

The Future of Information Security

A Keynote address is designed to present the issues of primary interest to an assembly and often to arouse unity and enthusiasm.
<http://www.webster.com>

Outline

- Who makes up the defensive information community?
- What are the forces that drive us?
- What are the tools we are using?
- Where are the emerging trends?
- How do I prepare?



Who Are We?

Who makes up the defensive information community?



Sex and Information Security

- 2002 – Primarily male < 40
- 2003 – Gender balance may improve as infosec audit and infosec disciplines begin to merge
- 2004 – 2007 Slow continued progress

INFOSEC Demographics

- 2002 – United States has the highest percent of highly trained information security professionals
- 2002 – Australia rapid advancement
- 2003 – Watch for results of government support in Malaysia and Singapore
- 2004 – 7 Canada, Europe race to catch up

Information Security Certification

- 2002 CISSP is most respected certification in hiring with 10,000 CISSPs
- 2003 GIAC will eclipse in terms of technical recognition
- 2003 There will be no clear winner as a large number of programs enter the market including CompTIA
- 2004 CISSP will be declining

Tougher Times

- 2002 – Wilshire total market index shows a drop from 17 Trillion to 10.3 Trillion from 3/2000 – 7/2002)
- This means there will be less money to invest in building security programs
- 2003 – 2007 The best security professionals will be focused on building business

Employment Outlook

- 2002 – Business post 9/11 has an increased emphasis on security. Security getting funding in a cooling economy
- A number of people are interested in entering infosec from systems and operations backgrounds
- 2003 – 2004 Stable, moderate growth

Intellectual Property

- 2002 – Under fire, consider the recording industry
- 2003 – Awareness increases through industry of the importance of protecting IP
- 2004 – 2007 Expect this to be a well paid specialist position in Infosec

Ethics in Information Security

- 2002 – No evidence Infosec workers have a strong sense of ethics (i.e. protect and serve)
- 2003 and beyond, this may represent a trouble spot as the boundaries between information systems audit and Infosec merge.



What Drives Us?

What are the forces that drive us?



Budget Drives Our Engineering


- Free solution vs. Paid solution
 - Nessus vs. ISS
 - Snort vs. Cisco Secure IDS
 - SANS Training vs. Buy the Book, or The Reading Room

2002 - Most Popular Tracks At SANS

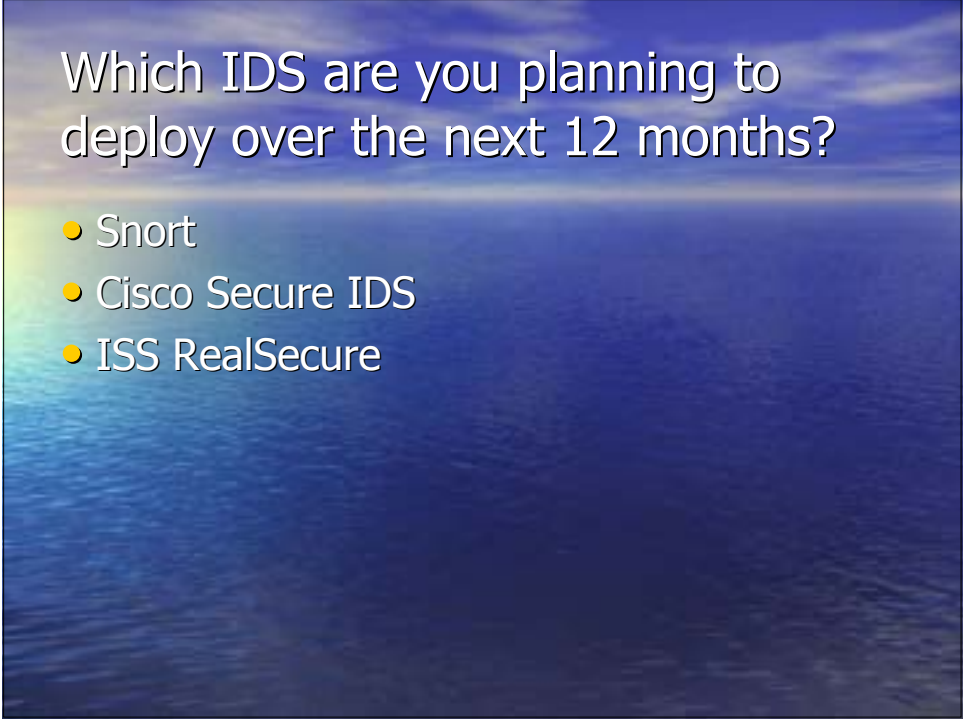
- Hacker Techniques 22.3%
- Intrusion Detection 21.7%
- Security Essentials 20%
- Firewalls and VPNs 16%
- The one to watch in the future:
- Audit – Hands On

July 2002 - Most Popular Categories in the Reading Room

- Windows 2000
- Firewalls & Perimeter Protection
- Security Basics
- Intrusion Detection
- Security Policies and Best Practices



What tools are we are using?



Which IDS are you planning to
deploy over the next 12 months?

- Snort
- Cisco Secure IDS
- ISS RealSecure

Network Intrusion Detection

- 2002 – Cost to benefits is very high, primarily done at high-end facilities, to meet audit requirements
- 2003 – Continue losing ground to increasing bandwidth
- 2004 – 2007 30% of sniffing will be policy enforcement for which there is a business case

Host Based Intrusion Detection

- 2002 – Personal firewalls are the most widely deployed HIDS - Enterprise type are actually useful
- 2003 – Expect the trend to continue
- 2004 – 2007 Operating system level HIDS that can control an application will be available at personal firewall prices

Which vulnerability scanner are you planning to deploy over the next 12 months?

- Nessus
- ISS
- The most important emerging standard is Common Vulnerabilities and Exposures, cve.mitre.org

Which firewall are you planning to deploy over the next 12 months?

- Checkpoint FW1
- Cisco Pix
- NetScreen

2002 – The Gold Standard

- The NSA/GSA/DISA/NIST/CIS “Gold Standard” for Win 2K Professional released July 2002
- By September 2002, this had been taught, hands-on in 33 cities worldwide and the courses were usually sold out
- 2003 – This becomes a roadmap for implementing standards

Where are we going?

“The best way to predict the future is to invent it.”
Alan Kay

Changing Battlescape

- 1970s – Mainframes – 100% insider problem
- 1980s
 - Vaxes – 100% insider problem
 - PCs - 100% unhackable, OS was too primitive, 100% of security based on physical security, no OS protections against keyboard attacks, highest risk was virus
 - Unix – finally an OS that could be hacked

Changing Battlescape (2)

- 1990
 - PCs grow in sophistication, now they can be “virused” and hacked. About 1995 they overtake Unix for the server market
 - Unix is still vulnerable to both insider and hacker attacks, malicious code still not an issue
 - Macintosh, probably the most secure desktop choice, if you remember to turn off the guest account
 - Vaxes, mainframes? If you can find one you can probably attack it.

Changing Battlescape (3)

- 2000
 - PCs and Unix are vulnerable to insider attacks, hacker attacks, automated attacks, self-perpetuating attacks
 - Macintosh becomes Unix
- 2003
 - .NET and other federated systems allow attackers to perpetuate an attack across domains

What are the three most important new initiatives your organization will undertake this year in improving security?

- Tied for First Place
 - Implement, Assess Policy
 - Implement Intrusion Detection
 - Security Awareness Training
- Second Place
 - HIPPA Compliance
 - Log Monitoring

IAM – (COBIT Light)

- Infosec Assessment Methodology
- www.iatrp.com
- Qualitative methodology for site assessment
- Lots of interest in audit community
- SOLD OUT at Black Hat 02

Enterprise Security Management Tools

- 2002 A ton of startups enter the field with young immature logwatcher products
 - Rationalize
 - IDMEF
 - Database Structure
 - Visualization Tools (data cubing)
- 2004 – 2007 Technology acceptance

For every dollar you spend on an IDS, spend a dollar on datastorage.

Internal Defense

- 2002 – Sites have essentially no defense past the perimeter
- 2003 – Government level PKI is becoming available and in use, potential to encrypt safely at rest, improve authentication
- 2004 – 2007 Slow, but steady progress

How do I prepare?
To be effective in 2003 and beyond?

Apply the Security Triad

- How does CONFIDENTIALITY empower my organization to compete in a global marketplace
- INTEGRITY
- AVAILABILITY

Apply IW Principles to Business

- Force Multipliers/Asymmetry
- Cycle Time
- Perception Management
- Predictable Response
- Intense Competition
- Dominant Defense

Become an IP Guru

- Economic Espionage Act -
<http://www.cybercrime.gov/eea.html>
- Copyrights –
<http://www.loc.gov/copyright/>
- DMCA -
<http://www.loc.gov/copyright/legislation/dmca.pdf>

Harness Free Security Tools

(At some point management is going to watch in the bottom line)

- Nessus
- Nmap
- Snort
- IPTables
- Ethereal
- Center for Internet Security tools

Master Windows XP or Unix

- At a minimum learn hardening, auditing and basic system administration
- Of Unix, Linux seems to be gaining dominance
- Strategies:
 - One new fact per day
 - Friday afternoons are play days

Be an Active Member of the Community

- Take all the resources you want
 - Reading Room
 - NewsBites
 - SCORE and Policy Examples
- But find a way to contribute at least once a year



That's All Folks