android phone. He is a four time winner of the CanSecWest Pwn2Own competition. He has authored three information security books and holds a PhD from the University of Notre Dame. He is currently being held in a maximum security prison in Cupertino, but hopes to be released soon for good behavior.

MATT MILLER *Microsoft*

Matt Miller works on the Security Science team within Microsoft's Security Engineering Center (MSEC) where he primarily focuses on researching and developing exploit mitigation technology. Some of Matt's past contributions in this space have included a functional implementation of Address Space Layout Randomization (ASLR) for Windows 2000/XP/2003 and a mitigation for SEH overwrites that is now known as SEHOP. Prior to joining Microsoft, Matt was involved with the Metasploit framework where he helped develop Metasploit 3.0 and contributed features like Meterpreter and VNC injection. Matt also co-founded the Uninformed Journal and has written articles on exploitation techniques, reverse engineering, and program analysis.

JULIEN MOINARD

Julien Moinard, an electronics technician with a solid background in this field (over 7 years) associated with many personal and professional experiments in the field of microcontrollers. Furthermore, he contributes to training 1st year students in an electrical engineering and industrial computing DUT (2-year technical degree). He is in the 2nd year of this program.

DAVID MORTMAN *enStratus*

David Mortman has been doing Information Security for well over 15 years and is currently the Chief Security Architect at enStratus. Most recently, he was the Director of Security and Operations at C3. Previously, David was the CISO at Siebel Systems and the Manager of Global Security at Network Associates. David speaks regularly at Black Hat, DEF CON, RSA and other conferences. Additionally, he blogs at emergentchaos.com, newschoolsecurity.com and securosis.com. David sits on a variety of advisory boards, including Qualys and Virtuosi. David holds a B.S. in Chemistry from the University of Chicago.

JEFF MOSS *ICANN*

Jeff Moss has been a hacker for over twenty years. In 1992 Jeff founded DEF CON, the largest hacker community and gathering in the world. Five years later, he started Black Hat, a series of technical conferences featuring the latest security research. In 2009, Jeff was appointed to the DHS Homeland Security Advisory Council, a group of subject matter experts providing advice to the Secretary of DHS. In 2011 Jeff was named Vice President and Chief Security Officer at the Internet Corporation for the Assignment of Names and Numbers (ICANN).

ICANN is a non-profit whose responsibilities include coordinating and ensuring the security, stability and resiliency of the Internet's unique global identifiers such

as IP address allocations, AS and protocol numbers, and digitally signing and maintaining the root zone of the Internet.

Jeff is uniquely qualified with his ability to bridge the gap between the underground researcher community and law enforcement, between the worlds of pure research and responsible application. As such, he is a popular keynote speaker at conferences and referenced in the Associated Press, CNN, New York Times, Reuters, Vanity Fair, and the Wall Street Journal. In 2011 Moss received the ICSA President's Award for Public Service and in 2012 he was named in Discovery Magazines "top 100 stories of 2012" as story #50.

Prior to ICANN Moss was the founder and CEO of Black Hat, where he remains as Conference Chair. He was a director at Secure Computing Corporation where he helped establish the Professional Services Department in the United States, Asia, and Australia. He has also worked for Ernst & Young, LLP in their Information System Security division. Moss graduated from Gonzaga University with a BA in Criminal Justice. He currently serves as a member of the U.S. Department of Homeland Security Advisory Council, and is a member of the Council on Foreign Relations.

COLLIN MULLINER

Technische Universitaet Berlin

Collin Mulliner is a researcher at Technische Universitaet Berlin (TU Berlin) and Deutsche Telekom Laboratories. Collin's main interest is in the area of security and privacy of mobile and embedded devices with an emphasis on mobile and smart phones. Since 1997 Collin has developed software and did security work for Palm OS, J2ME, Linux, Symbian OS, Windows Mobile, Android, and the iPhone. In 2006 he published the first remote code execution exploit based on the multimedia messaging service (MMS). Collin's most recent projects are in the area of vulnerability analysis and offensive security.

NILS ***MWR InfoSecurity***

Nils is heading the security research at MWR InfoSecurity. He likes to break and exploit stuff, which he demonstrated at pwn2own 2009 and 2010. He has spent most of 2010 and 2011 researching different mobile platforms and how to evade the exploitation mitigations techniques in place on these platforms. His current interest are embedded payment devices. Nils has previously presented at Black Hat on Android security.

STEVE OCEPEK ***Trustwave***

Steve Ocepek serves as the Senior Security Research Manager for Trustwave's SpiderLabs division -the advanced security team focused on penetration testing, incident response, and application security. An innovative network security expert with an entrepreneurial spirit, Steve Ocepek has been a driving force in pioneering Network Access Control (NAC) technologies delivering comprehensive endpoint control for mitigation of zero attacks, policy enforcement, and access management, for which he has been awarded 4 patents with 1 patent pending.

With a reputation for preventing, intercepting, and resolving malicious attacks from malware, viruses, and worms, Steve has provided consultative testing, and made recommendations for remediation for Fortune 500 and government enterprises in financial, credit card processing, educational, healthcare, and high-tech industries. His testing of network penetration, use of Network Access Control (NAC), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Web Application Firewalls (WAF), Network Firewalls, and Encryption Solutions enable him to advise on new countermeasures improving security, saving clients millions of dollars in losses of intellectual property, client data, customer confidence, and litigation costs.

Steve has led the growth of SpiderLabs Security Research Department, more than doubling services providing solutions to meet the needs of clients worldwide in identifying, preventing, and solving network security threats and problems. He is known as a trusted resource and problem solver by chief information officers, directors of security, chief technical officers, chief operating officers, chief executive officers, and military and national security leaders.

JEONG WOOK OH ***Microsoft***

I am a security researcher from Microsoft Malware Protection Center. We are dealing with all sorts of malwares and vulnerabilities.

One of my main subject of researches was patch analysis in the past. I released DarunGrim as an opensource project (*http://darungrim.org*) and it is one of the popular patch analysis tools.

Currently my research interests include but not limited to binary instrumentation, Java and Adobe Flash related vulnerabilities, application virtual machines, reverse engineering methodology and toolsets.

TSUKASA OI

Fourteenforty Research Institute, Inc.

Tsukasa Oi is a research engineer at Fourteenforty Research Institute, Inc. He is interested in low-level technologies such as virtualization and rootkits. He spoke at PacSec about anti-forensic rootkit and virtualization-based tracer. Currently, he focuses on mobile security and reverse engineering.

MING-CHIEH PAN ***Trend Micro***

Ming-chieh's (Nanika) major areas of expertise include vulnerability research, exploit techniques, malware detection and mobile security. He has 10+ years of experience on vulnerability research on Windows platform and malicious document and exploit. He has discovered numerous Windows system and document application vulnerabilities, such as Microsoft Office, Adobe PDF, and Flash. He frequently presents his researches at security conferences in Asia, including Syscan Singapore/Taipei/Hong Kong 08/10, Hacks in Taiwan 05/06/07/09/10. Ming-chieh is a staff research engineer with Trend Micro. He and Sung-ting are members of CHROOT security group in Taiwan.

TOMISLAV PERICIN ***ReversingLabs***

Tomislav Pericin has been analyzing and developing software packing and protection methods for the last 9 years. He is one of the founders of ReversingLabs and the chief software architect behind such projects as TitaniumCore, TitanEngine, NyxEngine and RLPack. Recently he spoke at Black Hat, ReCon, CARO Workshop, SAS and TechnoSecurity conferences.

NICHOLAS PERCOCO ***Trustwave***

With more than 15 years of information security experience, Percoco leads the global SpiderLabs organization that has performed more than 1300 computer incident response and forensic investigations globally, run thousands of ethical hacking and application security tests for clients, and conduct bleeding-edge security research to improve Trustwave's products.

Prior to joining Trustwave, Percoco ran security consulting practices at VeriSign, and Internet Security Systems. In 2004, he drafted an application security framework that became known as the Payment Application Best Practices (PABP). In 2008, this framework was adopted as a global standard called Payment Application Data Security Standard (PA-DSS).

As a speaker, he has provided unique insight around security breaches, malware, mobile security and InfoSec trends to public (Black Hat, DEF CON, SecTor, You Sh0t the Sheriff, OWASP) and private audiences (Including DHS, US-CERT, Interpol, United States Secret Service) throughout North America, South America, Europe, and Asia.

Percoco and his research has been featured by many news organizations including:The Washington Post, eWeek, PC World, CNET, Wired, Hakin9, Network World, Dark Reading, Fox News, USA Today, Forbes, Computerworld, CSO Magazine, CNN, The

Times of London, NPR, Gizmodo, Fast Company, Financial Times and The Wall Street Journal.

In 2011, SC Magazine named Percoco Security Researcher of the Year. In addition, he was inducted into the inaugural class of the Illinois State University College of Applied Science and Technology Academy of Achievement.

Percoco is a member of the Dean's Advisory Board for The College of Applied Science & Technology at Illinois State University and a co-creator on the planning committee of THOTCON, a hacking conference held in Chicago each year. He has a Bachelor of Science in Computer Science from Illinois State University.

JAMES PHILPUT

Information Assurance Professionals

James Philput has worked in Information Technology for the past 15 years. Specializing in Information Security, he has worked for organizations in the Education, Healthcare, Communications, Government, and Defense fields.

James is currently a Sr. Information Security Analyst with IAP, Information Assurance Professionals. There he works with clients to secure their infrastructure, focusing on organizational architecture, and compliance with applicable laws and standards. In addition to consulting on security architecture, James is responsible for the design and maintenance of the intrusion detection and prevention systems, writing and updating information security policy, and running the vulnerability assessment tools needed to keep abreast of potential vulnerabilities within client networks.

Prior to his work with the IAP, James worked to improve the state of information security as a whole in his time as an author and instructor for the SANS Institute. At SANS, James co-authored a course on Linux Systems Administration, and acted as editor and technical reviewer for various security courses. While acting as an author and editor, James also taught various courses on information security and IT operations at SANS conferences across the US.

James plays an active role in the security community. An active participant of the GIAC advisory board, and several other mailing lists, he provides information and opinion that is used to shape future training classes and best practices within the industry. James continues to work on a volunteer basis for the SANS Institute as a technical reviewer for new and updated course material, and has begun working as a guest speaker for organizations such as the Virginia Information Security Officers Advisory Group and the League of Women Voters.

ALEXANDER POLYAKOV ***ERPSCAN***

Alexander Polyakov aka @sh2kerr, CTO at ERPSCAN, head of DSecRG and architect of ERPSCAN Security scanner for SAP. His expertise covers security of enterprise business-critical software like ERP, CRM, SRM, RDBMS, banking and processing software. He is the manager of OWASP-EAS (OWASP subproject), a well-known security expert of the enterprise applications of such vendors as SAP and Oracle, who published a significant number of the vulnerabilities found in the applications of these vendors. He is the writer of multiple whitepapers devoted to information security research, and the author of the book "Oracle Security from the Eye of the Auditor: Attack and Defense" (in Russian). He is also one of the contributors to Oracle with Metasploit project. Alexander spoke at the international conferences like Black Hat, HITB (EU/ASIA), Source, DeepSec, CONFidence, Troopers.

PHIL PURVIANCE ***AppSec Consulting***

Phil Purviance is an Application Security Consultant for AppSec Consulting where he researches application security vulnerabilities and performs penetration testing. Phil's body of work includes the discovery and proof-of-concept exploitations of critical security vulnerabilities, design flaws, and system weaknesses in hundreds of custom web sites and web application frameworks. Purviance also consults with clients and recommends helpful countermeasures that are useful to mitigate serious security vulnerabilities. Phil's recent exploit talks include the security of HTML5, and the revealing of cross-site scripting vulnerabilities in Skype for iOS. Phil's contributions to the security community have earned him a placement into both the Google and Facebook Security Hall of Fame.

MARCUS RANUM ***Tenable Security, Inc.***

Marcus J. Ranum is a world-renowned expert on security system design and implementation. He is recognized as an early innovator in firewall technology, and the implementor of the first commercial firewall product. Since the late 1980's, he has designed a number of groundbreaking security products including the DEC SEAL, the TIS firewall toolkit, the Gauntlet firewall, and NFR's Network Flight Recorder intrusion detection system. He has been involved in every level of operations of a security product business, from developer, to founder and CEO of NFR. Marcus has served as a consultant to many FORTUNE 500 firms and national governments, as well as serving as a guest lecturer and instructor at numerous high-tech conferences. In 2001, he was awarded the TISC "Clue" award for service to the security community, and the ISSA Lifetime Achievement Award. Marcus is Chief of Security for Tenable Security, Inc., where he is responsible for research in open source logging tools, and product training. He serves as a technology advisor to a number of start-ups, established concerns, and venture capital groups.

RYAN REYNOLDS ***Crowe***

Ryan has been with Crowe for five years and is the Manager responsible for Crowe's Penetration Testing methodology and tool development. Ryan has a wide range of knowledge and experience in system administration and networking to include security applications and controls. He is a technical lead for engagements including application, network and infrastructure penetration testing on both internal and external systems.

STEPHEN RIDLEY

Stephen A. Ridley is a security researcher with more than 10 years of experience in software development, software security, and reverse engineering. He currently serves as Director of Information Security for a financial services firm. Before this, Mr. Ridley served as Senior Researcher at Matasano. Prior to that:Senior Security Architect at McAfee where he helped build the McAfee Security Architecture research group. Before that, he was a founding member of ManTech International's Security and Mission Assurance (SMA) group where he did vulnerability research and reverse engineering in support the U.S. defense and intelligence communities. He has spoken about reverse engineering and software security on every continent except Australia and Antartica (Black Hat, ReCon, Summercon, EuSecWest, Syscan and others). Mr. Ridley currently lives in Manhattan and frequently guest lectures at New York area universities such as NYU and Rensselaer Polytechnic Institute.

IVAN RISTIC ***SSL Labs***

Ivan Ristic is a respected security expert and author, known especially for his contribution to the web application firewall field and the development of ModSecurity, an open source web application firewall. He is also the author of Apache Security, a comprehensive security guide for the Apache web server, and ModSecurity Handbook. He founded SSL Labs, a research effort focused on the analysis of the real-life usage of SSL and the related technologies. A frequent speaker at computer security conferences, Ivan is a member of the Open Web Application Security Project (OWASP), and an officer of the Web Application Security Consortium (WASC).

TOM RITTER *iSEC Partners*

Tom Ritter is a Security Consultant at iSEC Partners, a strategic digital security organization, performing application and system penetration testing and analysis for multiple platforms and environments. He graduated from Stevens Institute of Technology with a Masters in Computer Science; prior to iSEC, he has worked as a Security Engineer at a lead security consulting company and a Team Lead in .Net and SQL Server Development for a Financial Services Company. He has presented at security conferences in Europe, North and South America and is involved in IETF Working Groups relating the internet-standard secure protocols. His research interests are centered around cryptography, anonymity, and privacy.

CHRIS ROHLF *Leaf Security Research*

Chris Rohlf has been working in computer security for nearly a decade and is currently an Independent Security Consultant and President of Leaf Security Research (Leaf SR). Prior to founding Leaf SR, Chris was a principal security consultant at Matasano Security in NYC. He has spent the last 10 years as a security researcher, consultant, developer and engineer for organizations including the US Department of Defense. He has spoken at industry conferences including Black Hat Vegas 2009 and 2011, guest lectured at NYU Poly in Brooklyn NY, has been published in IEEE Security and Privacy magazine and is occasionally quoted by various media outlets. His security advisories include every major web browser, operating systems and more.

MATHEW ROWLEY *Matasano Security*

Mathew Rowley is a security consultant for Matasano Security with over 6 years experience as a computer security professional. His experience includes reverse engineering, mobile security, web application security assessment, network security, fuzzing, and application development.

PAUL ROYAL

Georgia Institute of Technology

Paul Royal is a Research Scientist at the Georgia Institute of Technology, where he engages in collaborative research on various facets of the online criminal ecosystem. Prior to Georgia Tech, Royal served as Principal Researcher at Purewire, Inc, where he worked with other researchers to identify threats and design methods that enhanced the company's web security service. Royal often focuses on research topics interesting to both academics and industry practitioners, with previous work presented at Black Hat USA that subsequently appeared in ACM CCS.

PAUL SABANAL *IBM*

Paul Sabanal is a security researcher on IBM ISS's X-Force Advanced Research Team. He has spent most of his career as a reverse engineer, initially as a malware researcher and now focusing mainly on vulnerability analysis and exploit development. He has previously presented at Black Hat with Mark Yason on the subject of C++ reversing and Adobe Reader's Protected Mode Sandbox. His main research interests these days are in protection technologies and automated binary analysis tools. He is currently based in Manila, Philippines.

RUBEN SANTAMARTA *IOActive labs*

Ruben Santamarta works as security researcher at IOActive labs. He has been mainly focused on offensive security and research, discovering dozens of vulnerabilities in leading software and industrial vendors, also worked in other areas such as malware analysis or anti-fraud technologies. During the last few years he has been researching into the ICS security, releasing important vulnerabilities and presenting a research about very specific attacks against the power grid. Ruben has been presenting at international conferences such as Ekoparty, AppSecDC, RootedCon.

BRUCE SCHNEIER

Bruce Schneier is an internationally renowned security technologist and author. Described by The Economist as a "security guru," Schneier is best known as a refreshingly candid and lucid security critic and commentator. When people want to know how security really works, they turn to Schneier. His first bestseller, "Applied Cryptography", explained how the arcane science of secret codes actually works, and was described by Wired as "the book the National Security Agency wanted never to be published." His book on computer and network security, Secrets and Lies, was called by Fortune "[a] jewel box of little surprises you can actually use."

His current book, Beyond Fear, tackles the problems of security from the small to the large: personal safety, crime, corporate security, national security. Schneier also publishes a free monthly newsletter, Crypto-Gram, with over 100,000 readers. In its seven years of regular publication, Crypto-Gram has become one of the most widely read forums for free-wheeling discussions, pointed critiques, and serious debate about security. As head curmudgeon at the table, Schneier explains, debunks, and draws lessons from security stories that make the news. Regularly quoted in the media, Schneier has written op ed pieces for several major newspapers, and has testified on security before the United States Congress on many occasions. Bruce Schneier is the founder and CTO of Counterpane Internet Security, Inc., the world's leading protector of networked information—the inventor of outsourced security monitoring and the foremost authority on effective mitigation of emerging IT threats.

SEAN SCHULTE *Trustwave*

Sean develops backend services for Trustwave SSL, and writes mobile apps and games in his spare time. He's done malware analysis on Android malware found in the wild, and discovered an Android design flaw that he presented at DEF CON.

FERMIN J. SERNA *Google*

My name is Ferm'n J. Serna (aka Zhodiac). I was born in Madrid (Spain) in the 1979. I am a Computer Science Engineer graduated at the UCM, and currently working for Google at the Mountain View (California) offices as a Information Security Engineer at the (ISE) team. Previously I have worked for Microsoft at the MSRC Engineering team.

I have lots of things that attract my attention, mainly security ones such as exploitation techniques, fuzzing, binary static analysis, reverse engineering, coding... but also Artificial Intelligence, chess...

SHREERAJ SHAH *Blueinfy*

Shreeraj Shah, B.E., MSCS, MBA, CSSLP is the founder of Blueinfy, a company that provides application security services. Prior to founding Blueinfy, he was founder and board member at Net Square. He also worked with Foundstone (McAfee), Chase Manhattan Bank and IBM in security space. He is also the author of popular books like Web 2.0 Security, Hacking Web Services and Web Hacking:Attacks and Defense. In addition, he has published several advisories, tools, and whitepapers, and has presented at numerous conferences including RSA, AusCERT, InfosecWorld (Misti), HackInTheBox, Black Hat, OSCON, Bellua, Syscan, ISACA etc. His articles are regularly published on Securityfocus, InformIT, DevX, Oreilly, HNS. His work has been quoted on BBC, Dark Reading, Bank Technology as an expert.

SERGEY SHEKYAN *Qualys*

Sergey Shekyan is a Senior Software Engineer for Qualys, where he is focused on development of the company's on demand web application scanning service. With more than 10 years of experience in software design, development, testing and documentation, Sergey has contributed key product enhancements and software modules to various companies. Prior to Qualys, he designed and implemented a web-based system for general aviation pilots. As a senior software engineer for Navis, he contributed to projects involving development of container terminal operating systems (TOS) simulation software. He also designed and developed data analysis software modules for Virage Logic, a provider of semiconductor IP for the design of complex integrated circuits. Prior to working at Virage Logic, he developed manufacturing test program generation software for Credence Systems Corporation. Sergey holds both Masters and BS Degrees in Computer Engineering from the State Engineering University of Armenia.

ADAM SHOSTACK *Microsoft*

Shostack helped found the CVE, the Privacy Enhancing Technologies Symposium and the International Financial Cryptography Association. He has been a leader at a number of successful information security and privacy startups, and is co-author of the widely acclaimed book, "The New School of Information Security". Shostack is currently

a principal program manager on the Microsoft Trustworthy Computing Usable Security team, where among other accomplishments, he's Shostack helped found the CVE, the Privacy Enhancing Technologies Symposium and the International Financial Cryptography Association. He has been a leader at a number of successful information security and privacy startups, and is co-author of the widely acclaimed book, The New School of Information Security. Shostack is currently a principal program manager on the Microsoft Trustworthy Computing Usable Security team, where among other accomplishments, he shipped the Microsoft Security Development Lifecycle (SDL) Threat Modeling Tool and the Elevation of Privilege threat modeling game as a member of the SDL team.

MICKEY SHKATOV *Intel Corporation*

My name is Mickey Shaktov (AKA Laplinker), I am from Israel and am an Information systems engineer graduated at the BGU. I am currently unaffiliated to any corporation, Previously I have worked for Intel Corporation as a security researcher and evaluator, breaking software, firmware and hardware.

A PROUD DC9723 MEMBER, NOT A MOSSAD AGENT, BREAKER OF CODE, RESEARCHER OF VULNERABILITIES THAT WILL NEVER SEE THE LIGHT OF DAY AND A GUY WHO WILL ALLWAYS SAY WHAT IS ON HIS ON MIND SO BRACE YOUR SELVES. CHENGYU SONG

Georgia Institute of Technology

Chengyu Song is a PhD student at Georgia Institute of Technology. His current research interest is in system security, with a special focus on topics that may have practical impact. Prior to Georgia Tech, Chengyu received his Bachelor's and Master's degree at Peking University China, where he worked with other researchers on malware analysis, botnet, underground economy and drive-by download attacks. He is also a member of the Honeynet Project.

SOLOMON SONYA

Solomon is an avid programmer and researcher focusing on the analysis of malware and computer memory management. Solomon's main research areas center on the discovery of vulnerabilities introduced by the mismanagement of volatile computer memory and resource allocations. Solomon has devoted many hours in academia mentoring students and teaching Computer Science techniques. As a Network Security Engineer, Solomon provides digital forensics capabilities and security solutions to better prevent, detect, respond to and mitigate network penetrations, malware infections and other threats from large-scale enterprise networks for the commercial, private, and government sectors. Solomon received his Undergraduate Degree in Computer Science and is currently pursuing Masters Degrees in Information Systems Engineering and Computer Science.

ALEX STAMOS *Artemis*

Alex Stamos is the CTO of Artemis, the division of NCC Group that is taking on hard security problems starting with the .Secure gTLD. He was the co-founder of iSEC Partners, one of the world's premier security consultancies and also a part of NCC Group. Alex has spent his career building or improving secure, trustworthy systems, and is a noted expert in Internet

infrastructure, cloud computing and mobile security. He is a frequently request speaker at conferences such as Black Hat, DEF CON, Amazon ZonCon, Microsoft Blue Hat, FS-ISAC and Infragard. He holds a BSEE from the University of California, Berkeley and his personal security writings are available at *http://unhandled.com*.

TIMOTHY STRAZZERE
Lookout Mobile Security

Tim Strazzere is a Security Engineer at Lookout Mobile Security. Along with writing security software, he specializes in reverse engineering and malware analysis. Some interesting past projects include having reversing the Android Market protocol, Dalvik decompilers and memory manipulation on mobile devices.

VAAGN TOUKHARIAN ***Qualys***

Toukharian is a developer for Qualys's Web Application Scanner. He has been involved in the security industry since 1999. Experience includes work on Certification Authority systems, encryption devices, large CAD systems, Web scanners. His outside of work interests include Web Design, Photography, and Ironman Triathlons.

SUNG-TING TSAI ***Trend Micro***

Sung-ting (TT) is a manager of an advanced threat research team in core tech department of Trend Micro. His major areas of interest include document exploit, malware detection, sandbox technologies, system vulnerability and protection, web security, cloud and virtualization technology. He also has been doing document application security research for years, and has presented his researches in Black Hat USA 2011, Syscan Singapore 10 and Hacks in Taiwan 08. He and Ming-chieh are members of CHROOT security group in Taiwan.

CHRIS VALASEK ***Coverity***

Chris Valasek is a Senior Security Researcher at Coverity. As part of the security research team in the Office of the CTO, Valasek is focused on reverse engineering and researching new and existing security vulnerabilities; building this knowledge into the Coverity technology portfolio and share it broadly across the development community. Prior to Coverity, Valasek was a Senior Research Scientist at Accuvant LABS and IBM Internet Security Systems. Valasek's research focus spans areas such as vulnerability discovery, exploitation techniques, and reverse engineering, contributing public disclosures and authoring research on these topics to the broader security community. While Valasek is best known for his publications regarding the Microsoft Windows Heap, his research has broken new ground in areas such as vulnerability discovery, exploitation techniques, reverse engineering, source code and binary auditing, and protocol analysis. Valasek has presented his research at major international security conferences including Black Hat USA and Europe, ekoparty, INFILTRATE, and RSA, and is the chairman of SummerCon, the nation's oldest hacker convention.

RAFAEL DOMINGUEZ VEGA
MWR InfoSecurity

Rafa works in the UK as a Security Consultant and Security Researcher for MWR InfoSecurity. He enjoys testing "out of the ordinary" technology and is particularly interested in embedded devices and hardware hacking. He has previously presented innovative research on topics such as USB drivers exploitation and Smart card hacking at various well known security conferences.

DAVID VO ***FishNet Security***

Over 10 years of IT experience. 5 yrs of experience in AppSec and Mobile Security. Currently on the Mobility team at FishNet Security working with MDM and Mobile Security. CISSP

MARIO VUKSAN ***ReversingLabs***

Mario has been involved in development of advanced security solutions for the last seven years and has rich engineering background spanning the last 20 years. Before founding ReversingLabs, Mario was the Director of Research at Bit9 and one of its founding engineers. He spoke at numerous conferences over the last 6 years including CEIC, Black Hat, RSA, DEF CON, Caro Workshop, Virus Bulletin and AVAR Conferences. He is author of numerous blog posts on security and has authored "Protection in Untrusted Environments" chapter for the "Virtualization for Security" book. He coordinates AMTSO Advisory Board and works with IEEE Malware Working Group.

MARK WEATHERFORD ***Cybersecurity***

Mark Weatherford is the Deputy Under Secretary for Cybersecurity for the National Protection and Programs Directorate (NPPD), a position that will allow DHS NPPD to create a safe, secure, and resilient cyberspace. Weatherford has a wealth of experience in information technology and cybersecurity at the Federal, State and private sector levels.

Weatherford was previously the Vice President and Chief Security Officer of the North American Electric Reliability Corporation (NERC) where he directed the cybersecurity and critical infrastructure protection program.

Before NERC, Weatherford was with the State of California where he was appointed by Governor Arnold Schwarzenegger as the state's first Chief Information Security Officer. Prior to California, he served as the first Chief Information Security Officer for the State of Colorado, where he was appointed by two successive governors. Previously, as a member of the Raytheon Company, he successfully built and directed the Navy/Marine Corps Intranet Security Operations Center (SOC) in San Diego, California, and also was part of a team conducting security certification and accreditation with the U.S. Missile Defense Agency. A former U.S. Navy Cryptologic Officer, Weatherford led the U.S. Navy's Computer Network Defense operations and the Naval Computer Incident Response Team (NAVCIRT).

Weatherford earned a bachelor's degree from the University of Arizona and a master's degree from the Naval Postgraduate School. He also holds the Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) certifications. He was awarded SC Magazine's prestigious "CSO of the Year" award for 2010. He was named one of the 10 Most Influential People in Government Information Security for 2012 by GovInfo Security.

Weatherford is an avid runner and enters races with his wife at least monthly. He also travels frequently for pleasure.

DON C. WEBER ***InGuardians***

Jack of All Trades and hardware analysis expert for the InGuardians. Don specializes in physical and information technology penetration testing, web assessments, wireless assessments, architecture review, incident response/digital forensics, product research, hardware research, code review, security tool development, and the list goes on. Don is currently focusing on hardware research specifically in the technologies surrounding products comprising the SMART GRID. He has focused on implementing various communication protocols and microprocessor disassemblers/emulators for research, testing, risk assessment, and anything else you can think of with these technologies.

RALF-PHILLIP WEINMANN
University of Luxembourg

Ralf-Philipp Weinmann is a research associate at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg. His research interests lie in the intersection of cryptography, privacy, mobile security and reverse-engineering. In the past years was involved in speeding up attacks against WEP, the deDECTed.org team that broke the proprietary crypto of DECT, PWN2OWN wins and the first demonstrated remote vulnerabilities in cellular baseband stacks. He is one of the authors of the "iOS Hacker's Handbook".

RAFAL WOJTCZUK ***Bromium***

Rafal Wojtczuk has over 15 years of experience with computer security. Specializing primarily in kernel and virtualization security, over the years he has disclosed many security vulnerabilities in popular operating system kernels and virtualization software. He is also well known for his articles on advanced exploitation techniques, including novel methods for exploiting buffer overflows in partially randomized address space environments. Recently he was researching advanced Intel security-related technologies, particularly TXT and VTd. He is also the author of libnids, a low-level packet reassembly library. He holds a Master's Degree in Computer Science from University of Warsaw.

Get buzzed for free.

Seriously.

Coffee all day at our booth in the Octavius Ballroom Foyer.

OWASP

The free and open software security community.

www.owasp.org

MARK VINCENT YASON *IBM*

Mark Vincent Yason is a security researcher on IBM's X-Force Advanced Research team. Mark's current focus area is vulnerability and exploit research -he analyzes known vulnerabilities, discovers new vulnerabilities, studies exploitation techniques, and creates detection guidance/algorithms which are used in the development of IDS/IPS signatures. He also previously worked on malware research which naturally involved some degree of software protection research. He authored the paper "The Art of Unpacking" and co-authored the papers "Reversing C++" and "Playing In The Reader X Sandbox", all of which were previously presented at Black Hat.

WORKSHOPS

ATLAS

Atlas is a doer of stuff. inspired by the illustrious sk0d0, egged on by invisigoth of kenshoto, atlas has done a lot of said 'stuff' and lived to talk about it. whether he's breaking out of virtual machines, breaking into banks, or breaking into power systems, atlas is always entertaining, educational and fun.

TIMUR DUEHR *Matasano Security*

Timur Duehr is a Senior Security Consultant at Matasano Security with over seven years computer consulting experience and a Master's degree in Mathematics. His professional experience includes application development, security assessment, and code review.

At Matasano he develops security assessment tools, maintains Ragweed and Buby, performs blackbox and code assisted penetration tests, and source code audits. He has tested applications employing numerous technologies. Previously, he has presented at OWASP Chicago and Black Hat Arsenal.

ERIC FULTON

Eric Fulton is a specialist in network penetration testing and web application assessments. His clients have included Fortune 500 companies, international financial institutions, global insurance firms, government entities, telecommunications companies, as well as world-renowned academic and cultural institutions. In his spare time, Eric works with local students to provide hands-on security training, and conducts independent security research on a number of topics.

ABRAHAM KANG *HP Fortify*

Currently am a Principal Security Researcher with HP Fortify Have been focused on Application Security for over 8 years. Working as a Security Architect, Security Code Reviewer/Vulnerability Researcher and Principal Security Researcher. Contributed content and articles for the OWASP Guide and OWASP Cheat Sheets.

Have been a developer since 1996. Have a Bachelor of Science from Cornell University and Juris Doctor from Lincoln Law School of San Jose.

KRZYSZTOF KOTOWICZ

AppSec Consulting

Krzysztof Kotowicz is a Web security researcher specialized in the discovery and exploitation of HTML5 vulnerabilities. He is the author of multiple recognized HTML5/UI redressing attack vectors. Speaker at international IT security conferences & meetings (SecurityByte, HackPra, Hack In Paris, CONFidence). Works as IT security consultant with SecuRing and IT security trainer with Niebezpiecznik.pl. Author of the "Hacking HTML5" training program. Takes part in multiple Security Bug Bounty programs (Google Security Bug Bounty, Facebook White Hat, Piwik Security Bug Bounty).

LONG LE

Long Le, CISA, is a security manager at one of the largest software outsourcing companies in Vietnam. He has been actively involved in computer security for more than 10 years since he and his friends founded the pioneer Vietnamese security research group VNSECURITY (*http://vnsecurity.net*). Described as neither a researcher nor a hacker, he loves playing wargames and Capture-The-Flag with the CLGT team in his spare time. He was also a speaker at various conferences including Black Hat USA, HackInTheBox, SyScan, PacSec.

KYLE OSBORN *AppSec Consulting*

Kyle Osborn is a penetration tester at AppSec Consulting, where he specializes in web application security, network penetration, and physical assessments. He plays a bad guy at the Western Regional Collegiate Cyber Defense Competition. Osborn has developed a CTF, with his team, for the United States Cyber Challenge ÒCyber CampsÓ, where a number of campers competed in. Osborn has previously discussed browser and mobile security at prominent conferences such as Black Hat USA, DEF CON, Toorcon, DerbyCon, and TakeDownCon.

CHRISTIEN RIOUX *Veracode*

Christien Rioux, co-founder and chief scientist of Veracode, is responsible for the technical vision and design of Veracode's advanced security technology. Working with the engineering team, his primary role is the design of new algorithms and security analysis techniques. Before founding Veracode, Mr. Rioux founded @stake, a security consultancy, as well as L0pht Heavy Industries, a renowned security think tank. Mr. Rioux was a research scientist at @ stake, where he was responsible for developing new software analysis techniques and for applying cutting edge research to solve difficult security problems. He also led and managed the development for a new enterprise security product in 2000 known as the SmartRisk Analyzer (SRA), a binary analysis tool and its patented algorithms, and has been responsible for its growth and development for the past five years.

At L0pht, he co-authored the best-selling Windows password auditing tool @stake LC (L0phtCrack) and the AntiSniff network intrusion detection system. His other activities with L0pht included significant security research, publication work and public speaking engagements. Mr. Rioux is also responsible for numerous security advisories in many applications, operating systems and environments. He is recognized as an authority in the areas of Windows product vulnerability assessment, application optimization and program analysis.

His background includes 23 years of computer programming and software engineering experience on a wide range of platforms and for numerous companies, including financial institutions, mechanical engineering firms, educational institutions and multimedia groups.

He graduated from the Massachusetts Institute of Technology in 1998, with a Bachelor's Degree in Computer Science.

CORY SCOTT *Matasano Security*

Cory Scott is a director at Matasano Security, an independent security research and development firm that works with vendors and enterprises to pinpoint and eradicate security flaws, using penetration testing, reverse engineering, and source code review. Prior to joining Matasano, he was the Vice President of Technical Security Assessment at ABN AMRO / Royal Bank of Scotland. He also has held technical management positions at @stake and Symantec. He has presented at Black Hat Briefings, USENIX, OWASP and SANS.

MICHAEL TRACY *Matasano Security*

Mike is a senior security consultant at Matasano.

JONATHAN ZDZIARSKI *viaForensics*

Jonathan is Sr. Forensic Scientist for viaForensics, a Chicago-based consulting firm where, among other things, he performs research and development, and penetration testing of iOS applications for corporate clients. Jonathan gets paid, in part, to hack things for a living.

Jonathan Zdziarski is better known as the hacker "NerveGas" in the iPhone development community. His work in cracking the iPhone helped lead the effort to port the first open source applications, and his first iOS-related book, iPhone Open Application Development, taught developers how to write applications for the popular device long before Apple introduced its own SDK. Jonathan has since written several books on iOS, including iPhone Forensics, iPhone SDK Application Development, and his latest book, Hacking and Securing iOS Applications.

Jonathan frequently trains and consults law enforcement agencies to assist forensic examiners in high profile criminal cases.

SPEAKERS

TURBO TALKS

RYAN BARNETT *SpiderLabs*

Ryan Barnett joined SpiderLabs after a decade in computer security. As Research -Surveillance Team Leader, he leads the SpiderLab team which specializes in application defense. This includes SPAM filtering, network IDS/IPS and web application firewalls. His main area of expertise is in application defense research.

Barnett is renowned in the industry for his unique expertise. He has serves as the Open Web Application Security Project (OWASP) ModSecurity Core Rule Set Project Leader and Project Contributor on the OWASP Top Ten and AppSensor Projects. He is a Web Application Security Consortium (WASC) Board Member and Project Leader for the Web Hacking Incident Database (WHID) and the Distributed Web Honeypot Projects. He is also a Certified Instructor at the SANS Institute.

Barnett is regularly consulted by industry news outlets like Dark Reading, SC Magazine and Information Week. He is the author of Preventing Web Attacks with Apache (Addison-Wesley Professional, 2006.) Key industry events he has addressed include Black Hat, SANS AppSec Summit and the OWASP Global Summit.

SEAN BARNUM *The MITRE Corporation*

Sean Barnum is a Cyber Security Principal at The MITRE Corporation where he acts as a thought leader and senior advisor on software assurance and cyber security topics to a wide variety of US government sponsors throughout the national security, intelligence community and civil domains. He has over 25 years of experience in the software industry in the areas of architecture, development, software quality assurance, quality management, process architecture & improvement, knowledge management and security. He is a frequent contributor, speaker and trainer for regional, national and international cyber security and software quality publications, conferences & events. He is very active in the Cyber Security community and is involved in numerous knowledge standards-defining efforts including the Common Weakness Enumeration (CWE), the Common Attack Pattern Enumeration and Classification (CAPEC), the Software Assurance Findings Expression Schema (SAFES), the Malware Attribute Enumeration and Characterization (MAEC), the Cyber Observables eXpression (CybOX), the Indicator Exchange eXpression (IndEX), the Structured Threat Information eXpression (STIX) and other elements of the Cyber Security Programs of the Department of Homeland Security, Department of Defense and NIST. He is coauthor of the book "Software Security Engineering:A Guide for Project Managers", published by Addison-Wesley. He serves as the official liaison between ISO/IEC JTC 1/SC 27/ WG 3 and the Cyber-Security Naming & Information Structures Group. He also acted as the lead technical subject matter expert for design and implementation

of the Air Force Application Software Assurance Center of Excellence (ASACoE).

ANG CUI *Columbia University*

Ang Cui is currently a PhD student at Columbia University in the Intrusion Detection Systems Laboratory. His research focuses on the exploitation and defense of embedded devices. Before starting his PhD, Ang worked as a security specialist within various financial institutions.

ALBAN DIQUET *iSEC Partners*

Alban Diquet is a Senior Security Consultant at iSEC Partners, a strategic digital security organization, performing application and system penetration testing and analysis for multiple platforms and environments.

While at iSEC, Alban has led or contributed to numerous security assessments on a variety of client/server applications, including large scale web applications, iOS/Android applications, thick clients, and server applications. Alban's research interests include web security, SSL, and PKI. He recently released an open source SSL scanner written in Python, called SSLyze.

Prior to working at iSEC, Alban was a Software Engineer at Sigma Designs Inc, where he was implementing Digital Right Management solutions for video content. Alban received a M.S. in Computer and Electrical Engineering from the "Institut Superieur d'Electronique de Paris" in Paris, France, and a M.S in "Secure and Dependable Computer Systems" from Chalmers University, in Gothenburg, Sweden.

NICK GALBREATH *Etsy*

Nick Galbreath is a director of engineering at Etsy, overseeing groups handling security, fraud, security, authentication and other enterprise features. Over the last 18 years, Nick has held leadership positions in number of social and e-commerce companies, including Right Media, UPromise, Friendster, and Open Market, and has consulted for many more. He is the author of "Cryptography for Internet and Database Applications" (Wiley), and was awarded a number of patents in the area of social networking. He holds a master's degree in mathematics from Boston University.

RYAN HOLEMAN *Ziften Technologies*

Ryan Holeman resides in Austin Texas where he works as a senior server software developer for Ziften Technologies. He has a Masters of Science in Software Engineering and has published papers though ICSM and ICPC. His spare time is mostly spent digging into various network protocols and shredding local skateparks.

MATIAS KATZ

Matias Katz is a Penetration Tester who specializes Web security analysis. He loves to build simple tools to perform discovery and exploitation on any software or network. Also, he is Super Mario World master!!

ZACH LANIER *Veracode*

Zach Lanier is a Security Researcher with Veracode, specializing in network, mobile, and web application security. Prior to joining Veracode, Zach served as Principal Consultant with Intrepidus Group, Senior Network Security Analyst at Harvard Business School, and Security Assessment Practice Manager at Rapid7. He has spoken at a variety of security conferences, including INFILTRATE, ShmooCon, and SecTor, and is a co-leader of the OWASP Mobile Security Project. Zach likes Android, vegan food, and cats (but not as food).

EIREANN LEVERETT *IOActive*

Eireann Leverett studied Artificial Intelligence and Software Engineering at Edinburgh University and went on to get his Masters in Advanced Computer Science at Cambridge. He studied under Frank Stajano and Jon Crowcroft in Cambridge's computer security

group. In between he worked for GE Energy for 5 years and has just finished a six month engagement with ABB in their corporate research Dept. He now proudly joins IOActive to focus on Smart Grid and SCADA systems.

His MPhil thesis at Cambridge was on the increasing connectivity of industrial systems to the public internet. He focussed on finding the cheapest way to find and visualise these exposures and associated vulnerabilities. He shared the data with ICS-CERT and other CERT teams globally, and presents regularly to academics and government agencies on the security of industrial systems.

More importantly, he is a circus and magic enthusiast, and likes to drink beer.

MORGAN MARQUIS-BOIRE *Google*

Morgan Marquis-Boire is a Security Engineer at Google on the Incident Response Team. He acts as a Technical Adviser at the Citizen Lab, Munk School of Global Affairs, University of Toronto and was one of the original organizers of the KiwiCON conference in New Zealand. In addition to talking about himself in the 3rd person and presenting at security conferences, he has spent time moon-lighting in such diverse fields as environmentalism and academia.

JUSTINE OSBORNE *iSEC Partners*

Justine Osborne is a Principal Security Consultant for iSEC Partners, an information security organization. At iSEC, Justine specializes in application security, focusing on web and mobile application penetration testing, code review, and secure coding guidelines. She also performs independent security research, and has presented at security conferences such as Black Hat, DEF CON, DeepSec, IT-Defense and SysScan. Her research interests include emerging web application technologies, dynamic vulnerability assessment tools, Rich Internet Applications (RIA), and mobile device security.

CHRIS PATTEN

Chris Patten performs penetration testing both day and night while researching new attack techniques. Chris has been participating in the security community for a number of years in various capacities. Only over the last year has his personal and professional interests aligned allowing for numerous opportunities to get back to the real passion with technology. Fortunately, Chris has the pleasure to currently work with some very talented individuals affording him the opportunity to consistently share penetration testing experiences.

ANDREW REITER *Veracode*

Andrew Reiter has been in someway involved with the security industry since the late 1990s. He has worked as a security researcher for Foundstone, BindView, and WebSense. Currently, he is working on the research team at Veracode. Andrew holds a BS and MS in Mathematics from UMASS-Amherst.

MAXIMILIANO SOLER

Maximiliano Soler lives in Buenos Aires, Argentina and currently works as Security Analyst, in a International Bank. Maxi has discovered vulnerabilities in different applications Web and Microsoft's products.

TOM STEELE *FishNet Security*

Tom Steele hails from Seattle Washington where he works as a Security Consultant at FishNet Security. The dynamic nature of his current role allows him to touch many areas of the offensive security spectrum. When not working he can be found gaming and creating tools to solve complex problems.

GREG WROBLEWSKI *Microsoft*

Greg Wroblewski, PhD, CISSP, is a senior security researcher at Microsoft's Trustworthy Computing Security group. Over the last 8 years he worked in many areas of security response, presenting part of his work at Black Hat 2007. At Microsoft he focuses on security problems in on-line services, detection of attacks and pentesting. In the past he was responsible for the technical side of patches in over 50 Patch Tuesday bulletins as well as hardening products like Windows and Office 2007. Recently he lead development effort to port ModSecurity module to IIS and nginx servers.

DAY ZERO BRIEFINGS

Tuesday, July 24 / Palace Ballroom III / 18:30-20:30

We've all been there. It is the night before the big show, you checked into the hotel, clothes put away, and maybe even a quick VPN back into the office to confirm that everything's not on fire. And now what?

Black Hat is pleased to announce the first ever Day Zero Briefings, a series of light-hearted and fun presentations. In addition to the briefings, drop by the Day Zero Lounge and have a bit of food and an adult beverage courtesy of Black Hat. The Lounge will also contain a gaming area powered by Microsoft and Xbox. Oh yes, there will be prizes.

18:30-18:50: Review Board Meet and Greet

Join the members of the Black Hat Review Board for an entertaining panel discussion. Ever wonder how the content was selected? Or which talks the Review Board Members are looking forward to? Come and join the discussion.

19:00-19:20: Collegiate Cyber Defense Competition: The Game

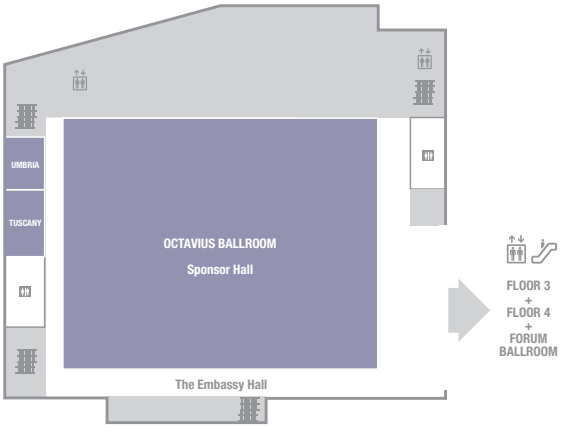
Representatives of the CCDC will be on hand to explain the first ever onsite Black Hat cyber challenge. Hop on the alternate SSID and join the fun. With prizes and bragging rights on the line, expect stiff competition.

19:30-20:30: My Arduino Can Beat Up Your Hotel Room Lock *by Cody Brocious*

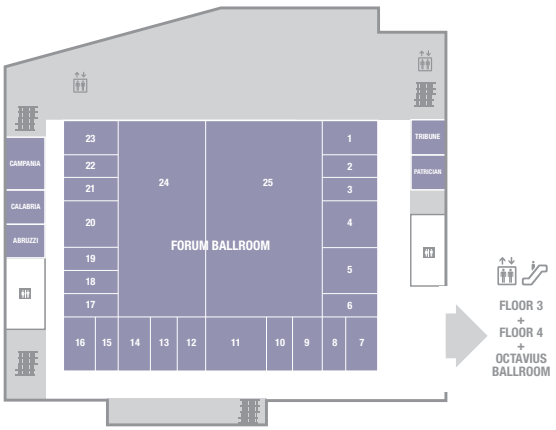
Nearly ten million Onity locks are installed in hotels worldwide, representing 1/3 of hotels and about 50% of hotel locks. This presentation will show, in detail, how they're designed and implemented. Then we will take a look at how they are insecure by design and release a number of critical, unpatchable vulnerabilities.

FLOOR PLAN

PROMENADE SOUTH



POOL LEVEL

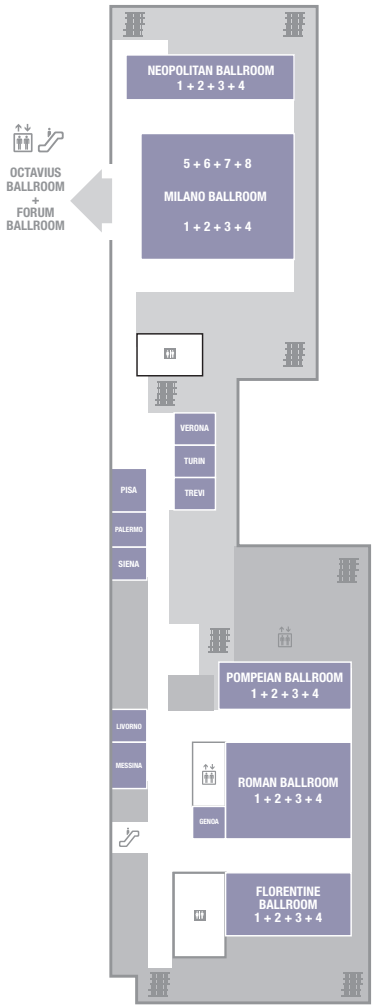


EMPERORS LEVEL

FLOOR 4

PROMENADE LEVEL

FLOOR 3



DAY 1 ONLY

DEFINING THE SCOPE	AUGUSTUS III + IV
UPPER LAYERS	AUGUSTUS I + II
LOWER LAYERS	AUGUSTUS V + VI
MOBILE—VINCENZO IOZZO	PALACE I
DEFENSE—SHAWN MOYER	PALACE II
BREAKING THINGS—CHRIS ROHLF	PALACE III
GNARLY PROBLEMS	ROMANS I-V
APPLIED WORKSHOP I	FLORENTINE
APPLIED WORKSHOP II	POMPEIAN

DAY 2 ONLY

BIG PICTURE	AUGUSTUS III + IV
WEB APPS—NATHAN HAMIEL	AUGUSTUS I + II
MALWARE—STEFANO ZANERO	AUGUSTUS V + VI
ENTERPRISE INTRIGUE	PALACE I
92.2% MARKET SHARE	PALACE II
OVER THE AIR AND IN THE DEVICE	PALACE III
MASS EFFECT	ROMANS I-IV
APPLIED WORKSHOP I	FLORENTINE
APPLIED WORKSHOP II	POMPEIAN

SPECIAL EVENTS

RECEPTION	OCTAVIUS BALLROOM
PWNIE AWARDS	AUGUSTUS III + IV

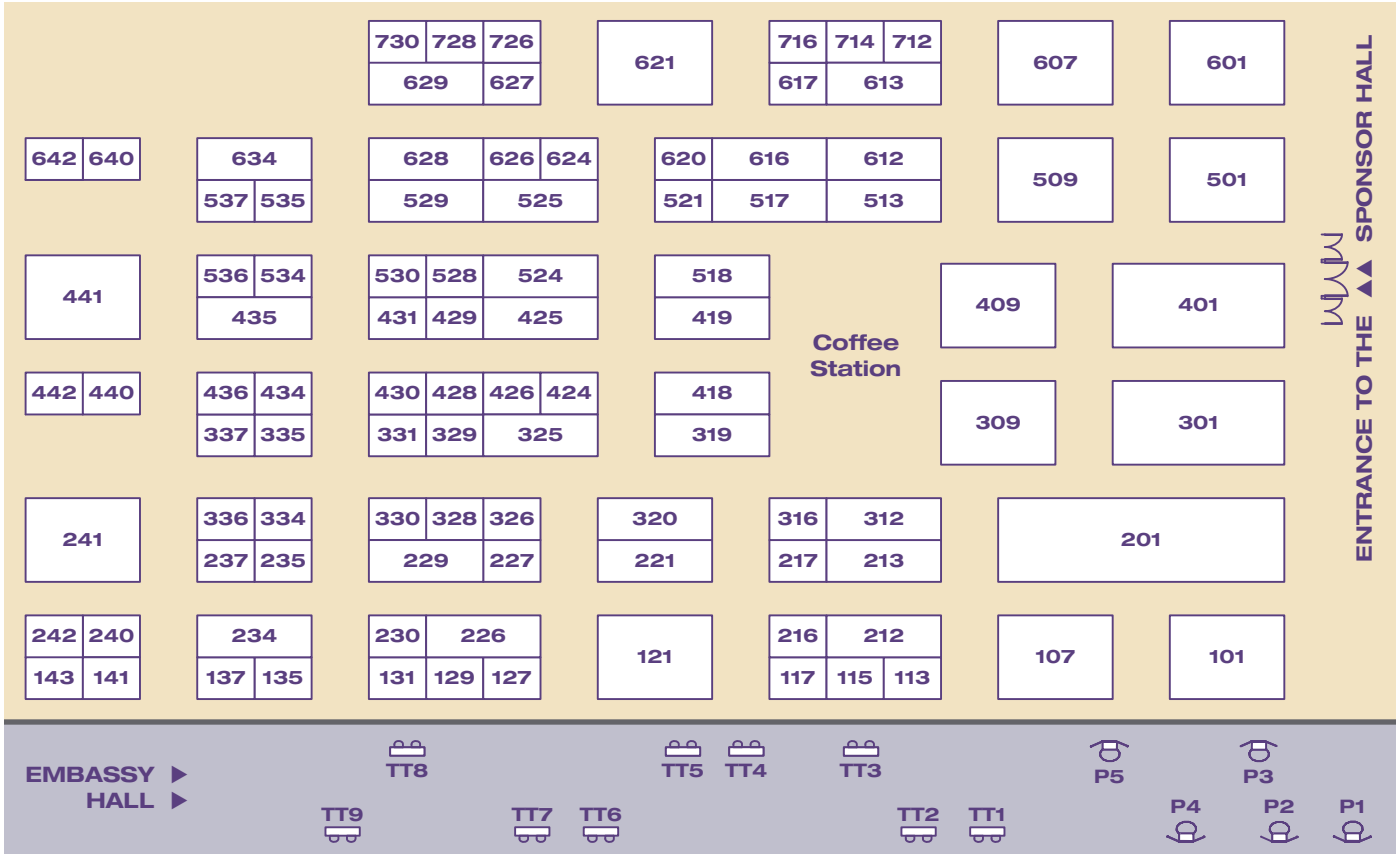
DAYS 1+2

BREAKFAST	OCTAVIUS BALLROOM
KEYNOTE	AUGUSTUS BALLROOM
LUNCH	FORUM BALLROOM
SPONSOR HALL	OCTAVIUS BALLROOM
EMBASSY HALL: MEDIA PARTNERS	OCTAVIUS FOYER
ARSENAL	AUGUSTUS FOYER

FLOOR PLAN: SPONSOR HALL

OCTAVIUS BALLROOM

Wednesday 7/25 08:00-19:30 – Thursday 7/26 08:00-17:00



SPONSOR BOOTH NUMBERS

AccessData Group 534
Accuvant LABS 107
AlienVault 442
Amazon.com 430
Barracuda Networks. 636
BeyondTrust. 629
Bit9, Inc. 331
Blue Coat Systems, Inc. 621
Booz Allen Hamilton 325
Cisco. 309
Click Security. 326
Codenomicon 328
Core Security Technology 409
Coverity. 728
Cybertap LLC. 521
Damballa Inc.. 620
Dell SecureWorks. 419
Dell SonicWALL 528
Emulex 141
ESET North America. 537
F5 Networks 127
Fidelis Security Systems. 616
FireEye 529
FireHost. 221
FireMon. 517
Fluke Networks 426
Foreground Security. 212
Forescout Technologies, Inc.. 513
Fortinet 640
GFI 613
Guidance Software. 113
GuruCul. 143
HBGary, Inc 428
HP Enterprise Security 312
IBM. 601
Imation Mobile Security 726
Immunity Inc.. 330
Imperva. 425
Lancope 336
Lieberman Software. 241
LogLogic, Inc 329
LogRhythm 607
Lookingglass Cyber Solutions . . . 501
Mandiant. 337
McAfee an Intel Company. 435
Microsoft Corporation. 301
MITRE–CVE/OVAL 216
Mocana. 227
Mykonos Software 441
nCircle 628
NCP Engineering 716
Neohapsis 115
Net Optics 617
Norman ASA 319
Onapsis, Inc. 316
OPSWAT 235
Oracle 135
Palo Alto Networks, Inc. 429
Parsons. 535
PhishMe.com. 712
Pico Computing 424
Qualys. 401
Radware 624
Rapid7 518
Red Lambda 117
RedSeal Networks 525
Research in Motion 335
Reversing Labs 131
RSA 201
RUNE 434
Saint Corp. 612
SecureNinja. 440
Securonix 129
Silicium Security 230
Silver Sponsor 334
Skybox Security 642
Solera Networks. 418
Sophos 137
Splunk. 320
SSH Communications Security . . 536
StillSecure 217
Stonesoft. 213
StrongAuth, Inc.. 240
Stroz Friedberg LLC 237
Symantec 101
TeleCommunication Systems Inc . 714
Tenable Network Security 431
The Hacker Academy 242
Trend Micro Incorporated 626
Tripwire 226
Trustwave 507
University of Maryland University College. 634
ValidEdge 627
Vasco Data Security 730
Venafi, Inc.. 530
Veracode. 229
Verizon 121
Vmware. 524
WatchGuard Technologies. 436
WhiteHat Security 234

EMBASSY HALL

Appthority P3
Carnegie Mellon University P1
ERPScan P4
Pwnie Express P2
yaSSL P5
Alta Associates Executive Women's Forum TT2
Cloud Security Alliance TT7
Denim TT1
Electronic Frontier Foundation. . . TT8
Federal Reserve Bank of SF TT3
Information Systems Security Association. TT4
LimitlessShot. TT9
OWASP Foundation TT5
UTSA-CCDC TT6

ARSENAL SCHEDULE

Day 1	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6	Pod 7
9:00	Keynote Speaker						
10:00	Break						
10:15	peepdf *by Jose Miguel Esparza*	HTExploit bypassing htaccess Restrictions *by Maximiliano Soler*	ThreadFix *by Dan Cornell*	Oyedata for OData Assessments *by Gursev Singh Kalra*	ice-hole 0.3 (beta) *by Darren Manners*	Registry Decoder *by Lodovico Marziale*	phpmap *by Matt Bergin*
11:15	Break						
11:45	Armitage *by Raphael Mudge*	OWASP Broken Web Applications Project *by Chuck Willis*	FakeNet *by Andrew Honig*	SAP Proxy *by Ian De Villiers*	ARPwner *by Nicolas Trippar*	Smartphone Pentesting Framework *by Georgia Weidman*	Generic Metasploit NTLM Relayer *by Rich Lundeen*
12:45	Lunch						
14:15	zCore IPS *by Itzhak (Zuk) Avraham*	Tenacious Diggity: New Google Hacking Diggity Suite Tools *by Francis Brown*	GDFuzz *by Rahul Sasi*	..cantor.dust.. *by Christopher Domas*	AWS Scout *by Jonathan Chittenden*	iSniff GPS *by Hubert Seiwert*	CrowdRE *by Georg Wicherski*
15:15	Break						
15:30	WATOBO: Web Application Toolbox *by Andreas Schmidt*	ModSecurity Open Source WAF *by Ryan Barnett*	LiME Forensics 1.1 *by Joe Sylve*	Semi-Automated iOS Rapid Assessment *by Justin Engler*	Vega *by David Mirza Ahmad*	Burp Extensibility Suite *by James Lester*	MAP *by Jerome Radcliffe*

Day 2	Pod 1	Pod 2	Pod 3	Pod 4	Pod 5	Pod 6	Pod 7
9:00	Keynote Speaker						
10:00	Break						
10:15	peepdf *by Jose Miguel Esparza*	ModSecurity Open Source WAF *by Ryan Barnett*	ThreadFix *by Dan Cornell*	Oyedata for OData Assessments *by Gursev Singh Kalra*	backfuzz *by Matías Choren*	CrowdRE *by Georg Wicherski*	phpmap *by Matt Bergin*
11:15	Break						
11:45	Armitage *by Raphael Mudge*	OWASP Broken Web Applications Project *by Chuck Willis*	FakeNet *by Andrew Honig*	bypassing Every CAPTCHA provider with clipcaptcha *by Gursev Singh Kalra*	Gsploit *by Gianni Gnesa*	Smartphone Pentesting Framework *by Georgia Weidman*	Generic Metasploit NTLM Relayer *by Rich Lundeen*
12:45	Lunch						
14:15	zCore IPS *by Itzhak (Zuk) Avraham*	Tenacious Diggity: New Google Hacking Diggity Suite Tools *by Francis Brown*	GDFuzz *by Rahul Sasi*	..cantor.dust.. *by Christopher Domas*	MIRV *by Konrads Smelkovs*	iSniff GPS *by Hubert Seiwert*	Redline *by Lucas Zaichkowsky*
15:15	Break						
15:30	Kautilya and Nishang *by Nikhil Mittal*	XMPPloit *by Luis Delgado*	LiME Forensics 1.1 *by Joe Sylve*	MAP *by Jerome Radcliffe*	Vega *by David Mirza Ahmad*	Burp Extensibility Suite *by James Lester*	Incident Response Analysis Visualization and Threat Clustering through Genomic Analysis *by Anup Ghosh*

Sponsored by

Back by popular demand, we are pleased to offer a Tool/ Demo area that will allow delegates to view and test open source community tools firsthand and have direct access to the developers of the tools.

PEEPDF

BY JOSE MIGUEL ESPARZA

S21sec

peepdf is a Python tool to explore PDF files in order to find out if the file can be harmful or not. The aim of this tool is to provide all the necessary components that a security researcher could need in a PDF analysis without using 3 or 4 tools to make all the tasks. It's included in BackTrack and REMnux.

Some of the peepdf features:

- It shows all the objects in the document, highlighting the suspicious elements and potential vulnerabilities.
- It supports all the most used filters and encodings.
- It can parse different versions of a file, object streams and encrypted documents.
- It provides Javascript and shellcode analysis wrappers, thanks to Spidermonkey and Libemu.
- It's able to create new PDF files and modify existent ones using obfuscation techniques.
- It's able to extract all the information easily thanks to its interactive console.

BIO: Jose Miguel Esparza is a security researcher and has been working as e-crime analyst at S21sec e-crime for more than 5 years, focused in botnets, malware and Internet fraud. Author of some exploits and analysis tools (http://eternal-todo.com/tools) like peepdf and Malybuzz, with which he has discovered vulnerabilities in several products. He is also a regular writer in the S21sec blogs (http://blog.s21sec.com and http://securityblog.s21sec.com) and http://eternal-todo.com about security and threats in Internet, and has taken part in several conferences, e.g. RootedCon (Spain), CARO Workshop (Czech Republic), Source Seattle (USA) and Black Hat (Netherlands).

HTEXPLOIT BYPASSING HTACCESS RESTRICTIONS

BY MAXIMILIANO SOLER

HTExploit is an open-source tool written in Python that exploits a weakness in the way that htaccess files can be configured to protect a web directory with an authentication process. By using this tool anyone would be able to list the contents of a directory protected this way, bypassing the authentication process.

Using HTExploit you will learn how to take advantage of weaknesses or miss-configurations in htaccess files, bypassing the authentication process. Download these protected files and proving against LFI, RFI and SQL Injection.

BIO: Maximiliano Soler lives in Buenos Aires, Argentina and currently works as Security Analyst, in a International Bank. Maxi has discovered vulnerabilities in different applications Web and Microsoft's products.

THREADFIX

BY DAN CORNELL

Denim Group

ThreadFix is an open source software vulnerability aggregation and management system that allows software security teams to reduce the time it takes to fix software vulnerabilities. ThreadFix imports the results from dynamic, static and manual testing to provide a centralized view of software security defects across development teams and projects. The system allows companies to correlate testing results and streamline software remediation efforts by simplifying feeds to software issue trackers. By auto generating web application firewall rules, this system also allows companies to protect vulnerable applications while remediation activities occur. ThreadFix empowers managers with vulnerability trending reports that demonstrate software security progress over time.

BIO: Dan Cornell has over fifteen years of experience architecting and developing web-based software systems. He leads Denim Group's security research team in investigating the application of secure coding and development techniques to improve web-based software development methodologies.

Dan was the founding coordinator and chairman for the Java Users Group of San Antonio (JUGSA) and currently serves as the OWASP San Antonio chapter leader, member of the OWASP Global Membership Committee and co-lead of the OWASP Open Review Project. Dan has spoken at such international conferences as RSA, OWASP AppSec USA, and OWASP EU Summit in Portugal.

OYEDATA FOR ODATA ASSESSMENTS

BY GURSEV SINGH KALRA

Foundstone, A Division of McAfee

OData is a new data access protocol that is being adopted by many major software manufacturers such as Microsoft, IBM, and SAP but hasn't been publically explored in terms of security. OData aims to provide a consistent access mechanism for data access from a variety of sources including but not limited to, relational databases, file systems, content management systems, and traditional web sites. I will be presenting and releasing a new tool that can be used to assess OData implementations. Tool features include:

1. Intuitive GUI based tool written in C#.
2. Ability to create attack templates from local and remote Service Documents and Service Metadata Documents.
3. Ability to generate attack templates for Creation of new Entries, updating existing Entries, Service Operation invocation, Entry deletion etc…
4. Ability to export attack templates in JSON and XML formats that can be fed to custom Fuzzers.
5. Support for XML and JSON data formats.
6. Ability to engage the OData services for manual testing.
7. Data generator for EDMSimpleType test data generation.
8. Ability to generate "Read URIs" for Entities, Entity Properties and Entity Property Values.
9. Ability to identify Keys, Nullable and Non-Nullable Properties and indicate the same in the attack templates.
10. Web proxy, HTTP and HTTPS support.

BIO: Gursev Singh Kalra serves as a Principal Consultant with Foundstone Professional Services, a division of McAfee. Gursev has done extensive security research on CAPTCHA schemes and implementations. He has written a Visual CAPTCHA Assessment tool TesserCap that was voted among the top ten web hacks of 2011. He has identified CAPTCHA implementation vulnerabilities like CAPTCHA Re-Riding Attack, CAPTCHA Fixation and CAPTCHA Rainbow tables among others. He is actively pursuing OData security research as well. He has also developed open source SSL Cipher enumeration tool SSLSmart and has spoken at conferences like ToorCon, OWASP, NullCon, Infosec Southwest and Clubhack.

ICE-HOLE 0.3 (BETA)

BY DARREN MANNERS

SyCom Technologies

Ice-hole is a java email phishing tool that identifies when a user has clicked on the link. It allows internal organizations to test their users social engineering defenses. The tool can be used in conjunction with various third party software like SET, Java Keystroke loggers and the BEEF framework to create real life social engineering attacks. Ice-Hole can also be used with training websites to not only capture when a user clicks on a link, but register when their training has been completed. A simple email phishing tool that can be expanded upon in multiple ways

BIO: 9 years Royal Naval Intelligence (Communication Technician (Analyst). Worked for 12 years in various security roles with VAR's and education. Certifications obtained include; SANS GSE (#42), CCIE sec (18929), OSCP, CISSP, and others. Written papers on iPhone backup files for penetration testing and anomaly detection using user agent headers. Designer of Sphere of Influence (security visualization tool) and Ice-hole. (email phishing tool)

REGISTRY DECODER

BY LODOVICO MARZIALE

Digital Forensics Solutions

The registry on Windows systems contain a tremendous wealth of forensic artifacts, including application executions, recently accessed files, application-specific passwords, removable device activity, search terms used and more. Existing registry analysis tools are poorly suited for investigations involving more than one machine (or even more that one registry file), for either registry acquisition or analysis. This problem is only exacerbated by the now-standard Volume Shadow Service, which makes available multiple historical copies of the registry by default. In order to make large scale investigations of

the registry feasible, we developed Registry Decoder, an open source tool for automated acquisitions and deep analysis of the large sets of Windows registry data. Registry Decoder includes powerful search functionality, activity timelining, plugin-based extensibility, a differencing engine and multi-format reporting. Since its release at Black Hat Vegas Arsenal 2011, it has been downloaded almost 10,000 times and has been nominated for the Computer Forensic Software Tool of the Year by Forensic 4cast. This year at Black Hat we plan to release Registry Decoder 2.0 which has a number of new features, including new plugins, better timelining, and huge performance enhancements.

BIO: Dr. Lodovico Marziale is a Senior Security Researcher at Digital Forensics Solutions, LLC, where he is responsible for conducting penetration tests, application security audits, and forensic investigations. He is also charged with engineering new applications to support security and forensics functions, performing training on incident response handling and digital forensics, and conducting research on cutting-edge techniques in computer security. He is active in the computer security research community and has numerous peer-reviewed publications, most emphasizing innovative, practical tools for computer security and digital forensics. Lodovico has designed and implemented several digital forensics and security applications, including co-developing the Scalpel file carver and Registry Decoder, a tool for automated acquisition and analysis of the Windows registry.

PHPMAP

BY MATT BERGIN
CORE Secuirty

Attempts to leverage the lack of input validation on the php eval() function in web applications.

ARMITAGE

BY RAPHAEL MUDGE
Strategic Cyber LLC

Armitage is a red team collaboration tool built on the open source Metasploit Framework. Released in December 2010, Armitage has seen constant updates and improvements since its inception—updates and improvements driven by feedback from its wonderful user community. This demonstration will show how Armitage works and dive into some of the lesser known features that are quite handy for penetration testers.

BIO: Raphael Mudge is the founder of Strategic Cyber LLC, a Washington, DC based company that creates software for red teams. He created Armitagefor Metasploit, the Sleep programming language, and the IRC client jIRCii. Previously, Raphael worked as a security researcher for the US Air Force, a penetration tester, and he even invented a grammar checker that was sold to Automattic. His work has appeared in Hakin9, USENIX ;login:, Dr. Dobb's Journal, on the cover of the Linux Journal, and the Fox sitcom Breaking In. Raphael regularly speaks on security topics and provides red team support to many cyber defense competitions.

OWASP BROKEN WEB APPLICATIONS PROJECT

BY CHUCK WILLIS
MANDIANT

The Open Web Application Security Project (OWASP) Broken Web Applications project (www.owaspbwa.org) provides a free and open source virtual machine loaded with web applications containing security vulnerabilities. This session will showcase the project and exhibit how it can be used for training, testing,

and experimentation by people in a variety of roles.

Demonstrations of the new 1.0 release will cover how the project can be used by penetration testers who discover and exploit web application vulnerabilities, by developers and others who prevent and defend against web application attacks, and by individuals who respond to web application incidents.

BIO: Chuck Willis is a Technical Director with MANDIANT, a full spectrum information security company in Alexandria, Virginia. At MANDIANT, Mr. Willis concentrates in several areas including application security, where he assesses the security of sensitive software applications through external testing and static analysis. He also studies static analysis tools and techniques and strives to identify better ways to evaluate and secure software. Mr. Willis is the leader of the OWASP Broken Web Applications project, which distributes a virtual machine with known vulnerable web applications for testing and training.

FAKENET

BY ANDREW HONIG

FakeNet is a tool that aids in the dynamic analysis of malicious software. The tool simulates a network so that malware interacting with a remote host continues to run allowing the analyst to observe the malware's network activity from within a safe environment. The tool is extremely light weight running inside the same virtual machine as the malware. This allows dynamic malware analysis without the burden of setting up multiple virtual machines. It supports HTTP, SSL, DNS, and several other protocols. The tool is extendable via Python extensions. It redirects all traffic to it's listeners on the localhost, including traffic to hard coded IP addresses. It creates output specific to the needs of a malware analyst. It also has the ability to create a packet capture from local traffic; something that's not possible with pcap based tools such as wireshark.

BIO: Andrew Honig is an independent security consultant and the co-author of Practical Malware Analysis. He spent eight years with the National Security Agency where he taught courses on software analysis, reverse-engineering, and Windows system programming at the National Cryptologic School. Andy discovered several zero-day exploits in VMware's virtualization products and has developed tools for detecting innovative malicious software, including malicious software in the kernel. An expert in analyzing and understanding both malicious and non-malicious software.

SAP PROXY

BY IAN DE VILLIERS

SensePost

The analysis and reverse engineering of SAP GUI network traffic has been the subject of numerous research projects in the past, and several methods have been available in the past for decoding SAP DIAG traffic. Until the release of SensePost's freely available proof of concept SAP DIAG tools (SAPProx and SApCap) in 2011, most methods were complicated and convoluted, or not in the public domain.

SAP is widely used and normally stores information of great sensitivity to companies. However, by default the communication protocol can be described as telnet-meets-gzip and Secure Network Communication (SNC) is not enabled in most organisations where SAP GUI is used. Furthermore, the protocol can be abused with relatively devastating effect against both server and client side components.

SensePost's tools for decoding and analysing SAP DIAG protocol has now been refined to a production ready, and offensive platform with scripting and fuzzing support. In addition, the toolset has been extended to include support for intercepting and decoding RFC-based communication.

BIO: Ian de Villiers is a security analyst at SensePost. Coming from a development background, his areas of expertise are in application and web application assessments. Ian has spent considerable time researching application frameworks, and has published a number of advisories relating to portal platforms. He has also provided security training and spoken at security conferences internationally.

ARPWNER

BY NICOLAS TRIPPAR

ARPwner is a tool to do arp poisoning and dns poisoning attacks, with a simple gui and a plugin system to do filtering of the information gathered, also has a implementation of sslstrip and is coded 100% in python, so you can modify on your needs

BIO: I'm independent security researcher based on vulnerability research and exploit development, I also program tools for fun.

SMARTPHONE PENTESTING FRAMEWORK

BY GEORGIA WEIDMAN

Bulb Security LLC

As smartphones enter the workplace, sharing the network and accessing sensitive data, it is crucial to be able to assess the security posture of these devices in much the same way we perform penetration tests on workstations and servers. However, smartphones have unique attack vectors that are not currently covered by available industry tools. The smartphone penetration testing framework, the result of a DARPA Cyber Fast Track project, aims to provide an open source toolkit that addresses the many facets of assessing the security posture of these devices. We will look at the functionality of the framework including information gathering, exploitation, social engineering, and post exploitation through both a traditional IP network and through the mobile modem, showing how this framework can be leveraged by security teams and penetration testers to gain an understanding of the security posture of the smartphones in an organization. We will also show how to use the framework through a command line console, a graphical user interface, and a smartphone based app. Demonstrations of the framework assessing multiple smartphone platforms will be shown.

BIO: Georgia Weidman is a penetration tester, security researcher, and trainer. She holds a Master of Science degree in computer science, secure software engineering, and information security as well as holding CISSP, CEH, NIST 4011, and OSCP certifications. Her work in the field of smartphone exploitation has been featured in print and on television internationally. She has presented her research at conferences around the world including Shmoocon, Hacker Halted, Security Zone, and Bsides. Georgia has delivered highly technical security training for conferences, schools, and corporate clients to excellent reviews. Building on her experience, Georgia recently founded Bulb Security LLC (http://www.bulbsecurity.com), a security consulting firm specializing in security assessments/penetration testing, security training, and research/development. She was awarded a DARPA Cyber Fast Track grant to continue her work in mobile device security.

GENERIC METASPLOIT NTLM RELAYER

BY RICH LUNDEEN

Microsoft

NTLM auth blobs contain the keys to the kingdom in most domain environments, and relaying these credentials is one of the most misunderstood and deadly attacks in a hacker's corporate arsenal. Even for smart defenders it's almost like a belief system; some people believe mixed mode IIS auth saves them, NTLMv2 is not exploitable, enabling the IIS extended protection setting is all you need, it was patched with MS08-068, you have to be in the middle, you have to visit a website, you have to be an administrator for the attack to matter, etc. etc.

http_ntlm_relay is a highly configurable Metasploit module I wrote that does several very cool things, allowing us to leverage the awesomeness of Metasploit and show the way for these non-believers:

- HTTP -> HTTP NTLM relay with POST, GET, HTTPS support.
- HTTP -> SMB NTLM relay with ENUM_SHARES, LS, WRITE, RM, and EXEC support. This extended support allows a lot of interesting attacks against non admins and multiple browsers that aren›t currently available in Metasploit.
- NTLMv2 support, which means that this attack now works a lot more often on modern windows environments.
- Mutex support allowing information from one request to be used in a future request. A simple example of this would be a GET to retrieve a CSRF token used in a POST. A more complex example would be an HTTP GET request to recover computer names, and then using that information to SMB relay to those computers for code execution.

It will be open source and I'll try my darndest to get it included in Metasploit proper before Black Hat.

BIO: Rich Lundeen graduated from Uofl with a Masters in CS, and is currently working for Microsoft where he does security research, penetration testing, code review, and tool development. He sometimes talks at conferences where he's usually a nervous

wreck, but he likes doing it anyway. He likes CTFs too, where he bangs his head against things until they break, or his head breaks.

ZCORE IPS

BY ITZHAK (ZUK) AVRAHAM

The awareness of cyber-espionage has increased significantly with recent malwares found, such as Stuxnet and Flame, and with the discovery of attacks, such as Aurora. A research published at DEF CON18 and BHDC showed that modern ARM architecture is not immune to vulnerabilities that are popular in X86 architecture. Hacking smartphones became common knowledge, and we've realized that it is only a matter of time until we will see the next Aurora on Smartphones. Hacking your computer has become harder with time and multiple versions so the attackers seek additional entry-points to your organization and your Smartphone, with features like VPN access being the perfect target!

We will go through modern government-grade attacks on smartphones and will prove that the same smartphone you are carrying with you today can act as a spying-machine that will reveal all of your secrets and data to your enemies.

The next step of the attackers will be finding a way into your internal network or other key-people at your organization, using the same infection routine.

Smartphones hacking has increased significantly as more researched have adopted this new technology. We will cover recent attacks and threats that are being discovered every-day that puts us at risk!

We will show and demonstrate several attack vectors that are being used today against targeted devices and how we're preventing those attacks using zCore IPS, our comprehensive Mobile IPS solution. This solution has been specially built for Smartphones with zMitigaion™, a highly effective technology for 0day protection offered to those who face targeted and government-grade attacks on Smartphones.

BIO: Itzhak "Zuk" Avraham is a Security Expert who has been engaged on a wide variety of vulnerability assessments. Zuk worked at the IDF as a Security Researcher and has also published a technique on shellcoding for modern ARM exploits. As the proud founder of the Mobile-Security company, Zimperium, and the Godfather of ANTI (Android Network Tollkit), Zuk is diligently working on the next big breakthrough in mobile security. Zuk is the proud holder of a SVC card, which is only in the possession of elite researchers such as Matt Swich. Zuk really dislikes writing about himself in the third person so for more information you can check out his personal hacking related blog at http://imthezuk.blogspot.com and on Twitter as @ihackbanme.

TENACIOUS DIGGITY: WNEW GOOGLE HACKING DIGGITY SUITE TOOLS

BY FRANCIS BROWN

Stach & Liu

All brand new tool additions to the Google Hacking Diggity Project—The Next Generation Search Engine Hacking Arsenal. As always, all tools are free for download and use.

When last we saw our heroes, the Diggity Duo had demonstrated how search engine hacking could be used to take over someone's Amazon cloud in less than 30 seconds, build out an attack profile of the Chinese government's external networks, and even download all of an organization's Internet facing documents and mine them for passwords and

Dev ♥ Security

(Ok, maybe not yet.)

Let us show you how.

Learn how Coverity has helped 1,100 companies including SAP, Juniper Networks, LG, and Emerson effectively build security into development.

Visit us at booth #728

Enter to Win Soul by Ludacris Headphones.

coverity®

www.coverity.com

secrets. Google and Bing were forced to hug it out, as their services were seamlessly combined to identify which of the most popular websites on the Internet were unwittingly being used as malware distribution platforms against their own end-users.

Now, we've traveled through space and time, my friend, to rock this house again…

True to form, the legendary duo have toiled night and day in the studio (a one room apartment with no air conditioning) to bring you an entirely new search engine hacking tool arsenal that's packed with so much tiger blood and awesome-sauce, that it's banned on 6 continents. Many of these new Diggity tools are also fueled by the power of the cloud and provide you with vulnerability data faster and easier than ever thanks to the convenience of mobile applications. Just a few highlights of new tools to be unveiled are:

- AlertDiggityDB—For several years, we've collected vulnerability details and sensitive information disclosures from thousands of real-time RSS feeds setup to monitor Google, Bing, SHODAN, and various other search engines. We consolidated this information into a single database, the AlertDiggityDB, forming the largest consolidated repository of live vulnerabilities on the Internet. Now it's available to you.
- Diggity Dashboard—An executive dashboard of all of our vulnerability data collected from search engines. Customize charts and graphs to create tailored views of the data, giving you the insight necessary to secure your own systems. This web portal provides users with direct access to the most current version of the AlertDiggityDB.
- Bing Hacking Database (BHDB) 2.0—Exploiting recent API changes and undocumented features within Bing, we've been able to completely overcome the previous Bing hacking limitations to create an entirely new BHDB that will make Bing hacking just as effective as Google hacking (if not more so) for uncovering vulnerabilities and data leaks on the web. This also will include an entirely new SharePoint Bing Hacking database, containing attack strings targeting Microsoft SharePoint deployments via Bing.
- NotInMyBackYardDiggity—Don't be the last to know if LulzSec or Anonymous post data dumps of your company's passwords on PasteBin.com, or if a reckless employee shares an Excel spreadsheet with all of your customer data on a public website. This tool leverages both Google and Bing, and comes with pre-built queries that make it easy for users to find sensitive data leaks related to their organizations that exist on 3rd party sites, such as PasteBin, YouTube, and Twitter. Uncover data leaks in documents on popular cloud storage sites like Dropbox, Microsoft SkyDrive, and Google Docs. A must have for organizations that have sensitive data leaks on domains they don't control or operate.
- PortScanDiggity—How would you like to get Google to do your port scanning for you? Using undocumented functionality within Google, we've been able to turn Google into an extremely effective network port scanning tool. You can provide domains, hostnames, and even IP address ranges to scan in order to identify open ports ranging across all 65,535 TCP ports. An additional benefit is that this port scanning is completely passive—no need to directly communicate with target networks since Google has already performed the scanning for you.
- CloudDiggity Data Mining Tool Suite—Ever wanted to data mine every single password, email, SSN, credit card number on the Internet? Our new cloud tools combine Google/Bing hacking and data loss prevention (DLP) scanning on a massive scale, made possible via the power of cloud computing. Chuck Norris approved.
- CodeSearchDiggity-Cloud Edition—Google recently shut down Code Search in favor of focusing on Google+, putting "more wood behind fewer arrows". I suppose we could have let the matter go, and let CodeSearchDiggity die, but that would be the mature thing to do. Instead, we are harnessing the power of the cloud to keep the dream alive—i.e. performing source code security analysis of nearly every single open source code project in existence, simultaneously.
- BingBinaryMalwareSearch (BBMS)—According to the Verizon 2012 DBIR, malware was used to compromise a staggering 95% of all records breached for 2011. BBMS allows users to proactively track down and block sites distributing malware executables on the web. The tool leverages Bing, which indexes executable files, to find malware based on executable file signatures (e.g. "Time Stamp Date:", "Size of Code:", and "Entry Point:").
- Diggity IDS—Redesigned intrusion detection system (IDS) for search engine hacking. Will still leverage the wealth of information provided by the various Diggity Alert RSS feeds, but will also make more granular data slicing and dicing possible through new and improved client tools. Also includes the frequently requested SMS/email alerting capabilities, making it easier than ever for users to keep tabs on their vulnerability exposure via search engines.

BIO: Francis Brown, CISA, CISSP, MCSE, is a Managing Partner at Stach & Liu, a security consulting firm providing IT security services to the Fortune 500 and global financial institutions as well as U.S. and foreign governments. Before joining Stach & Liu, Francis served as an IT Security Specialist with the Global Risk Assessment team of Honeywell International where he performed network and application penetration testing, product security evaluations, incident response, and risk assessments of critical infrastructure. Prior to that, Francis was a consultant with the Ernst & Young Advanced Security Centers and conducted network, application, wireless, and remote access penetration tests for Fortune 500 clients.

Francis has presented his research at leading conferences such as Black Hat USA, DEF CON, InfoSec World, ToorCon, and HackCon and has been cited in numerous industry and academic publications.

Francis holds a Bachelor of Science and Engineering from the University of Pennsylvania with a major in Computer Science and Engineering and a minor in Psychology. While at Penn, Francis taught operating system implementation, C programming, and participated in DARPA-funded research into advanced intrusion prevention system techniques.

GDFUZZ

BY RAHUL SASI
iSIGHT partners

PHP Framework is built in native C and the no of memory corruptions and chances of code executions in the frame work is high. PHP framework takes inputs form web applications and process it on the web server. There are a lot of image processing functions in PHP where user controls the input "Images" . The usage of image processing functions could be detected via the metadata they insert in the images.

We would be demonstrating a cool fuzzer [GDFuzz] that is specifically made capable to Fuzzing PHP GD Engine. Its basically an image Fuzzer which we have build from scratch. It's uniqueness is it's ability to handle PHP Framework and fuzz reveal PHP script engine [GDI] bugs.

We would be demonstrating our tool along with many Stack ,Heap corruptions revealed by our Fuzzer , that could get attacker Code execution on the Webserver via crafted Images. With few changes in the tool it could be used to Fuzz browsers, Windows system or anything that renders an image.

The tool would be of intrest to Wep App Enthusiast and Vulnerability Researchers .

BIO: Rahul(fb1h2s) is working as an Info Security Researcher for iSIGHT partners. He has responsibly disclosed vulnerabilities/Bugs to Google, Apache, Banking sectors and many IT giants. Rahul has authored articles and spoken at Clubhack, Cocon(2011), Nullcon(2011,2012), HITB(2012) and Black Hat(2012). His work could be found at www.Garage4Hackers.com.

REGISTRY DECODER

BY LODOVICO MARZIALE
Digital Forensics Solutions

The registry on Windows systems contain a tremendous wealth of forensic artifacts, including application executions, recently accessed files, application-specific passwords, removable device activity, search terms used and more. Existing registry analysis tools are poorly suited for investigations involving more than one machine (or even more that one registry file), for either registry acquisition or analysis. This problem is only exacerbated by the now-standard Volume Shadow Service, which makes available multiple historical copies of the registry by default. In order to make large scale investigations of the registry feasible, we developed Registry Decoder, an open source tool for automated acquisitions and deep analysis of the large sets of Windows registry data. Registry Decoder includes powerful

search functionality, activity timelining, plugin-based extensibility, a differencing engine and multi-format reporting. Since its release at Black Hat Vegas Arsenal 2011, it has been downloaded almost 10,000 times and has been nominated for the Computer Forensic Software Tool of the Year by Forensic 4cast. This year at Black Hat we plan to release Registry Decoder 2.0 which has a number of new features, including new plugins, better timelining, and huge performance enhancements.

BIO: Dr. Lodovico Marziale is a Senior Security Researcher at Digital Forensics Solutions, LLC, where he is responsible for conducting penetration tests, application security audits, and forensic investigations. He is also charged with engineering new applications to support security and forensics functions, performing training on incident response handling and digital forensics, and conducting research on cutting-edge techniques in computer security. He is active in the computer security research community and has numerous peer-reviewed publications, most emphasizing innovative, practical tools for computer security and digital forensics. Lodovico has designed and implemented several digital forensics and security applications, including co-developing the Scalpel file carver and Registry Decoder, a tool for automated acquisition and analysis of the Windows registry.

AWS SCOUT

BY JONATHAN CHITTENDEN

iSEC Partners

The scale and variety of Amazon Web Servers (AWS) has created a constantly changing landscape. What was previously managed by enterprise IT groups is now done through a variety of Amazon-based services, leaving many questions concerning the risk and security of these environments unanswered. This presentation will discuss the most common mistakes that we have seen in the field and show you how to audit them using AWS Scout.

Scout is a security tool that lets AWS administrators make an assessment of their environments security posture. Using the AWS API, we can gather configuration data for manual inspection or highlight high-risk areas automatically. Rather than pouring through dozens of pages on the web, we can get an clear view of the attack surface.

BIO: During his employment with iSEC Partners, Jonathan has been tasked with a variety of engagements. Of which his memorable projects include, code reviewing custom kernel modules to be used for virtualization and reviewing both public and private cloud architectures. Outside of project work, Jonathan is in the process of writing a cloud security book to be published by McGraw-Hill in 2012.

Prior to his employment with iSEC, Jonathan worked for the Air Force as a civilian. His roles consisted of reverse engineering malware for both signature development. During this time, he also assisted in the development of an open-source intelligence application to be used to identify indicators of compromise.

ISNIFF GPS

BY HUBERT SEIWERT

iSniff GPS performs passive wireless sniffing to identify nearby iPhones and iPads.

Data disclosed by all iDevices when they connect to WiFi networks is used to track where each device has recently been. Each device's recent locations and other information is displayed on a live-updated map. There will be a live demonstration at Black Hat Arsenal.

iSniff GPS is a combination of a commandline tool and web application written in Python. A turnkey Linux VM image containing the complete tool ready to run will be made available at Black Hat, with source code to be published on Github.

References: http://arstechnica.com/apple/2012/03/anatomy-of-an-iphone-leak

BIO: Hubert is an experienced penetration tester and security consultant with more than 5 years industry experience in the UK and Australia. His main interests are web and mobile application security. He has given talks on iPhone security at Ruxmon and presented an iPhone SSL man-in-the-middle tool at the CCC Conference in 2011.

CROWDRE

BY GEORG WICHERSK

CrowdStrike

Reversing complex software quickly is challenging due to the lack of professional tools that support collaborative analysis. The CrowdRE project aims to fill this gap. Rather than using a live distribution of changes to all clients, which has proven to fail in the past, it leverages from the architecture that is being used with success to organize source code repositories: a system that manages a history of changesets as commit messages. The central component is a cloud based server that keeps track of commits in a database. Each commit covers one or more functions of an analyzed binary and contains information like annotations, comments, prototype, struct and enum definitions and the like. Clients can search the database for commits of functions by constructing a query of the analyzed binary's hash and the function offset. Different concurring commits for a function are possible; in such cases it is up to the user to decide which commit is better.

This basic concept is sufficient for a collaborative workflow on a per-function basis for a shared binary. One exciting feature is a similarity hashing scheme that considers the basic block boundaries of a function. Each function is mapped on a similarity preserving hash of fixed size. A database query for such a functions similarity hash returns a set of functions sorted by their similarity value, and the analyst can choose amongst them. This is extremely helpful when analyzing variants based on the same code or generations of a malware family, for example.

The CrowdRE client is now freely available as an IDA Pro plugin. CrowdStrike maintains a central cloud for the community to share their commits amongst each other. It is our goal to help building a public database of known, well annotated functions to speed up the analysis of standard components, somewhat similar to what BinCrowd (which is offline nowadays) offered but with support for multiple co-existing commits for the same function. We also supports list-based commit visibility to give users control over who else can see and import their contributions. In the coming days we will release a series of how-to blog posts and videos to speed up adoption of CrowdRE.

BIO: Georg Wicherski is a Senior Security Researcher with CrowdStrike, mostly analyzing advanced targeted threats but also putting himself in attackers' shoes from time to time. He loves to work on a low level, abandoning all syntactic sugar that HLL offer and working on instructions or bytecode. Recently, he has developed an interest for the ARM architecture in addition to his old x86 adventures.

WATOBO: WEB APPLICATION TOOLBOX

BY ANDREAS SCHMIDT

Siberas

Doing manual penetration tests on web applications is time-consuming and can be very boring or even frustrating. On the other hand, if you use an automated tool you often don't know if or how things have been checked because there's too much "Voodoo" under the hood.

Each approach has its advantages and disadvantages but the selection of tools which merge both worlds is very limited.

In this presentation I will introduce WATBO (Web Application Toolbox) which closes the gap and combines the advantages of both, the manual and the automated approach to web application assessments. WATOBO works like a local proxy and is analyzing the traffic on the fly for helpful information and vulnerabilities. It also has automated scanning capabilities, e.g. SQL-Injection, XSS-Checks and more. It can handle of One-Time-Tokens (aka Anti-CSRF-Tokens) and has powerfull session management capabilities.

WATOBO is written in (FX)Ruby and was initially released in May 2010 as an open source project on SourceForge (http://watobo.sourceforge.net).

BIO: Andreas Schmidt started working as a security consultant in 1998. At the beginning he was involved with planning and implementing high security infrastructures. Later on he focused on security audits and penetrationtests. He also developed and held hands-on hacking trainings focused on Windows and Unix systems. Andreas is Co-Founder of the german security consulting company siberas (http://www.siberas.de) and author of WATOBO.

MODSECURITY OPEN SOURCE WAF

BY RYAN BARNETT

SpiderLabs

ModSecurity is already the most widely deployed WAF in existence protecting millions of web sites, but we are now also announcing that we have ported the module to both the Microsoft IIS and Nginx platforms. These ports will allow you to run ModSecurity natively

within the web servers you want to protect. Come to this demo to see the latest new features recently added to ModSecurity including crypto/hashing protections.

BIO: Ryan Barnett joined SpiderLabs after a decade in web security. He currently leads the web server security research team which specializes in web application defense. Barnett is renowned in the industry for his unique web operational security expertise. He has serves as the Open Web Application Security Project (OWASP) ModSecurity Core Rule Set Project Leader and Project Contributor on the OWASP Top Ten and AppSensor Projects. He is a Web Application Security Consortium (WASC) Board Member and Project Leader for the Web Hacking Incident Database (WHID) and the Distributed Web Honeypot Projects. He is also a Certified Instructor at the SANS Institute. Barnett is regularly consulted by industry news outlets like Dark Reading, SC Magazine and Information Week. He is the author of Preventing Web Attacks with Apache (Addison-Wesley Professional, 2006.) Key industry events he has addressed include Black Hat, SANS AppSec Summit and the OWASP Global Summit.

LIME FORENSICS 1.1

BY JOE SYLVE DIGITAL

Forensics Solutions

LiME (formerly DMD) is a Loadable Kernel Module (LKM), which allows the acquisition of volatile memory from Linux and Linux-based devices, such as those powered by Android. The tool supports acquiring memory either to the file system of the device or over the network. LiME is unique in that it is the first tool that allows full memory captures from Android devices. It also minimizes its interaction between user and kernel space processes during acquisition, which allows it to produce memory captures that are more forensically sound than those of other tools designed for Linux memory acquisition.

BIO: Joe Sylve is a senior security researcher at Digital Forensics Solutions, where he conducts forensic investigations and penetration tests, performs training on incident response handling and digital forensics, and researches cutting edge technologies in computer security and digital forensics. He is the author of LiME Forensics, the first tool set that allows full physical memory acquisition from Android devices, and has presented this work on Android memory acquisition and analysis at Shmoocon 2012 and the SANS Digital Forensic and Incident Response Summit. He holds a M.S. In Computer Science, with a concentration in Information Assurance, from the University of New Orleans and is also a GIAC Certified Forensic Analyst.

SEMI-AUTOMATED IOS RAPID ASSESSMENT

BY JUSTIN ENGLER

FishNet Security

Apple's AppStore continues to grow in popularity, and iOS devices continue to have a high perception of security from both users and experts. However, applications on the AppStore often have security or privacy flaws that are not apparent, even to sophisticated users. Security experts can find these flaws via manual tests, but the enormity of the AppStore ensures that only a small minority of apps could ever be manually tested.

This presentation will demonstrate a new tool and methodology to perform automated or semi-automated assessment of iOS applications and assist with manual testing.

BIO: Justin Engler is a Senior Security Consultant for FishNet Security's Application Security practice. His focus is on the security of web applications, mobile devices, web-backed thick clients, databases, and industrial control systems. Justin has previously spoken at Black Hat USA and DEF CON.

VEGA

BY DAVID MIRZA AHMA

Subgraph

Vega is a GUI-based, multi-platform, free and open source web security scanner that can be used to find instances of SQL injection, cross-site scripting (XSS), and other vulnerabilities in your web applications. Vega also includes an intercepting proxy for interactive web application debugging. Vega attack modules are written in Javascript, users can easily modify them or write their own. The Vega web vulnerability scanner runs on Linux, Windows, and OS X.

Vega can be downloaded from our website, http://www.subgraph.com.

BIO: David has over 10 years in the information security business. He started his professional experience as a founding member of Security Focus, which was acquired by Symantec in 2002. David also moderated the Bugtraq mailing list, a historically important forum for discussion of security vulnerabilities, for over four years. He has spoken at Black Hat, Can Sec West, AusCERT and numerous other security conferences, as well as made contributions to books, magazines and other publications. David also participated in a NIAC working group on behalf of Symantec to develop the first version of the CVSS (Common Vulnerability Scoring System) model and served as editor for the Attack Trends section of IEEE Security & Privacy for over three years. His current obsession is building Subgraph, a Montreal-based open source security startup.

BURP EXTENSIBILITY SUITE

BY JAMES LESTER

IOActive

Whether it be several Class B Subnets, a custom Web Application utilizing tokenization, or the integration of 3rd party detection/exploitation software, there comes a time when your go-to testing application is not sufficient as is. With Burp Suite Extensibility you can push these requirements to the next level by building functionality that allows you to perform your required task, maintaining efficiency, value, and most of all, detection/exploitation of the specified target. Several Extensions along with a common extensibility framework will be on display demonstrating its ability, adaptation, and ease of use while overall being able to reach your testing requirements. Along with the demonstration, these extensions will be released to the public during the week of Black Hat to encourage further development and extensibility participation.

BIO: As a Senior Security Consultant at IOActive, James Lester works with platinum-level clients on network and application penetration tests, PCI compliance, and general consulting engagements. Before joining the IOActive team with the goal of taking his talents to the next level, he was a Senior Security Analyst with the McAfee Corporation. Passionate about Internet security and privacy, James enjoys designing new procedures and methods to Identify, test, secure, and mitigate compromised and high-risk websites. He has previously been a featured speaker at many local security chapter roundups and Internal Corporate Security events.

MAP

BY JEROME RADCLIFFE

Smart Device Threat Center for Mocana

With MAP, enterprise apps can be wrapped post-development, so there is no code to write: just point and click to add new security features to any app. All that is needed is the binary file of the app (.apk for Android and .ipa for Apple iOS) to be loaded into

the Mocana MAP server on-premise in the enterprise datacenter, or to a secure cloud-based environment in the near future. There is no need to have access to the original source code, no need for an SDK, and no need for a separate agent on the device.

The resulting Self Defending App™ can then be made available through any app catalog or private app store the enterprise chooses. And MAP is totally transparent to end users, with no need for separate client-side software or agents. Newly-secured apps work like users expect them to. MAP protects corporate data without compromising the user experience, while alternative technologies restrict end users to a tiny selection of unfamiliar apps, or confine their apps in "walled" environments or virtual machines.

BIO: Jay Radcliffe has been working in the computer security field for over twelve years and is currently the Director for the Smart Device Threat Center for Mocana. He has an extensive public speaking background, going back to middle school, and has spoken on a variety of security and legal topics at major conferences, universities, and other community events. He holds a Masters degree in Information Security Engineering form SANS Technology Institute as well as a bachelor's degree in Criminal Justice/Pre-Law from Wayne State University. His experience with radios and hardware goes back to when he was 12 and earned his Ham Radio license, now with the callsign N8OS.

KAUTILYA AND NISHANG

BY NIKHIL MITTAL

Kautilya is a toolkit and framework which allows usage of USB Human Interface Devices in Penetration Tests. The toolkit contains useful payloads and modules which could be used at different stages of a Penetration Test. Kautilya is tested with Teensy++ device but could be used with most of the HIDs. It has been successfully tested for breaking into Windows 7, Ubuntu11 and Mac OS X Lion.

Nishang is a framework and collection of scripts and payloads which enables usage of PowerShell for offensive security and post exploitation. The scripts are written on the basis of requirement by the author during real Penetration Tests. It contains many interesting scripts like download and execute, keylogger, password hash dumper, time based payload and much more.

BIO: Nikhil Mittal is a hacker, info sec researcher and enthusiast. His area of interest includes penetration testing, attack research, defence strategies and post exploitation research. He has many years of experience in Penetration Testing of many Government Organizations of India and other global corporate giants.

He specializes in assessing security risks at secure environments which require novel attack vectors and "out of the box" approach. He has worked extensively on using HID in Penetration Tests and powershell for post exploitation. He is creator of Kautilya, a toolkit which makes it easy to use Teensy in penetration tests. In his free time, Nikhil likes to scan full IP ranges of countries for specific vulnerabilities, does some vulnerability research and works on his projects. He has spoken/trained at Clubhack'10, Hackfest'11, Clubhack'11, Black Hat Abu Dhabi'11, Troopers'12, PHDays'12, GrrCon'12 and Black Hat Europe'12.

XMPPLOIT

BY LUIS DELGADO

XMPPloit is a command-line tool to attack XMPP connections, allowing the attacker to place a gateway between the client and the server and perform different attacks on the client stream.

The tool exploit, implementation vulnerabilities at the client&server side and XMPP protocol.

The main goal is that all the process is transparently for the user and never replace any certificate (like HTTPS attacks).

Some features are:

- Downgrade the authentication mechanism (can obtain the user credentials)
- Force the client not to use an encrypted communication
- Set filters for traffic manipulation

Filters that have been implemented in this version for Google Talk are:

- Read all the the user's account mails
- Read and modify all the user's account contacts (being or not in the roster).

A preliminary version was described in my talk 'XMPP, more than chat' (http://slidesha.re/GWBwMF) presented in RootedCON 2012 (Spain).

BIO: Luis Delgado is a security researcher focused on Web&IM security, wireless protocols and android security&development. He is a regular writer on Security by Default (http://www.securitybydefault.com), one of the most important spanish security blogs and has published many vulnerabilities and research papers that have ranged from messaging protocols security to the Android market security measures. Author of WIFI Auditor (http://www.ldelgado.es/?wifiauditor), a wireless security analyzer with more than 800K downloads. He works as a freelance auditor for customers in the defense sector and important ISPs.

BYPASSING EVERY CAPTCHA PROVIDER WITH CLIPCAPTCHA

BY GURSEV SINGH KALRA

Foundstone

reCAPTCHA and other CAPTCHA service providers validate millions of CAPTCHAs each day and protect thousands of websites against the intertube bots. A secure CAPTCHA generation and validation ecosystem forms the basis of the mutual trust model and large scale damage can happen if any component of this ecosystem is compromised.

The presentation explains third party CAPTCHA provider integration and explains vulnerabilities that affect almost every CAPTCHA provider including reCAPTCHA. These vulnerabilities can be exploited to completely bypass the protection offered by CAPTCHA providers. A new signature based tool clipcaptcha will be introduced and released that can be used to exploit these vulnerablities to bypass CAPTHCA provider protection. clipcaptcha's operational modes will be demonstrated. The operational modes include the following three mondes among others:

1. Avalanche Mode: All CAPTCHA validation requests are approved.
2. Stealth Mode: Only attacker provided CAPTCHAs are approved.
3. DoS Mode: All CAPTCHA validation requests are denied.

Demonstrations will explain these modes along with live CAPTCHA provider bypass on the test server.

BIO: Gursev Singh Kalra serves as a Principal Consultant with Foundstone Professional Services, a division of McAfee. Gursev has done extensive security research on CAPTCHA schemes and implementations. He has written a Visual CAPTCHA Assessment tool TesserCap that was voted among the top ten web hacks of 2011. He has identified CAPTCHA implementation vulnerabilities like CAPTCHA Re-Riding Attack, CAPTCHA Fixation and CAPTCHA Rainbow

tables among others. He is actively pursuing OData security research as well. He has also developed open source SSL Cipher enumeration tool SSLSmart and has spoken at conferences like ToorCon, OWASP, NullCon, Infosec Southwest and Clubhack.

..CANTOR.DUST..

BY CHRISTOPHER DOMAS

..cantor.dust.. is an interactive binary visualization tool, a radical evolution of the traditional hex editor. By translating binary information to a visual abstraction, reverse engineers and forensic analysts can sift through mountains of arbitrary data in seconds. Even previously unseen instruction sets and data formats can be easily located and understood through their visual fingerprint. ..cantor.dust.. dramatically accelerates the analysis process, and, for the experienced user, forms an indispensable tool in the reverser's arsenal.

BIO: Chris is an embedded systems engineer and cyber security researcher, focused on low level hardware and software RE and exploitation.

BACKFUZZ

BY MATÍAS CHOREN

backfuzz is a fuzzing tool for different protocols (FTP, HTTP, IMAP, etc) written in Python.

The general idea is that this script has several predefined functions, so whoever wants to write their own plugin's (for another protocol) can do that in few lines.

BIO: Independent Security Researcher & System Engineer Student at Buenos Aires, Argentina.

GSPLOIT

BY GIANNI GNESA

Ptrace Security

Gsploit is a scriptable penetration testing framework written in Python that not only provides a simple platform to launch multi-stage / multi-vector attacks, but also provides a rich set of functions to develop exploits for several different architectures.

This tool is particularly useful for penetration testers and vulnerability researchers who need to quickly turn a Proof-of-Concept (PoC) into a working exploit that can be subsequently used in a real penetration test.

BIO: Gianni Gnesa is a Malware Analyst at Ptrace Security. He has been working in the information security industry for over 6 years and has been focused on exploit development and penetration testing. In his spare time, he likes to find and exploit vulnerabilities in Web browser and interpreted languages, such as Java and PHP.

MIRV

BY KONRADS SMELKOVS KPMG

MIRV (Metasploit's Incident Response Vehicle) is a new tool (based on Metasploit's meterpreter) which was created to address the perceived shortcomings in existing host-based incident response tools: they do not operate on large amounts of nodes, are difficult to get past change advisory boards that grant approval for deployment, are not stealthy and do not have the ability to be safely extended.

MIRV's main design feature are the embedded Lua micro-agents to monitor various system activity events and the ability to act on those events using the full flexibility and most importantly—safety of Lua.

It also revives the discussion of active defence—not just alarms, but traps: can the defender use the attacker's connection to obtain some information about the attacker's system, or even attack the attacker's system? An example based on terminal services shared drive feature is presented. MIRV's features can also be used for offence as a flexible rootkit and some examples are given.

Paper: https://docs.google.com/document/d/1cCD6fAnMpfltchPbfreWgIZxzI87F4lt2E5RjWV0OqU/edit; Video: http://youtu.be/teMgpW3hAuk

BIO: My name is Konrads Smelkovs and I am a security consultant within KPMG's Information Protection practice in London, UK where I practice the arts of attacking web application and network security as well as defence—incident response and malware reverse engineering. At the moment I believe that defending is more intellectually stimulating than attacking, albeit the rush from getting root is never getting old. My research is focused on how to help defenders to fight back. Previous speaking engagements include CRESTCon and ISF Nordic spring.

REDLINE

BY LUCAS ZAICHKOWSKY

MANDIANT

Redline is free utility from Mandiant that makes both experienced and entry-level incident responders faster and more efficient. Using Redline, responders can perform a guided investigation of possibly compromised systems.

The updated version 1.5 of Redline includes new features and enhancements to existing capabilities, including:

- Improved Analysis Capabilities
- Include and search for Indicators of Compromise (IOC) and create a searchable report detailing any suspicious activity found matching those IOCs. Simultaneously perform multiple tasks such as conducting an investigation while searching for IOCs.
- Check the progress of an investigation at any time via "Background Tasks" in the main menu and receive a notification when a background task has been scheduled.
- Enhanced Data Collection and Configuration Configure and collect a much broader range of data about the target host, such as event logs and file listings.
- Convert this into searchable data using the new IOC search options.
- Specify a set of IOCs before collection and Redline will now help tailor the configuration to provide meaningful search results and ensure that all the data required by the chosen IOCs is collected.
- See the detailed information associated with each indicator when choosing which indicators to include in a search.

BIO: Lucas Zaichkowsky is an engineer at MANDIANT with over fifteen years of diverse information technology and information security experience. He conducts threat briefs and customizes solutions for Fortune 1000 companies to detect and respond to advanced targeted threats. Prior to joining MANDIANT, Lucas worked for a payment processor, specializing in electronic payment processing, Point of Sale (POS) systems, PCI standards, and merchant breach response coordination.

INCIDENT RESPONSE ANALYSIS VISUALIZATION AND THREAT CLUSTERING THROUGH GENOMIC ANALYSIS

BY ANUP GHOSH

Invincea

By capturing real-time forensic information on thwarted zero-day attacks using virtual environments for browsers and PDF readers and feeding that information to the Invincea Threat Data Server, the paradigm can shift from one of post-facto breach detection and analysis to pre-breach forensic examinations on the motives and methods of the adversary. Feeding this information into a high dimention data analysis engine that categorizes malware based on core genomic characteristics, Invincea provides a visualization capability for malware research. A demonstration of this capability can be seen here: http://www.invincea.com/2012/06/applying-machine-learning-to-security-incident-response-with-invincea/

BIO: Anup Ghosh, Ph.D., is Founder and CEO at Invincea. Additionally, he is Research Professor and Chief Scientist in the Center for Secure Information Systems (CSIS) at George Mason University. He was previously Senior Scientist and Program Manager in the Advanced Technology Office of the Defense Advanced Research Projects Agency (DARPA) where he managed an extensive portfolio in information assurance and information operations programs. He previously held a role as Vice President of Research at Cigital, Inc. In his career he has served as principal investigator on contracts from DARPA, NSA, and NIST's Advanced Technology Program and has written more than 40 peer-reviewed conference and journal articles. He was awarded the NSA's Frank Rowlett Trophy for Individual Contributions in 2005 and the Secretary of Defense Medal for Execptional Public Service for his contributions while at DARPA. Anup was named to the Naval Studies Board for a National Academies Study in 2008 on Information Assurance for Network-Centric Naval Forces and currently sits on a number of advisory boards informing the future of American cyber-defenses.

SPECIAL EVENTS

BLACK HAT BOOKSTORE

Emperors Foyer, Floor 4 / July 22-26
Come by the official bookstore and browse and purchase the latest titles in security.

BLACK HAT EMBASSY HALL

Octavius Ballroom / July 25-26
Come by the Embassy Hall and learn more about our media partners, venerable institutions such as Federal Reserve of SF, OWASP, ISSA, and more.

BLACK HAT MERCHANDISE STORE

Venice, Floor 4 / July 24-26
Get your Black Hat branded merchandise—t-shirts, jackets, mugs, barware and more! *Please note: No cash will be accepted. Purchases can be made with any major credit.*

BLACK HAT SPONSOR HALL

Octavius Ballroom / July 25-26
Here is your chance to meet with representatives from and explore the offerings that the top security companies have to offer.

BLACK HAT WORKSHOPS

Florentine & Pompeian / July 25-26
In our experience, Security professionals are always looking for the latest tools and resources to perform their jobs effectively and efficiently. This year we will be hosting two tracks of security workshops to provide delegates a deeper understanding with regards to a specific subject. These tracks will run concurrently with the Briefings presentations and are available to all persons holding a Briefings pass, space permitting.

What we hope to achieve: Greater awareness and access to terrific work for the security world at large.

These will be deep technical sessions that can give delegates a chance to delve deeply into tech and hopefully take away practical applications to the information presented.

PWNIE AWARDS

AUGUSTUS III+IV Ballroom / July 25, 18:15
In 2012 the Black Hat USA Briefings are once again providing the venue for the Pwnie Awards, the security industry's premier award show celebrating the achievements and failures of the security community over the past year. For more information about the awards, please visit the official Pwnie Awards website at *http://pwnies.com*

BLACK HAT EXECUTIVE BRIEFING

ROMAN I-IV / July 24
One hundred executives from Global 2000 corporations and federal agencies are invited to attend a full day of high-level discussions about topics unique to Black Hat. The Executive Briefing will begin with an introduction from one of the highest-ranked US government officials, discussing the importance of cyber security to homeland security. The morning sessions will preview the most important technical discussions planned for the main Black Hat Briefings. Lead by Jeff Moss, founder of Black Hat and DEF CON, these previews will enable executives to discuss the implications of the newest vulnerabilities and attacks with their peers and the actual researchers. Executives can then use this knowledge to prepare their teams ahead of time and direct their technical experts to the most important research being released.

As an attendee, you'll have opportunities for discussion with presenters and peers, plus the chance to ask "threat direction" questions. Those questions will be funneled to the appropriate Black Hat speakers to discussion in the afternoon.

The afternoon sessions will further include strategic discussions around the latest threats to the public and private sectors and long-term countermeasures to be taken into consideration. Round out the afternoon with cocktails followed by a dinner in one of the great restaurants housed in the Caesar's complex.

After the Executive Briefing dinner, executives are invited to mingle with speakers at the Black Hat VIP Party until midnight.

Premium & Dinner Co-Sponsor: Qualys

Foundation Sponsor: Adobe

Event Sponsors: CORE Security Technologies, BeyondTrust, SAIC

Dinner Co-Sponsor: VERACODE

DEF CON BADGE PICKUP

Emperors Ballroom / July 26, 11:00-17:00
DEF CON badge pickup will take place on July 26 starting at 11:00 for Black Hat delegates from the Emperors Ballroom. You will need to present both the DEF CON voucher portion of your badge as well as show your main Black Hat badge.

DEF CON Badges must be pre-purchased as a part of your Black Hat registration. Discount pricing will not be offered at the regular DEF CON registration desk at the Rio.

ARBOR NETWORKS

An exciting night awaits you at Black Hat's "No Limit Hold'em" Poker Tournament, sponsored by Arbor Networks, on Wednesday, July 25th, 7pm, at Caesars Palace. Back by popular demand, this game of strategy, skill and psychology is an invitation-only event not to be missed! Register today at arbornetworks.com/poker12

EMULEX

Emulex, a leader in Fibre Channel and 10GbE networking solutions has leveraged their enterprise expertise in the new Network Xceleration solution, Sniffer10G™. We're hosting a very exclusive customer event during the conference—please RSVP, stop by booth 141 where the team will demonstrate Sniffer10G, and enter for a chance to win a spot at this event. http://connect.emulex.com/LP=423

eset

Visit us at booth 537 for your chance to win tickets to our private party on Cleopatra's Barge with L.A. indie rockers, NO. http://nomusicfor.me/

Do you rule the code? Find out by taking our crack-me challenge, eset.com/us/rulethecode. Winner gets admission to Black Hat USA or Europe 2013 and $1000 cash.

MANDIANT

Join Mandiant for our annual M After Dark party at the Shadow Bar in Caesars Palace! Festivities begin on Tuesday, July 24 at 7:00 p.m. Register here: http://marketing.mandiant.com/Mafterdark-shadowbar

QUALCOMM

Mobile Security Reception by invite only.

SOLERA NETWORKS

How deep can you dive in your data? How low can you go at the Solera Networks World-Famous Blue Martini Party? Find out on Wednesday, July 25, 7:30-9:30 pm, at the Shadow Bar. Text "Hacked" to (702) 749-4808 to pre-register and score exclusive prizes throughout Black Hat!

STONESOFT

The Stonesoft Enrichment Center is now accepting more test subjects. Stop by the Pisa Room where food, drinks, games, prizes and an authentic Portal Gun replica will be given away. Stop by booth 213 for details, and to secure your spot.

Symantec.

Come by Symantec booth #101 with your notebook and penetration tools, try your hacking skills, and see if you can break into one of our systems. A grand prize of $2000 will be given to the person who captures the main flag and several other GREAT prizes will be awarded for those that capture several flags.

THE OFFICIAL BLACK HAT WIRELESS NETWORK

Aruba Networks is proud to be supplying, installing, and managing the WLAN infrastructure at Black Hat USA 2012.

A / B / G / N WLAN Access
SSID: BlackHat
WPA2-PSK: ArubaNetworks

Be sure to visit the Aruba NOC in GENOA Meeting Room (3rd Floor/Promenade Level) to speak with wireless security engineers or see the actual BH USA 2012 network

STAY CONNECTED

- **Twitter:** Twitter.com/Black HatEvents
- **Facebook:** Facebook.com/Black Hat
- **LINKED.IN:** search for "Black Hat" on LinkedIN Groups

UPCOMING EVENTS:

- **Black Hat Training: HALO Summit 2012**
  San Diego, CA October 29-November 2
- **Black Hat UAE 2012**
  Abu Dhabi, United Arab Emirates December 10-13
- **Black Hat EU 2013**
  Amsterdam, The Netherlands March 11-14
- **Black Hat USA 2013**
  Las Vegas, Nevada July 27-August 1

EVENT AUDIO + VIDEO

THE SOURCE OF KNOWLEDGE

PALACE BALLROOM FOYER / JULY 25-26

Afraid you'll miss a session? The Source of Knowledge will be onsite to sell audio and video recordings of the Briefings sessions. Media, including iPad ready presentations, may be purchased onsite at a substantial discount.

BOOK SIGNGINGS

with these speakers in the Palace Ballroom Foyer:

July 25 / 15:15
Dino Dai Zovi, Stefan Esser, Vincenzo Iozzo, Charlie Miller, Ralf-Philip Weinmann authors of the *ios Hackers Handbook*

July 26 / 10:00
Neal Stephenson author of *Snow Crash, Cryptonomicon, Anathem, Quicksilver*

July 26 / 11:15
Bruce Schneier authors of *Liars and Outliers, Beyond Fear, Secrets & Lies*

VIDEO GUIDELINES

Keynotes and Sessions: All video content must be attributed to Black Hat USA 2012. Zooming in on laptops is not permitted. Camera crews and videographers must receive permission from the subject being recorded.

Major media companies: contact Black Hat show management for special arrangements. We encourage sharing of video content with Black Hat show management for greater exposure and cross promotion opportunities. Sponsor Hall & General Areas: Handheld cameras and mobile devices are not permitted on the Sponsor Hall or in main traffic areas.

Booths & Sponsors: Sponsors may record videos within the confines of their booth, but may not record other Sponsors booths or their staff without their permission. Before doing stand-up or fixed video recording, Sponsors should contact Show Management for special arrangements. For more information, contact Show Management in the Press Room, Messina and Livorno rooms, Floor 3.

LATEST INTEL

"scientia potentia est" = "Knowledge is Power"
Thomas Hobbes was not speaking directly about the world of Information Security, but he should have been. Survival in InfoSec is determined by one's ability to keep up. Black Hat's Latest Intel provides inside information on the latest discoveries, breaking content, speaker selections, schedules, contests, and in general, all things Black Hat. So be sure to check back regularly!

Black Hat is exclusively focused on the security community. If you have any new and interesting Intel of your own that the rest of the world should know, email "intel (at) Black Hat (dot) com"

SPONSORS

DIAMOND

QUALYS® ON DEMAND SECURITY

Microsoft

LOOKINGGLASS

PLATINUM

ACCUVANT LABS

BlueCoat

cisco

CORE SECURITY™ Thinking ahead.

IBM

LIEBERMAN SOFTWARE

LogRhythm COMPLY. SECURE. OPTIMIZE.

mykonos a Juniper Networks company

RSA

Symantec.

Trustwave® Security begins with Trust™

verizon

GOLD

beyondtrust

Booz | Allen | Hamilton
strategy and technology consultants

FIREMON

ForeScout

hp

McAfee An Intel Company

nCircle

NORMAN

RAPID7

SOLERA NETWORKS

VERACODE

vmware

WhiteHat SECURITY

SILVER

AccessData

AlienVault

amazon.com

BARRACUDA NETWORKS

Bit9

CLICK SECURITY

CODENOMICON

coverity

cybertap

DAMBALLA

DELL SecureWorks

DELL SonicWALL

DENIM GROUP

EMULEX

eset

The Ethical Hacker Network www.ethicalhacker.net

f5

FIDELIS

FireEye

firehost SECURE CLOUD HOSTING

FLUKE networks

FOREGROUND SECURITY

FORTINET

Guidance SOFTWARE

GURUCUL

The Hacker Academy

HBGary

imation

IMMUNITY

Lancope Network Performance + Security Monitoring™

loglogic

MANDIANT

mocana

NCP SECURE COMMUNICATIONS

NEOHAPSIS

NSS Labs

onapsis Securing business essentials

OPSWAT

ORACLE

paloalto the network security company™

PARSONS

phishme.com

Pico stay mighty machines

radware Smart Network. Smart Business.

RedSeal

REVERSING LABS

RIM

rune Information Security Corporation Pte Ltd

SAIC

SAINT

SecureNinja Forging IT Security Experts

SECURONIX

SILICIUM SECURITY

skybox security

SOPHOS

splunk>

ssh

StillSecure

STONESOFT

StrongAuth Securing the Core

STROZ FRIEDBERG

TCS TeleCommunication Systems Enabling Convergent Technologies®

TENABLE Network Security™

TREND MICRO

UMUC

VENAFI

WatchGuard

VASCO THE AUTHENTICATION COMPANY

MEDIA

BEYOND security

ASSOCIATED

CSA cloud security alliance™

EWF

ISSA Information Systems Security Association

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

OWASP The Open Web Application Security Project

OFFICIAL WIRELESS PROVIDER

ARUBA networks

Learn About Next-Generation Threat Prevention

Palo Alto Networks™ next-generation firewalls identify known and unknown threats on all ports, all traffic, all the time.

Our top malware and vulnerability researchers are available to share Palo Alto Networks latest advancements in network security, including WildFire™, which has uncovered thousands of new and targeted malware samples.

www.paloaltonetworks.com

paloalto NETWORKS

the network security company™