



Information Security in Academic Institutions

Strengthening Our Infrastructure and Public Safety



Development of the Higher Education Network Analysis (HENA) for Intrusion Detection and Prevention

NYS Cyber Security Conference

June 14 - 15, 2006

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.



Agenda

I. Background

II. HENA Tool

III. Preliminary Results

IV. Next Steps





Colleges and Universities Face Unique Cyber Security Issues

Sensitive Information

- R&D projects
- Government-sponsored activities
- Plethora of intellectual property
- Personal information:
SSN, DLN, account details



Diverse Users

- Students (remote, residence halls, CC)
- Faculty (remote, sharing access)
- IT and admin staff
- Guests and contractors
- Disgruntled and experimenting students
- Hackers, criminals, terrorists

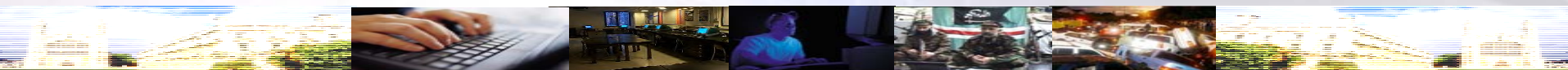
At-Risk Culture & Activities

- Tension between culture and security
 - Freedom of speech, access rights
- High user turnover rate
- Diverse access methods
- P2P, IM, e-learning

Wide-Ranging Incidents

- Hacking and data theft
- Copyright infringement
- File-sharing downloads (top 6 400Mx)
- Data tampering
- Botnet infections
- System down-time, bandwidth costs
- Reputation and credibility

This combination of issues positions academic institutions as a weak link in protecting critical infrastructure and public safety





Compromise of Institutions' Data Is Becoming Pervasive

Number	Losses and Victims	Method	Date and Institution
60,000	SSNs, names, DoB and medical records for students, faculty, workers	Hackers accessed records in health center	May 11, 2006 Ohio University's Hudson Health Center
300,000	SSNs and biographical information for alumni	Hackers accessed computer system in alumni relations dept	May 2, 2006 Ohio University
197,000	SSNs, names, DoB for current/prospective students, alumni, faculty, recruiters, staff	Hackers accessed records at McCombs School of Business	April 24, 2006 University of Texas
38,941	SSNs, names, partial e-mail addresses for current/former students, faculty, staff	Hackers accessed a university server on Fairbanks campus	April 21, 2006 University of Alaska
41,000	SSNs, names, DoB of seniors served by the Office on Aging	Hacking	March 5, 2006 Georgetown University
93,000	SSNs, names for students registered between 1996 and 2005	Stolen laptop	March 3, 2006 Metropolitan State College

Breaches in March to May, 2006 involving over 30,000 individuals
Source: www.privacyrights.org May 24, 2006.





Financial Losses and Critical Infrastructure Are Also Involved

Financial Losses

- Average \$299,571 per university from Blaster worm's havoc¹
- \$806,000 and 18,420 hours to repair one university's machines¹

Critical Infrastructure

- Bot attacks on a hospital and several universities²
- "Botmaster Network" attack on government computers³

WHAT ONE WORM COST				
During five weeks last summer, when the Blaster worm hit the Internet, colleges devoted hundreds of hours to fixing infected computers. Here are the costs reported by four universities during that period.				
	Number of computers infected	Percentage of computers infected	Hours spent to repair	Total cost
Stanford U.	6,000	30%	18,420	\$806,000
U. of Chicago	1,600	18%	9,000	\$377,000
U. of Colorado at Boulder	265	3%	465	\$9,000
U. of Michigan at Ann Arbor	2,600	7%	16,100	\$543,000

Academic institutions are un-quantified and relatively unprotected critical assets that are open to exploitation

¹Chronicle of Higher Education, March 19, 2004; ²New.com, May 5, 2006; ³Reuters, May 9, 2006





Quantitative Data Is Sought by a Variety of Stakeholders

Stakeholders

- ◆ **Government**
 - Law enforcement
 - Standards agencies
 - Cybercrime bureaus
- ◆ **Academic and Research Institutions**
- ◆ **InfoSec Associations**
- ◆ **Technical Providers**

Data Types

- ◆ **Domestic/International**
 - Policy and practice
 - Standards
 - Benchmark / time series
- ◆ **Efficiency, Best Practices**
- ◆ **Apply / Leverage Info**
- ◆ **Develop / Sell Services**





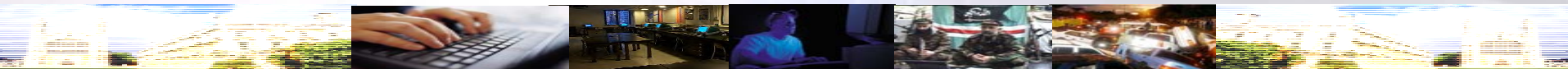
Instant Messaging

II. HENA Tool

Peer to Peer Networking

Wireless Access

Identity Theft





HENA Background

◆ Goals

- ◆ Empirically assess institutions' network activity
- ◆ Detect and prevent attacks
- ◆ Generate data-driven actions for policy and practice

◆ Users

◆ Features

- ◆ Installation and maintenance – simple and consistent
- ◆ Data collection and analysis – automated, comprehensive, almost real-time, visual, flexible
- ◆ Based on DShield.org





Components and Capabilities



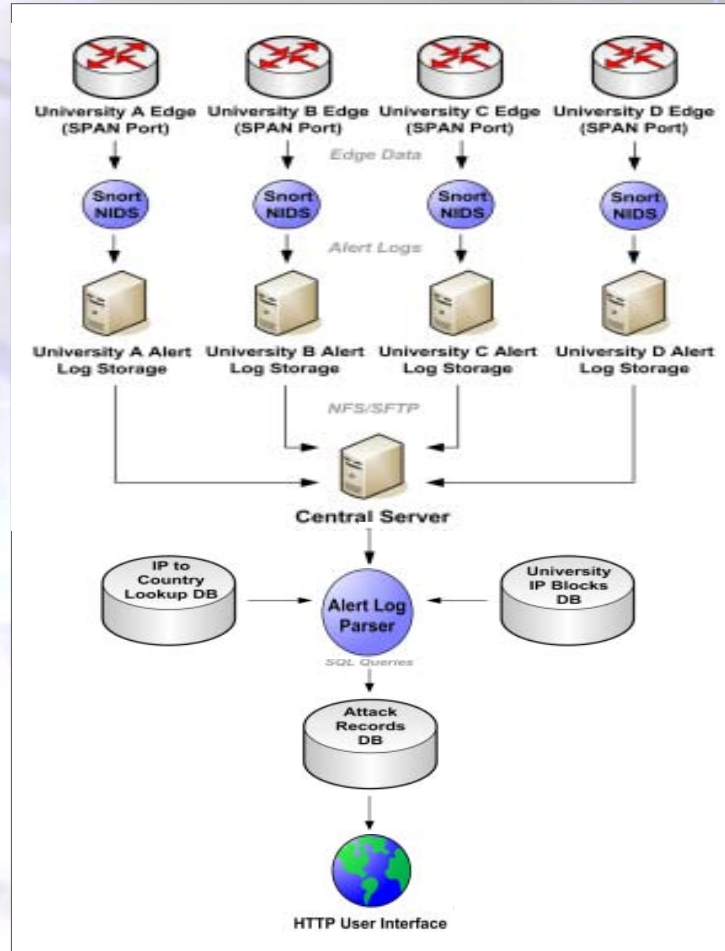
Information Security in Academic Institutions
Strengthening Our Infrastructure and Public Safety



Network Analysis

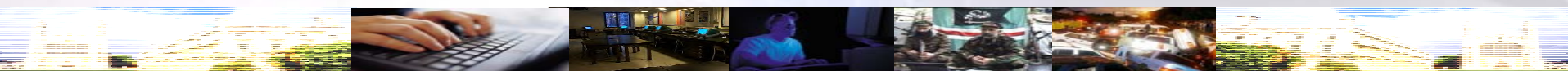


DSHield.org



DEMO

Instant Messaging
Peer to Peer Networking
Wireless Access
Identity Theft





III. Preliminary Results

January 1 – May 31, 2006

Instant Messaging

Peer to Peer Networking

Wireless Access

Identity Theft





Frequency and Types of Attacks

Inbound Attacks

- 1,996,914 attacks
- 95.5% of total attacks

Inbound Attacks per Signature ID (Aggregate)

Type of Attack	Attacks	% of Total
MS-SQL probe response overflow attempt *	492,932	24.7%
DOS MSDTC attempt *	365,482	18.3%
MYSQL 4.0 root login attempt *	272,052	13.6%
FTP format string attempt *	124,723	6.2%
snort_decoder: Experimental TCP options *	85,265	4.3%
EXPLOIT ssh CRC32 overflow filler *	65,278	3.3%
frag3: Fragmentation overlap *	60,965	3.0%
WEB-CLIENT HTML DOM invalid element creation attempt *	47,705	2.4%
SCAN FIN *	37,814	1.9%
WEB-MISC apache directory disclosure attempt *	37,273	1.9%
Others	407,425	20.4%



Outbound Attacks

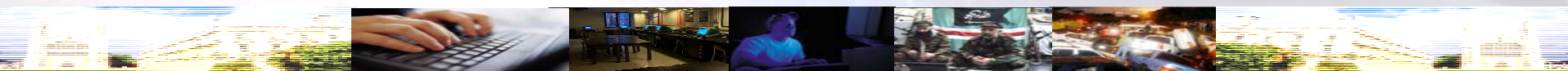
- 93,307 attacks
- 4.5% of total attacks

Outbound Attacks per Signature ID (Aggregate)

Type of Attack	Attacks	% of Total
spp_stream4: TTL Evasion attempt *	21,297	22.8%
http_inspect: BARE BYTE UNICODE ENCODING *	14,845	15.9%
spp_rpc_decode: Incomplete RPC segment *	11,423	12.2%
spp_rpc_decode: Multiple Records in one packet *	10,339	11.1%
VIRUS_OUTBOUND bad file attachment *	7,600	8.1%
http_inspect: DOUBLE DECODING ATTACK *	7,350	7.9%
http_inspect: OVERSIZE REQUEST-URI DIRECTORY *	5,805	6.2%
BAD-TRAFFIC IP Proto 103 PIM *	3,720	4.0%
frag3: Fragmentation overlap *	2,032	2.2%
ATTACK-RESPONSES Invalid URL *	1,379	1.5%
Others	7,517	8.1%



Ins
Peer
Wireless
Identity





Top 10 Individual Attackers

Inbound Attacks

- **653,552 attacks**
- **32.73% of inbound attacks**

Top 10 Inbound Targets (Aggregate)

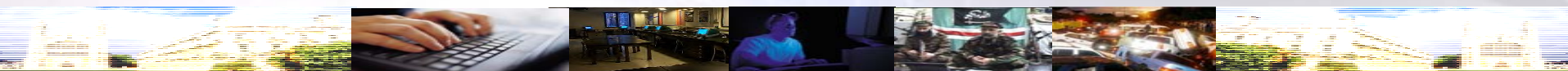
IP	Country	Attacks	% of Total
61.109.245.140	Republic of Korea	258,787	15.4%
218.4.139.234	China	118,293	7.0%
87.210.66.109	Netherlands	106,355	6.3%
160.81.236.74	United States	76,113	4.5%
69.156.167.63	Canada	26,312	1.6%
163.13.158.113	Taiwan	22,656	1.3%
60.213.54.117	China	15,322	0.9%
152.3.138.2	United States	11,074	0.7%
83.253.2.63	Sweden	10,721	0.6%
211.46.55.231	Republic of Korea	7,939	0.7%

Outbound Attacks

- **24,837 attacks**
- **27% of inbound attacks**

Top 10 Outbound Targets (Aggregate)

IP	Country	Attacks	% of Total
83.90.144.3	Denmark	5,394	8.7%
218.111.18.4	Malaysia	4,133	6.6%
144.232.187.198	United States	3,720	6.0%
72.37.157.36	United States	2,851	4.6%
24.9.242.131	United States	2,313	3.7%
85.14.217.41	Germany	1,870	3.0%
80.219.125.74	Switzerland	1,220	2.0%
209.208.193.226	United States	1,168	1.9%
209.10.215.36	United States	1,154	1.9%
80.166.149.180	Denmark	1,014	1.6%





Top 10 Countries Associated with Attacks











Inbound Attacks

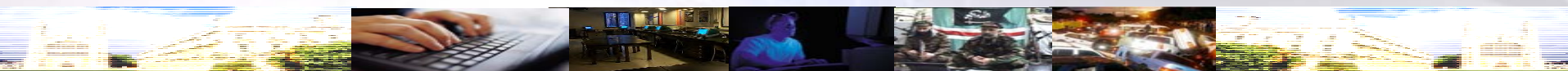
- 176 countries
- 1,760,083 attacks
- 88% of inbound attacks

<u>Country</u>	<u># Attacks</u>	<u>% Total</u>
 United States	794,839	40%
 Republic of Korea	298,986	15%
 China	243,243	12%
 Netherlands	142,194	7%
 Canada	90,826	4%
 Taiwan	49,356	2%
 United Kingdom	47,600	2%
 Germany	37,122	2%
 Sweden	34,048	2%
 Poland	21,869	1%

Outbound Attacks

- 89 countries
- 82,777 attacks
- 89% of outbound attacks

<u>Country</u>	<u># Attacks</u>	<u>% Total</u>
 United States	53,267	57%
 Denmark	6,578	7%
 China	5,033	5%
 Germany	4,767	5%
 United Kingdom	4,239	4%
 Malaysia	4,155	4%
 Switzerland	1,844	2%
 Canada	1,252	1%
 Unknown	916	1%
 Japan	726	1%





Examples of Interesting Attacks

Incident: An attempt to access a Trojan program

Source: Beijing, China – CNCGROUP NW

Output: [1:2182:8] BACKDOOR typot trojan traffic [Classification: A Network trojan detected]
[Priority: 1] 01/04-21:11:31 .0553 17 218.9.29.154:2237 -> 128.***.**.***:20295 TCP

Incident: Multiple attempts to gain access post buffer overflow

Source: Seoul, Korea – NW Management Center

Output: [1:1390:5] SHELLCODE x86 inc ebx NOOP [Classification: Executable code detected]
[Priority: 1]01/04-17:54:28. 412981 222.122.74.26:23601 -> 128.***.**.***:4397TCP

Incident: Three focused scans on multiple machines on several subnets

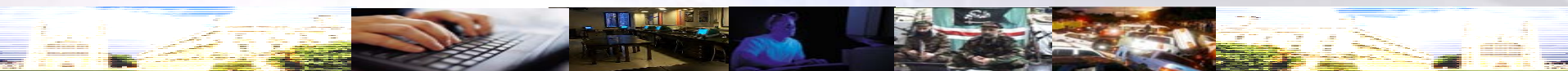
Source: Kerman Iran - Shahid Bahonar University

Output: [117:1:1] (spp_portscan2) Portscan detected from 194.225.77.222: 6 targets 6 ports in
0 seconds [**] 10/12-18:26:02.727687 194.225.77.222:11223 -> 129.***.**.***:5250 TCP
TTL:105 TOS:0x0 ID:30348 IpLen:20 DgmLen:48 DF *****S* Seq: 0xC7F697DF
Ack: 0x0 Win: 0x4000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK

Incident: An attempt *from* a university to hack *into* a Russian Website

Source: An account within University A

Output: [1:2436:5] WEB-CLIENT Microsoft wmf metafile access Classification: Attempted User
Privilege Gain] [Priority: 1] 01/04-17:38:53.524107 128.***.**.***:2936 -> 1.9.5.9:80TCP





Differences in Institutions

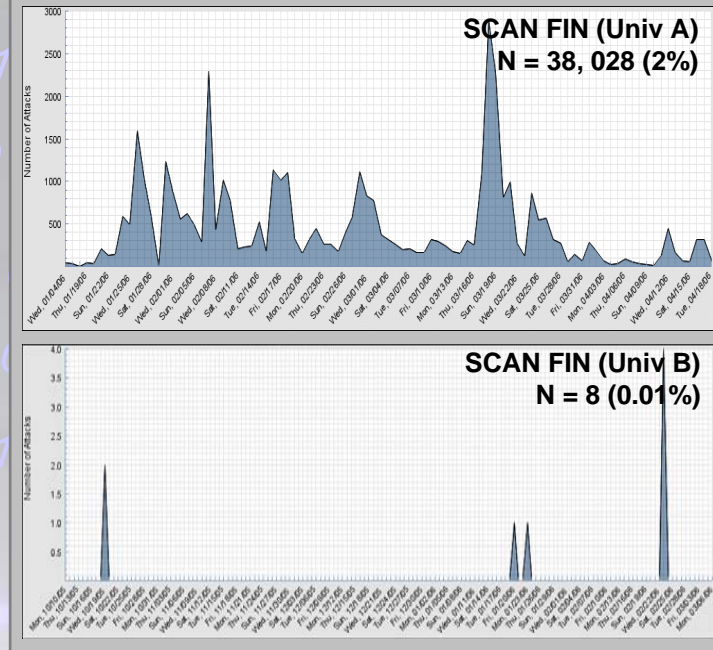
University A

- ◆ **Frequency:** 1,897,761 inbound (95% i.b.)
92,362 outbound (99% o.b.)
- ◆ **Types:** Attacks on databases, DOS, Reconnaissance
- ◆ **Top 10:** Asia, US, Canada
- ◆ **Countries:** US, Korea, China
- ◆ **Duration:** Typically prolonged

University B

- ◆ **Frequency:** 99,153 inbound (5% i.b.)
945 outbound (1% o.b.)
- ◆ **Types:** Edge router related
- ◆ **Top 10:** Asia, US, Europe
- ◆ **Countries:** US, Korea, China
- ◆ **Duration:** Spikes of short duration

Attack Types over Time





III. Next Steps

Instant Messaging

Peer to Peer Networking

Wireless Access

Identity Theft





Build on Progress

◆ Refine HENA

- ◆ Create user management system
- ◆ Associate AS number with records
- ◆ Establish 360° view of specific IP addresses

◆ Apply to Other Research Topics

- ◆ Terrorists' use of Internet
- ◆ Transnational criminal activity
- ◆ Measuring impact of controls

◆ Partner with Others

- ◆ Researchers
- ◆ Practitioners
- ◆ Potential participants





Contact Information

Steffani Burd, Ph.D.
Executive Director

sburd@infosecurityresearch.org
917.783.8496

Boris Kochergin
Network Analysis Expert

bk@isis.poly.edu
516.849.8140

Lois Lehman
Academic Institutions Specialist

lois.lehman@asu.edu
602.430.0104

www.infosecurityresearch.org





Instant Messaging
Peer to Peer Working
Wireless Access
Identity Theft

**This document was prepared for the
NYS Cyber Security Conference, June 14-15, 2006**

END OF DOCUMENT

This project is supported by Grant No. 2004-IJ-CX-0045 awarded by the National Institute of Justice, Office of Justice Programs, US Department of Justice. Points of view in this document are those of the author and do not necessarily represent the official position or policies of the US Department of Justice.

