# Building a Global Culture of Security





Marcus H. Sachs, P.E. National Cyber Security Division US Department of Homeland Security Washington D.C. 20528

# Outline



- Setting the Stage
- Critical Infrastructure Protection
- Terrorist Attacks on New York City
- The Department of Homeland Security
- The National Strategy to Secure Cyberspace
- A Global Security Culture
- Closing Thoughts





### A Quote...

"In some ways, this is a classic deterrence mission. If we want to try and prevent people from trying to attack us - trying to use the soft underbelly, if you will, of the American economy or American military forces or American society - then we have to be honest that there is a problem, that there are adversaries that will try and exploit it, and we have to show that we are prepared to deal with it."



- Dr. Condoleezza Rice, Internet Security Policy Forum II, March 2001



### Another Quote...

"The Cold War is over; the Soviet Union is gone; and so is the nuclear balance of terror. But the world faces new kinds of threats. A growing number of countries, including some of the world's least responsible states, are developing nuclear, biological, and chemical weapons and some already possess the technology for ballistic missiles to deliver them. Others are developing new capabilities to conduct cyber terrorism. We must work together to deter and address all these unconventional threats."



- President George W. Bush, Meeting of the North Atlantic Council, June 2001



### A Challenge...





### A Revelation...





### **New Vulnerabilities...**





### And New Exploits...

```
/**
* ShadowChode - 0daze b0mb th4 fUg 0uT uV m0zT aNy c1sK0 r0ut3rz!@#
*
* Ping target router/switch for TTL to host. Subtract that number from 255
* and use that TTL on the command line. The TTL must equal 0 or 1 when it
* reaches the target. The target must accept packets to the given target
* interface address and there are some other caveats.
*
* BROUGHT TO YOU BY THE LETTERS C AND D
*
* [L0cK]
*/
#include <stdio.h>
#include <sys/types.h>
#include "libnet.h"
#define MIN PAYLOAD LEN (26)
#define CLEANUP
                     { \
                     libnet destroy(lh); \
                     free(payload); \
                    }
. . .
```



### ... Including Remote Admin

Based on FlashSky/Benjurry's http://www.xfocus.org/documents/200307/2.html

- RPC DCOM Overflow Discovered by LSD
- Code by FlashSky, Benjurry, HDM
- Usage: ./dcom <Target ID> <Target IP>
- Targets:

/\*

- 0 Windows 2000 SP0 (english)
- 1 Windows 2000 SP1 (english)
- 2 Windows 2000 SP2 (english)
- 3 Windows 2000 SP3 (english)
- 4 Windows 2000 SP4 (english)
- 5 Windows XP SP0 (english)
- 6 Windows XP SP1 (english)
- \*/

. . .

#include <stdio.h>
#include <stdlib.h>
#include <error.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <unistd.h>

bash-2.04# ./dcom 6 192.168.1.13 - RPC DCOM Overflow Discovered by LSD - Code by FlashSky, Benjurry, HDM - Using return address of 0x77e9afe3 - Dropping to System Shell... Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp. C:\WINDOWS\system32>cd \ cd \ C:\>dir dir Volume in drive C has no label. Volume Serial Number is 1866-14EC Directory of C:\ 01/11/2003 02:12 PM <DIR> Paltalk 0 CONFIG.BAK 08/04/2001 07:12 PM 01/26/2003 09:04 PM 21.810 oval.wav 06/07/2001 01:28 PM <DIR> WINDOWS 01/26/2003 02:46 PM 28,860 triangle2.wav

. . .



### Communication Infrastructure Turning Point: AT&T Breakup

- Prior to 1982
  - Monolithic telecommunications network largely owned by AT&T
  - Domestic, terrestrial, circuit-switched voice network
  - Supported primarily by mechanical controls
- January 1982
  - AT&T divestiture agreement with Department of Justice
  - Concern that critical telecommunication infrastructures would fail, particularly those that supported the military
- January 1984
  - The Bell System ceases to exist.
  - In its place are seven Regional Bell Operating Companies and a new AT&T that retains its long distance telephone, manufacturing, and research and development operations





### Communication Infrastructure after the breakup of AT&T

- Telecommunications have become interdependent and diverse
- Both circuit and packet switched networks
- Terrestrial, satellite, and wireless transmissions systems support voice, data, image, and video communications
- Controlled primarily by software
- Many companies share common facilities
- New laws let just about anybody "play"



### Another Turning Point: Emerging Threats in Cyberspace

- 1997
  - Defense Department's Eligible Receiver Exercise
  - President's Commission on Critical Infrastructure
     Protection Report
- 1998
  - Solar Sunrise Investigation
  - Presidential Decision Directive 63
  - Moonlight Maze Investigation
  - Joint Task Force for Computer Network Defense



### Protecting America's Critical Infrastructures:

### **Presidential Decision Directive 63**

Established four new organizations:

- National Infrastructure Protection Center (NIPC)
- Information Sharing and Analysis Centers (ISACs)
- Critical Infrastructure Assurance Office (CIAO)
- National Infrastructure Assurance Council (NIAC)

and several "sector liaisons" such as:

- Dept of Energy Electric Power Sector
- Dept of Treasury Banking and Finance Sector
- Dept of Commerce Telecommunications Sector



#### Gas & Oil Storage and Delivery

Water Supply Systems

Banking &

Finance

## Critical Infrastructures

#### Telecommunications

Electrical Energy

Transportation



## Information Sharing and Analysis Centers

- Vital part of critical infrastructure protection
- Gather, analyze, and disseminate information on security threats, vulnerabilities, incidents, countermeasures, and best practices
- Early and trusted advance notification of member threats and attacks
- Organized by industry: cross-sector awareness, outreach, response, and recovery





## September 11<sup>th</sup> 2001

"Make no mistake: The United States will hunt down and punish those responsible for these cowardly acts..."

- President George W. Bush







## Lower Manhattan





## **Ground Zero**



## Verizon Building Exterior







## Verizon Building Interior





## New Cables at Street Level







## Lessons Learned in NYC

- Lower Manhattan's (and most other urban areas) telephones are connected to a single Central Office, with little separation of redundancies
- Telephones failed when cables were cut
- Phone switches continued working on batteries
- Cellular phones failed due to congestion and missing antennas; no means for determining priority of calls
- Internet continued to work as long as there was a physical connection and power
- Collocation of utilities (water, gas, steam, electric) caused tremendous impact on restoration efforts

### National Strategy for Homeland Security





### **Three Key Objectives**

#### **Key Objective I**

Prevent terrorist attacks within the United States

#### **Key Objective II**

Reduce America's vulnerability to terrorism

#### **Key Objective III**

Minimize the damage and recover from attacks that do occur



### Department of Homeland Security









### New Homeland Security Strategies





http://www.whitehouse.gov/homeland/

### What is the National Strategy to Secure Cyberspace?



- A policy and programmatic road map for government and industry
- Written in conjunction with the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets
- Contributions from industry and private citizens
- A "living" strategy, modular and changing as needed
- An initial framework for organizing and prioritizing efforts



## A Case for Action



- Nation fully dependent on cyberspace
- Range of threats: script kiddies to nation states
- Fix vulnerabilities, don't orient on threats
- New vulnerabilities require constant vigilance
- Individual vs. national risk management
- Government alone cannot secure cyberspace



### Priority I A National Cyberspace Security Response System



- Establish a public-private architecture for responding to national level cyber incidents
- Provide for the development of tactical and strategic analysis of cyber attacks and vulnerability assessments
- Encourage the development of a private sector capability to share a synoptic view of the health of cyberspace
- Expand CWIN to support DHS's security role in coordinating crisis management for cyberspace security
- Exercise cybersecurity continuity plans for Federal systems

# **Priority II**



### A National Cyberspace Security Threat and Vulnerability Reduction Program

- Enhance law enforcement's capabilities for preemption, prevention, and prosecution
- Secure the mechanisms of the Internet including improving protocols and routing
- Foster trusted digital control systems/ supervisory control and data acquisition systems
- Reduce and remediate software vulnerabilities
- Improve physical security of cyber and telecommunications systems



### Priority III A National Cyberspace Security Awareness and Training Program



- Promote a comprehensive national awareness program to empower all Americans to secure their own parts of cyberspace
- Foster adequate training and education programs to support the nation's cybersecurity needs
- Increase the efficiency of existing federal cybersecurity training programs
- Promote private sector support for well-coordinated, widely recognized professional cybersecurity certifications

### Priority IV Securing Government's Cyberspace



- Authenticate and maintain authorized users of federal cyber systems
- Secure federal wireless local area networks
- Improve security in government outsourcing and procurement
- Encourage state and local governments to consider establishing IT security programs



U.S. Department o Homeland Security

### **Priority V** National Security and International Cyberspace Security Cooperation



- Strengthen cyber-related counterintelligence efforts
- Improve attack attribution and suppression capabilities
- Improve coordination for responding to cyber attacks within the United States national security community
- Promote a global "culture of security"
- Foster the establishment of national and international watch and warning networks
- Encourage other nations to accede to the Council of Europe Convention on Cybercrime



## Council of Europe Convention on Cybercrime



The 2001 *Convention* is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with:

- Infringements of copyright
- Computer-related fraud
- Child pornography
- Violations of network security



• Search and seizure of computer networks and information

The main objective is to pursue a common criminal policy aimed at the protection of society against cyber crime.

## OECD Security Guidelines



OECD Guidelines for the Security of Information Systems and Networks TOWARDS A CULTURE OF SECURITY

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information VERS UNE CULTURE DE LA SÉCURITÉ



In July 2002, the *Organisation for Economic Cooperation and Development* published guidelines for cyber security that outline nine complementary principles:

- Awareness
- Responsibility
- Response
- Ethics
- Democracy
- Risk Assessment
- Security Design and Implementation
- Security Management
- Reassessment

## APEC Leader's Statement



APEC members now account for over 60 percent of the world's Internet users, and 14 of the world's 20 largest Internet Service Providers.

The APEC Leaders' Statement calls on APEC members, by the time of the next Summit in October 2003, to:

 Enact comprehensive cyber security laws, on par with existing international standards, particularly the Council of Europe Cybercrime Convention

• Identify or create national cybercrime units and international hightechnology assistance contact points

• Establish institutions, such as Computer Emergency Response Teams, that exchange threat and vulnerability assessments and information.



## United Nations General Assembly Resolution 57/239

"... effective cybersecurity is not merely a matter of government or law enforcement practices, but must be addressed through prevention and supported throughout society"

"... technology alone cannot ensure cybersecurity ... priority must be given to cybersecurity planning and management throughout society"





**U.S.** Department of

Homeland Security



## Defending the Global Computer Networks

- The Internet was created as a way to connect academia, the military, and governments (as we know)
  - but was not designed to protect information from malicious users
- Networking protocols have been predominantly "open"
- We built it, shouldn't we secure and defend it?





## A "Secure" Internet

To enable a "secure" Internet, we need:

- Accountable addressing (like IPv6)
- Dependable network services (routing, naming)
- Trusted (or trustworthy) software
- Authenticated user services (web, email)
- A <u>working</u> public key infrastructure





## A "Secure" Internet

We also need:

- Networks to be built "secure" from the ground up
- Adoption of Best Practices
- Protection from, and for, clueless users
- Certification of network engineers
- A mechanism for information sharing
- Agreements between nations



## Cyberspace Security Best Practices

- FCC's Network Reliability and Interoperability Committee (NRIC)
  - http://www.bell-labs.com/user/krauscher/nric/
- Internet Security Alliance
  - http://www.isalliance.org/resources/index.htm
- FBI's InfraGard
  - http://www.infragard.net/library/seven\_pc\_tips.htm
- National Cyber Security Alliance
  - http://www.staysafeonline.info/
- SANS/FBI
  - http://www.sans.org/top20/













## But What is "Security"?

- Measures and controls taken to protect
  - Authenticity
  - Integrity
  - Confidentiality
- Protection against, or prevention of, the unauthorized disclosure, manipulation, or deletion of information
- Or is it something else?



# **Closing Thoughts**



- Security responsibility starts with individuals
- We must seek to instill a "culture of security"
- What we are building now is the foundation for the future
- International cooperation plays a key role in securing cyberspace



## **Contact Information**



PRINT	*, 'MARCUS H. SACHS, P.E.'	AND SECUR
PF	RINT *, 'NATIONAL CYBER SECURITY DIVISION'	
<b>ва г</b> 000	PRINT *, 'US DEPARTMENT OF HOMELAND SECURITY'	
111 00	PRINT *, 'WASHINGTON, DC 20528'	
222 11	11 999 PRINT *, '202-282-8186'	
333 22	22 111 PRINT *, 'MARCUS.SACHS@DHS.GOV'	
<sup>444</sup> 33 555 ,		
666 55		
<b>1</b> 77 66	Marcus H. Sachs, P.E.	111111
888 Bi	<sup>77</sup> National Cyber Security Division	222222
88		1 <mark>333333</mark>
9	• US Department of Homeland Security	44444
	Washington, DC 20528	555555
	202 282 8186	666666
		******************