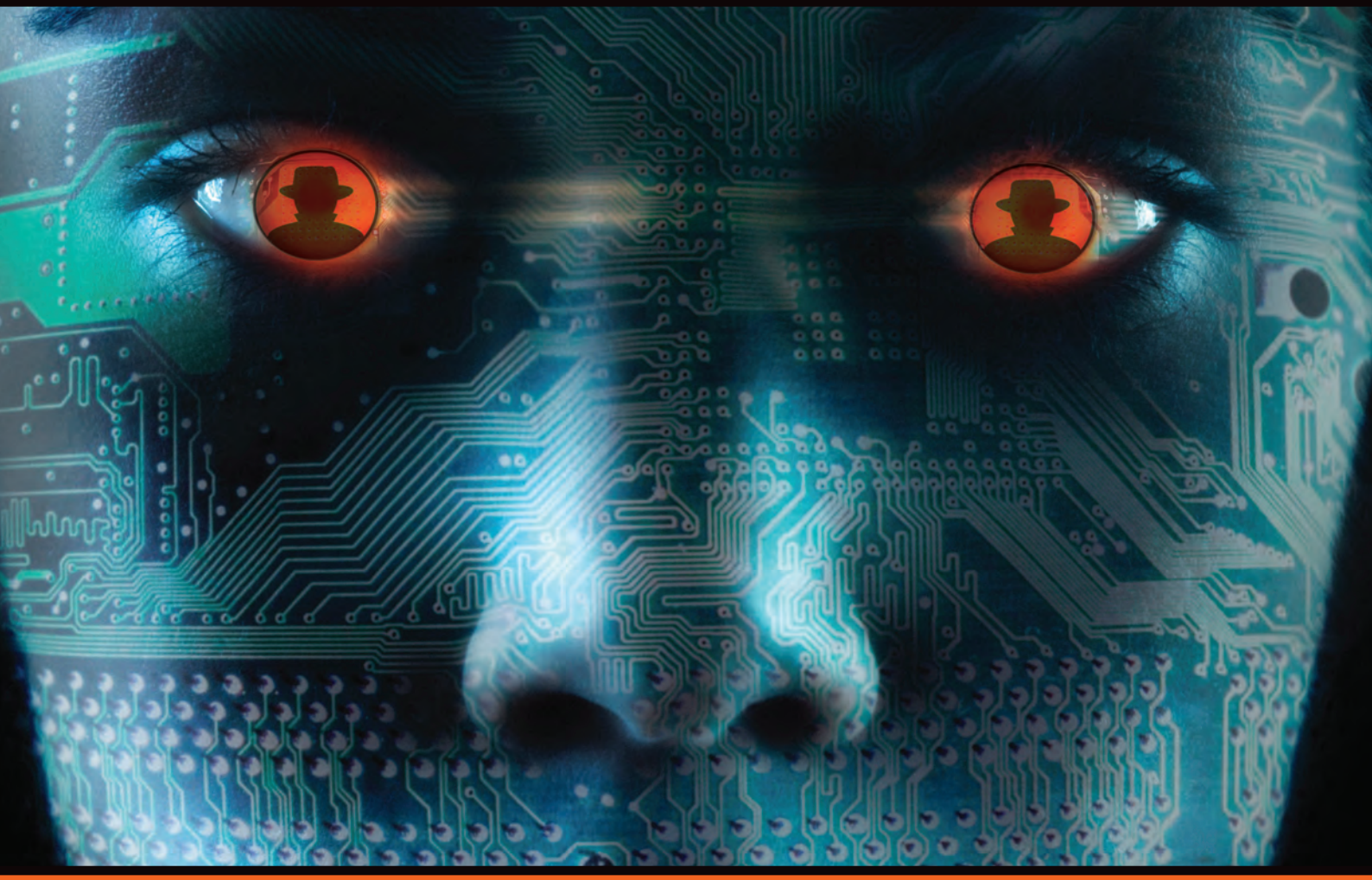
Knowledge & Technology



Come together at Black Hat Europe.

Once again the world's ICT Security Elite gather to share their knowledge and experience with you.
This is your chance to meet and network with peers and professionals at this world renown event.
Two days. Ten Classes. Twenty-five presentations.

Black Hat®

Briefings & Training Europe 2007

27-30 March 2007 • Mövenpick Hotel Amsterdam City Centre

www.blackhat.com

sponsors

platinum

FORTINET
REAL TIME NETWORK PROTECTION

Google

CODENOMICON

gold

CORE SECURITY TECHNOLOGIES

FIBERLINK
Simple. Secure. Mobility. ™

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Lancope®

Microsoft®

Training

Analyzing Software for Security Vulnerabilities
taught by Halvar Flake

This is an intense course encompassing binary analysis, reverse engineering and bug finding. The C programming language gives the programmer a lot of rope to hang himself with - and C++ just adds to the featurelist. Both languages have an impressive number of subtle pitfalls, and many of these can be leveraged by a skilled attacker to execute code on a computer on which these vulnerable programs run. But while almost everybody seems to understand the significance of these programming mistakes, few actually sit down and analyze code from the security analysis perspective. This workshop focuses on teaching security-specific code-analysis, both in source and in binary form.

Early: 1600 EUR / Regular: 1700 EUR / Late: 1850 EUR

Enterprise Security From Day 1 to Completion: A Practical Approach to Developing an Information Security Program
taught by Chris Conacher

Whether you are starting from scratch, working within an existing framework, or investigating what an Information Security program could mean for your company, creating a comprehensive Information Security program can be a daunting task. This course aims to provide a practical, step-by-step approach to securing an entire organization.

Early: 1500 EUR/ Regular: 1600 EUR/ Late: 1700 EUR

The Exploit Laboratory: Analyzing Vulnerabilities and Writing Exploits
taught by Saumil Udayan Shah

The Exploit Laboratory is an intense hands-on class for those wishing to dive into vulnerability analysis and exploit writing. The Exploit Laboratory starts off with a basic insight into system architecture, process execution, operating systems and error conditions. The class then quickly accelerates to analysing vulnerabilities with debuggers, reproducing reliable error conditions and writing working exploits for the same. The Exploit Laboratory features popular third party applications and products as candidates for vulnerability analysis and exploitation, rather than building up on carefully simulated lab exercises. Most of the class time is spent working on lab exercises and examples.

Early: 1500 EUR/ Regular: 1600 EUR/ Late: 1700 EUR

Hacking by Numbers: Combat Training by SensePost

Hacking By Numbers Combat Edition is SensePost's flagship course. Combat is an unique new concept — a series of carefully crafted Capture-The-Flag 'missions', each designed to teach a specific hacking skill or concept. This course is all hack, no talk. Combat has been described as 'Zen' for hackers. This is an advanced level course.

Early: 1700 EUR / Regular: 1850 EUR/ Late: 2000 EUR

Invisible Network, Invisible Risk
taught by Adam Laurie

This course will cover the best practice procedures for deploying wireless networks securely, as well as the tools available for both auditing and penetration testing. During the course, students will learn the history of the problems associated with wireless networking, the measures and counter measures taken along the way, and some of the more interesting phenomena surrounding the technology such as war-driving and 'free' community network projects, such as Consume in the UK and BAWUG in the USA.

Early: 1500 EUR/ Regular: 1600 EUR/ Late: 1700 EUR

Live Digital Investigation – Investigating the Enterprise
taught by WetStone Technologies

Upon completion of this intense two-day course, forensic examiners, private investigators, digital auditors, corporate security personnel, federal, state and local Law enforcement investigators, prosecutors and corporate IT personnel will have a complete understanding of the latest methods and techniques for acquiring, analyzing and investigating "Live" running enterprise computers.

Early: $2000 / Regular: $2200 / Late: $2300

Metasploit 3.0 Internals
taught by Matt Miller aka skape

This course will provide attendees with an in-depth understanding of the 3.0 version of the Metasploit Framework. The Metasploit Framework is an advanced, open-source exploitation framework that is designed to aide in the research, development, and testing of exploits. The course itself is broken down into three tracks. The first track will deal with the introductory aspects of the framework from a user's perspective. This will give students a good introduction to what the framework is capable of. The second track will take things a step deeper by diving into the internals of the framework. Students will learn about the underlying APIs that the framework is built on and how they can be used to write custom extensions to the framework itself. The third and final track will show where the framework is going in the future by exposing students to some of its more powerful aspects, such as post-exploitation and automation.

Early: 1500 EUR/ Regular: 1600 EUR/ Late: 1700 EUR

Tactical VoIP: Applied VoIPhreaking
taught by the Grugq

This course addresses exploiting VoIP—from end user devices through carrier grade servers—including protocol level attacks, application bugs and common dangerous deployment mistakes. The course provides deep coverage of a broad spectrum of VoIP relevant security threats.

Early: 1500 EUR/ Regular: 1600 EUR/ Late: 1700 EUR

Ultimate Hacking: Black Hat Edition
taught by Foundstone

Ultimate Hacking: Black Hat Edition begins from a "zero-knowledge" perspective. Start by profiling your target, then learn how to identify and exploit well-known and obscure vulnerabilities in the most popular operating systems including Windows and multiple Unix flavors. Foundstone challenges you with countless hands-on exercises to demonstrate your expertise as you race other students to achieve the ultimate goal...getting root.

Early: 1600 EUR / Regular: 1700 EUR / Late: 1850 EUR

Web Application (In)security
taught by NGS Software

In this course we cover all areas of web application security from Cross-Site Scripting, SQL Injection, LDAP Injection, Java Applet disassembly, Command Injection, Shared Hosting security bypasses, IDS Evasion and vulnerabilities in off-the-shelf products. Delegates will get the opportunity to try their hand at all of these and much more in the practical exercises.

Early: 1600 EUR / Regular: 1700 EUR / Late: 1850 EUR

Black Hat®

For more information and to register:
www.blackhat.com

Antivirus (In)Security

Sergio 'shadown' Alvarez, Security Solution Consultant, n.runs AG

Now a days Antivirus Software are the larger defence deployed in corporations and final user desktops (mail servers, file servers, http and ftp internet gateways, workstations, etc) and their engines are reused in the IPSs that the same vendors develop.

This talk will be about the findings and leassons learned while targeting the antivirus sofware that most of companies and users use.

The talk will focus mainly in the type of Bugs found (stack based buffer overfows, heap overflows, integer issues, uninitialized variables, traversals, etc) and the techniques used to find them.

Web Service Vulnerabilities

Nish Bhalla, Founder, Security Compass

The talk covers the dependency of web services on xml, the various forms of xml-based attacks, including exploiting parsers and validators, and finally provides recommendations and countermeasures.

This talk is intended for developers and web application architects. It drills down to the details of web services implementation, while maintaining a focus on good versus bad architectural design.

NIDS: False Positive Reduction Through Anomaly Detection

Damiano Bolzoni

The Achilles' heel of network IDSes lies in the large number of false positives (i.e., false attacks) that occur: practitioners as well as researchers observe that it is common for a NIDS to raise thousands of mostly false alerts per day. False positives are a universal problem as they affect both signature-based and anomaly-based IDSs. Finally, attackers can overload IT personnel by forging ad-hoc packets to produce false alerts, thereby lowering the defences of the IT infrastructure.

Our thesis is that one of the main reasons why NIDSs show a high false positive rate is that they do not correlate input with output traffic: by observing the output determined by the alert-raising input traffic, one is capable of reducing the number of false positives in an effective manner. To demonstrate this, we have developed APHRODITE (Architecture for false Positives Reduction): an innovative architecture for reducing the false positive rate of any NIDS (be it signature-based or anomaly-based). APHRODITE consists of an Output Anomaly Detector (OAD) and a correlation engine; in addition, APHRODITE assumes the presence of a NIDS on the input of the system. For the OAD we developed POSEIDON (Payl Over Som for Intrusion DetectiON): a two-tier network intrusion detection architecture.

Software Virtualization Based Rootkits

Sun Bing, Research Scientist

We will discuss the complete technical scheme of a novel VM Based Rootkit. The VMBR itself is sort of light weight VMM. After the VMBR is loaded, the VMBR will ensure the target system is still running by placing it into a rootkit created virtual execution environment. It then becomes very difficult for the victim to perceive the rootkits' presence or to find any virtualization footprint. Although this novel VMBR is just a proof of concept, it has at least achieved the coexisting transparently and perfectly with the target system.

Wi-Fi Advanced Fuzzing

Laurent Butti, Network Security Expert, France Telecom RD labs

Fuzzing is a software testing technique that consists in finding implementation bugs. Fuzzing Wi-Fi drivers is becoming more and more attractive as any exploitable security bug will enable the attacker to run arbitrary code with ringo privileges (within victim's radio coverage).

This presentation will describe all the processes involved in the design from scratch of a fully-featured Wi-Fi fuzzer. It will pinpoint all issues and constraints when fuzzing 802.11 stacks (scanning, bugs identification, replaying bugs, analyzing kernel crashes...).

Then some features will be focused on, in order to understand which kind of implementation bugs may be discovered and which vulnerabilities we discovered thanks to this tool.

Finally, a real-world example will be fully explained: how we found the first (publicly known) madwifi stack-based overflow thanks to our Wi-Fi fuzzer.

Hacking Databases for Owning Your Data

Cesar Cerrudo, Founder, Argeniss
Esteban Martinez Fayo, Security Researcher, Argeniss

This talk will discuss the Data Theft problem focusing on database attacks, we will show actual information about how serious the data theft problem is, we will explain why you should care about database security and common attacks will be described, the main part of the talk will be the demostration of unknown and not well known attacks that can be used or are being used by criminals to easily steal data from your databases, we will focus on most used database servers: MS SQL Server and Oracle Database, it will be showed how to steal a complete database from Internet, how to steal data using a database rootkit and backdoor and some advanced database oday exploits. We will demostrate that compromising databases is not big deal if they haven't been properly secured. We will also discuss how to protect against attacks so you can improve database security at your site.

Kernel Wars

Joel Eriksson, CTO of Bitsec
Karl Janmar, Security Researcher, Bitsec
Christer Öberg, Security Researcher, Bitsec

Kernel vulnerabilities are often deemed unexploitable or at least unlikely to be exploited reliably. Although it's true that kernel-mode exploitation often presents some new challenges for exploit developers, it still all boils down to "creative debugging" and knowledge about the target in question.

This talk intends to demystify kernel-mode exploitation by demonstrating the analysis and reliable exploitation of three different kernel vulnerabilities without public exploits. From a defenders point of view this could hopefully serve as an eye-opener, as it demonstrates the ineffectiveness of HIDS, NX, ASLR and other protective measures when the kernel itself is being exploited.

The entire process will be discussed, including how the vulnerabilities were found, how they were analyzed to determine if and how they can be reliably exploited and of course the exploits will be demonstrated in practice.

Vboot Kit: Compromising Windows Vista Security

Nitin Kumar, Independent Security Engineer and Researcher
Vipin Kumar, Independent Security Engineer and Researcher

Vboot kit is first of its kind technology to demonstrate Windows vista kernel subversion using custom boot sector. Vboot Kit shows how custom boot sector code can be used to circumvent the whole protection and security mechanisms of Windows Vista. The booting process of windows Vista is substantially different from the earlier versions of Windows.

We will also review sample Ring Ø Shell code (for Vista). The sample shellcode effectively raises the privileges of certain programs to SYSTEM. A live demonstration of vboot kit POC will be done.

Make My Day – Just Run a Web Scanner: Countering The Faults of Typical Web Scanners Through Byte-code Injection

Toshinari Kureha, Technical Lead and Principal Member of Technical Staff, Fortify Software
Dr. Brian Chess, Chief Scientist, Fortify Software

In this talk, we'll explore that "looking inside the application as the security test runs" possibility—through byte-code instrumentation. We will see how we can use aspect oriented technologies such as AspectJ to inject security monitors directly inside a pre-compiled Java / .NET web application. We will also go through a proof of concept and demo—turning a typical blackbox test into a 'whitebox' test using the techniques discussed in this talk, gaining a more complete picture: gaining coverage insight, finding more vulnerabilities, weeding out false positives reported by the scanners, and gaining root cause source information.

SCTPscan: Finding entry points to SS7 Networks & Telecommunication Backbones

Philippe Langlois, Founder and Senior Security Consultant, Telecom Security Task Force

This presentation will explain how SCTPscan manages to scan without being detected by remote application, how discrepancies between RFC and implementation enable us to scan more efficiently and how we manage to scan without even being detect by systems like SANS - Dshield.org. Here we will have a look at INIT packet construction, stealth scanning and a beginning of SCTP fingerprinting.

Then, we go on to detail upper layer protocols that use SCTP and the potentials of the SIGTRAN protcol suite in term of security. We'll see the M2UA, M3UA, M2PA, IUA which are SIGTRAN-specific protocols, and also the more generic SS7 protocols such as ISUP, BICC, BSSAP, TCAP, SCCP and MTP.

RFIDIOts!!! - Practical RFID Hacking (Without Soldering Irons)

Adam Laurie, CSO and Director, The Bunker Secure Hosting

RFID is being embedded in everything...From Passports to Pants. Door Keys to Credit Cards. Mobile Phones to Trash Cans. Pets to People even! For some reason these devices have become the solution to every new problem, and we can't seem to get enough of them...

Challenging Malicious Inputs with Fault Tolerance Techniques

Bruno Luiz, Security Reseacher

We humans, being imperfect creatures, create imperfect software. This presentation is regarding implementation of software fault tolerance techniques to recover the effects of malicious inputs. Most of the attacks that cause flaws to software appears of malicious inputs that are introduced by a human with the malicious objective of causing harm to the system. In the research, we examine the type of recovery used in fault tolerant software, and the types of redundancy used in software fault tolerance techniques.

During presentation, programming techniques such the assertions, checkpointing, and atomic actions, necessary for implementation of the techniques: Recovery Blocks, N-Version Programming, Retry Blocks, and N-Copy

Programming are analyzed. Investigate basic approach to self-checking software and some types of acceptance tests: Reasonableness Test and Computer Run-Time Tests. Two applications of the techniques are proposed: Recovering Exploration and Anti-Fuzzing.

Data Seepage: How to Give Attackers a Roadmap to Your Network

David Maynor, Founder & CTO, Errata Security
Robert Graham, co-founder and CEO, Errata Security,

Long gone are the days of widespread internet attacks. What's more popular now are more directed or targeted attacks using a variety of different methods. Since most of these attacks will be a single shot styled attack attackers will often look for anyway to increase the likelihood of success.

This is where data seepage comes in. Unbeknownst to a lot of mobile professional's laptops, pdas, even cell phones can be literally bleeding information about a company's internal network. This can be due to applications like email clients that are set to start up and automatically search for its mail server, windows may be attempting to remap network drives, an application could be checking for updates.

All this information can be used by an attacker to make attacks more accurate with a higher likelihood of success.

Don't laugh and dismiss this as a trivial problem with no impact. Through demonstrations and packet caps we will show how this problem can be the weak link in your security chain.

SMTP Information Gathering

Lluis Mora

The SMTP protocol, used in the transport and delivery of e-mail messages, includes control headers along with the body of messages which, as opposed to other protocols, are not stripped after the message is delivered, leaving a detailed record of e-mail transactions in the recipient mailbox.

Detailed analysis of SMTP headers can be used to map the networks traversed by messages, including information on the messaging software of clients and gateways. Furthermore, analysis of messages over time can reveal organization patching policies and trends in user location and movements—making headers a very valuable resource during the target selection phase of targeted attacks.

Attacking the Giants: Exploiting SAP Internals

Mariano Nuñez Di Croce

Our presentation will describe, after a short description of RFC interface purpose and internals, new vulnerabilities discovered in our research, both in the RFC protocol implementation and in the RFC Library itself.

Beyond new vulnerabilities discovered, our presentation will include description of some new advanced attacks we have developed, abusing default mis-configurations and design vulnerabilities. These are mainly RFC connection hi-jacking and MITM attacks, targeting connections between SAP R/3 and external programs working as RFC servers.

To make knowledge practical and publicly available, we will be presenting and releasing a new open-source tool, which will enable penetration testers and researchers to perform security assessments of SAP systems' RFC interface, allowing them to mine information and exploit the vulnerabilities and attacks described during our presentation.

New Botnets Trends and Threats

Augusto Paes de Barros, President, Brazilian ISSA Chapter
André Fucs
Victor Pereira, Security Consultant

The last years have seen the growth of botnets and its transformation into a highly profitable business. Most of the botnets seen until now have used the same basic concepts. This presentation intends to show what are the major challenges faced by botnet authors and what they might try in the future to solve them.

The presentation will pass through some interesting solutions for botnet design challenges. A layered and extensible approach for Bots will be presented, showing that solutions from exploit construction (like metasploit), P2P networks (Gnutella and Skype), authentication (digital signatures) and covert channels research fields can be used to make botnets more reliable, extensible and hard to put down.

Kicking Down the Cross Domain Door (One XSS at a Time)

Billy Rios, Senior Researcher, Advanced Security Center, Ernst and Young
Raghav Dube, Senior Researcher, Advanced Security Center, Ernst and Young

Cross Site Request Forgery (XSRF) has been billed as the newest weapon for cross domain web application exploitation. Despite the massive impact of XSRF, the attack remains extremely difficult to complete, as it requires an attacker to blindly strike against external domains, praying their attacks were successful. Now, imagine a new scenario... a scenario where an attacker can instantly see the results of their cross domain attacks. Imagine that an attacker can now steal cookies from a site you haven't been to in a week, brute force username/password combinations for internal network devices, or use your browser to run a Nikto scan against a website you've never visited!

The complexity of XSRF and Cross Site Scripting (XSS) attacks have grown by bounds over the last few years... but the two exploits are rarely used to complement each other. During this presentation, you will see the impact of an XSRF/XSS one-two combination as we demonstrate a variety of cutting-edge web application attacks, including techniques to break through the cross domain boundary.

NACATTACK

Dror-John Roecher, Senior Security Consultant, ERNW
Michael Thumann, Chief Security Officer, ERNW

We do not wish to simply release a tool; we want the audience to understand how Cisco NAC works, why it is not as secure as Cisco wants us to believe and which mitigations exist, if NAC is implemented (there actually exist mitigations and secure setup-approaches). We will present our approach, disclose technical details yet unpublished and release our tool. As an "add-on"-benefit we will explain how to tackle a complex system like NAC when doing security research.

Heap Feng Shui in JavaScript

Alexander Sotirov, Vulnerability Researcher, Determina

This presentation introduces a new technique for precise manipulation of the browser heap layout using specific sequences of JavaScript allocations. This allows an attacker to set up the heap in any desired state and exploit difficult heap corruption vulnerabilities with great reliability and precision.

This talk will begin with an overview of the current state of browser heap exploitation and the unreliability of many heap exploits. It will continue with a discussion of Internet Explorer heap internals and the techniques for JavaScript heap manipulation. I will present a JavaScript heap exploitation library that exposes an abstract heap manipulation API. Its use will be demonstrated by exploit code for two complex heap corruption vulnerabilities.

The talk will focus on Internet Explorer exploitation, but the general technique presented is applicable to other browsers as well.

Next Generation Debuggers for Reverse Engineering

ERSI Team

Classical debuggers make use of an interface provided by the operating system in order to access the memory of programs while they execute. As this model is dominating in the industry and the community, we show that our novel embedded architecture is more adapted when debuggee systems are hostile and protected at the operating system level.

This alternative model is also more efficient as the debugger executes from inside the debuggee program and can read the memory of the host process directly. We give detailed information about how to keep memory unintrusiveness using a new technique called allocation proxying.

We reveal how we developed the organization of our multi-architecture framework and its multiple modules so that they allow for graph-based binary code analysis, compositional fingerprinting, program instrumentation, real-time tracing, multithread debugging and general hooking of systems. Finally we reveal the reflective essence of our framework: our analyzers are made aware of their own internal structures using concepts of aspect oriented programming, embedded in a weakly typed language dedicated to reverse engineering.

GS and ASLR in Windows Vista

Ollie Whitehouse

The following presentation is two parts, the first covers aspects of Microsoft's GS implementation and usage. The second is a complementary section dealing with ASLR in Windows Vista, its implementation and some surprising results...

ScarabMon: Automating Web Application Penetration Tests

Jonathan Wilkins, iSEC Partners

ScarabMon is a new tool and framework for simplifying web application pentests. It makes the process of finding many common webapp flaws much easier. The user simply navigates the target site while using the WebScarab proxy and ScarabMon constantly updates the user with information on discovered flaws.

360° Anomaly Based Unsupervised Intrusion Detection

Stefano Zanero, Partner and CTO, Secure Network

In this talk, after briefly reviewing why we should build a good anomaly-based intrusion detection system, we will briefly present two IDS prototypes developed at the Politecnico di Milano for network and host based intrusion detection through unsupervised algorithms.

We will then use them as a case study for presenting the difficulties in integrating anomaly based IDS systems (as if integrating usual misuse based IDS system was not complex enough...). We will then present our ideas, based on fuzzy aggregation and causality analysis, for extracting meaningful attack scenarios from alert streams, building the core of the first 360° anomaly based IDS.

Sponsors

Platinum Sponsor: Codenomicon

The Codenomicon DEFENSICS™ platform provides proactive, pre-deployment security and robustness for IP, wireless and digital media systems DEFENSICS is the most effective black-box solution for developers, service providers and enterprises to defend their software, devices and data from security exposures and system failure. DEFENSICS technology ensures that users will identify known and zero-day vulnerabilities - The Codenomicon Protocol Modeling Engine and Attack Simulation Engine have been developed over 10 years and have proven to be the most effective and efficient methodology for finding vulnerabilities. DEFENSICS, a software-only solution, provides users with broader code and RFC coverage - helping find more vulnerabilities and critical flaws than other negative, fuzzing-based solutions. The DEFENSICS platform creates systematic and repeatable tests and can easily integrate into your current testing environment. www.codenomicon.com

Platinum Sponsor: Google

Google's innovative search technologies connect millions of people around the world with information every day. Founded in 1998 by Stanford Ph.D. students Larry Page and Sergey Brin, Google today is a top web property in all major global markets. Google's targeted advertising program, which is the largest and fastest growing in the industry, provides businesses of all sizes with measurable results, while enhancing the overall web experience for users. Google is headquartered in Silicon Valley with offices throughout North America, Europe, and Asia. www.google.com.

Platinum Sponsor: Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated multi-threat security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection–including firewall, antivirus, intrusion prevention, VPN, spyware prevention and antispam--providing customers a way to protect multiple threats as well as blended threats. Leveraging a custom ASIC and unified interface, Fortinet's award-winning FortiGate™ series of multi-threat security systems are the new generation of real time network protection systems. Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. The combination of our industry-leading FortiGuard Subscription Service offerings and our intelligent systems offer Enterprise, MSSP and SMB users unparalleled value, best in class performance, and unmatched functionality when compared to any single purpose security appliance or competing Unified Threat Management system. www.fortinet.com

Gold Sponsor: Core Security Technologies

Since 1996, Core Security Technologies has been committed to delivering breakthrough software and services that address the information security (IS) needs of corporations and government organizations worldwide. Our customers seek to protect their information assets from unauthorized access while complying with industry and governmental regulations, both today and as their networks expand in the future. Our Flagship product CORE IMPACT is the first automated, comprehensive penetration testing product for assessing specific information security threats to an organization. By safely exploiting vulnerabilities in your network infrastructure, the product identifies real, tangible risks to information assets while testing the effectiveness of your existing security investments. www.coresecurity.com

Gold Sponsor: FiberLink

Fiberlink delivers software and services that help simply secure mobility - bringing together everything IT needs to connect, secure and manage mobile workers. Combining robust security measures like Zero-Day protection, data encryption, information protection, device control, and managed personal firewalls with comprehensive connectivity, Fiberlink solutions ensure increased productivity for mobile users, and total network protection and control for IT. For 15 years, Fiberlink has been the trusted mobility expert to companies such as Bloomberg, Continental Airlines, General Electric and Novartis, keeping their networks secure and their employees productive. Additional information about Fiberlink is available at www.fiberlink.com.

Gold Sponsor: IOActive

Established in 1998, IOActive is a professional security consulting firm specializing in information risk management and application security analysis for global organizations and software development companies. To our credit, IOActive is one of three firms in the world that were tasked by Microsoft with the security code review of the Vista client operating system. Unlike commoditized network security services and off the shelf code scanning tools, IOActive performs gap analysis on information security policies and protocols, and conducts in-depth analysis of information systems, software architecture and source code using leading information risk management security frameworks and carefully focused threat models. As a home for highly skilled and experienced computer security professionals, IOActive has attracted the likes of Dan Kaminsky, Chris Paget, Dinis Cruz, Jason Larsen, Josh Schmidt, Theodore Ipsen, key advisors like Steve Wozniak, and a crew of unequivocally talented "white-hat" hackers who, before being asked to host the infamous Capture the Flag at Def Con, owned the competition three years in a row. www.ioactive.com

Sponsors

Supporting Associations

Book Sponsor

Lead Print Media Partner

Print & PDF Publications

Portals & Consultancies

Sponsors

Gold Sponsor: Lancope

Lancope is the pioneer and market leader in network behavior analysis (NBA) and response solutions that defeat zero-day worms, internal network misuse and other anomalies which compromise network integrity. Lancope's award-winning StealthWatch cost-effectively protects internal enterprise networks by integrating security and network management. Defending the networks of Global 2000 organizations, academic institutions and government entities, StealthWatch protects hundreds of enterprise customers, more than all direct competitors combined. For more information, visit www.lancope.com or email international@lancope.com.

Lancope®

Gold Sponsor: Microsoft

Microsoft is proud to be a continuing sponsor of the Black Hat Security conference. We appreciate Black Hat providing a unique forum in which security researchers from all over the world, IT Pros and industry luminaries can gather to share insights, knowledge and information to advance security research. Microsoft remains dedicated to software security and privacy and continues to collaborate with the community of people and technology organizations helping to protect customers and the broader ecosystem, Microsoft is also dedicated to software security and privacy. Since the onset of Trustworthy Computing we have fostered a culture of security within Microsoft that includes developing secure code, building strong relationships with industry researchers and partners, and providing guidance to help protect customers. We would like to thank all of the customers, partners and security researchers who have worked with us to advance the state of the art in security science. Only by working together with partners, researchers and the community can we all ensure the advancement and success of the technology industry.
www.microsoft.com/security

Microsoft®

Sustaining Sponsors

IOActive™
COMPREHENSIVE COMPUTER SECURITY SERVICES

Microsoft®

DIGITAL SELF DEFENSE

For more information and to register:
www.blackhat.com