Lawrence Berkeley National Laboratory

Computer Security: The Why's and Wherefores

E. Eugene Schultz, Ph.D., CISSP, CISM
Berkeley Lab
eeschultz@lbl.gov

InterLab 2003
Palo Alto, California
November 5, 2003

Agenda

- Introduction
- Security in distributed networks
- Proven system and network security measures
- Security administration issues
- Getting the most return on investment (ROI)
- Status of cybersecurity legislation
- Conclusion

What is computer security?

- General definition: computer security involves providing appropriate levels of assurance of
  - ***Availability*** of computing services and data/information stored in computing systems
  - ***Confidentiality*** of data/information stored in computing systems
  - ***Integrity*** of computing systems and data/information stored therein
  - ***Auditability*** of usage of computing systems and access to data/information stored therein
  - ***Non-repudiability*** of transactions initiated by individuals and organizations

The number of security-related incidents is escalating

Hacker forces Sun to cut off outside access

Computer system is shut down in an effort to stop possible sabotage of a product.

BY TOM SCHMITZ

Mercury News Staff Writer

Sun Microsystems Inc. cut off outside access to its computer system Friday in an attempt to block a hacker who insiders say has been wreaking havoc on the company's internal network, possibly trying to sabotage one of Sun's products.

POLICE FOIL £1M HACKING PLOT

30 January 2000 - Police have charged a woman under the Computer Misuse Act following a £1 million hacking incident at a leading city finance company.

Elaine Borg, a computer operator at fund managers Henderson Financial Investment Services, is accused of hacking into the company's computer system between 1 October 1999 and 19 January 2000 with intent to defraud it of £1 million.

Borg appeared at City Magistrates' Court in London last week where police charged her under section two of the Computer Misuse Act. Section two covers unauthorized access to system with the aim of assisting a more serious crime, such as fraud or blackmail.

Borg was arrested after security devices in the company's OS/390 based systems detected irregular procedures. The irregularities were monitored and traced back to Borg's terminal.

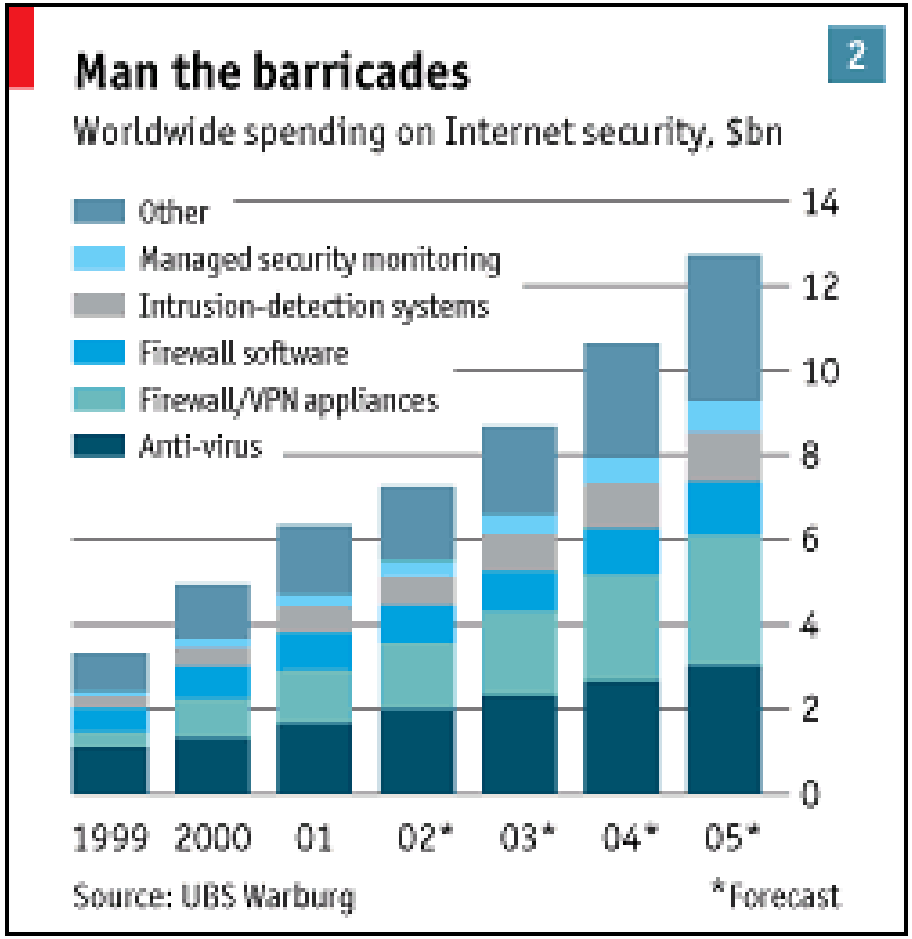
GE Says Computers Linked to Internet Were Infiltrated

BY JARED SANDBERG
Staff Reporter of the WALL STREET JOURNAL

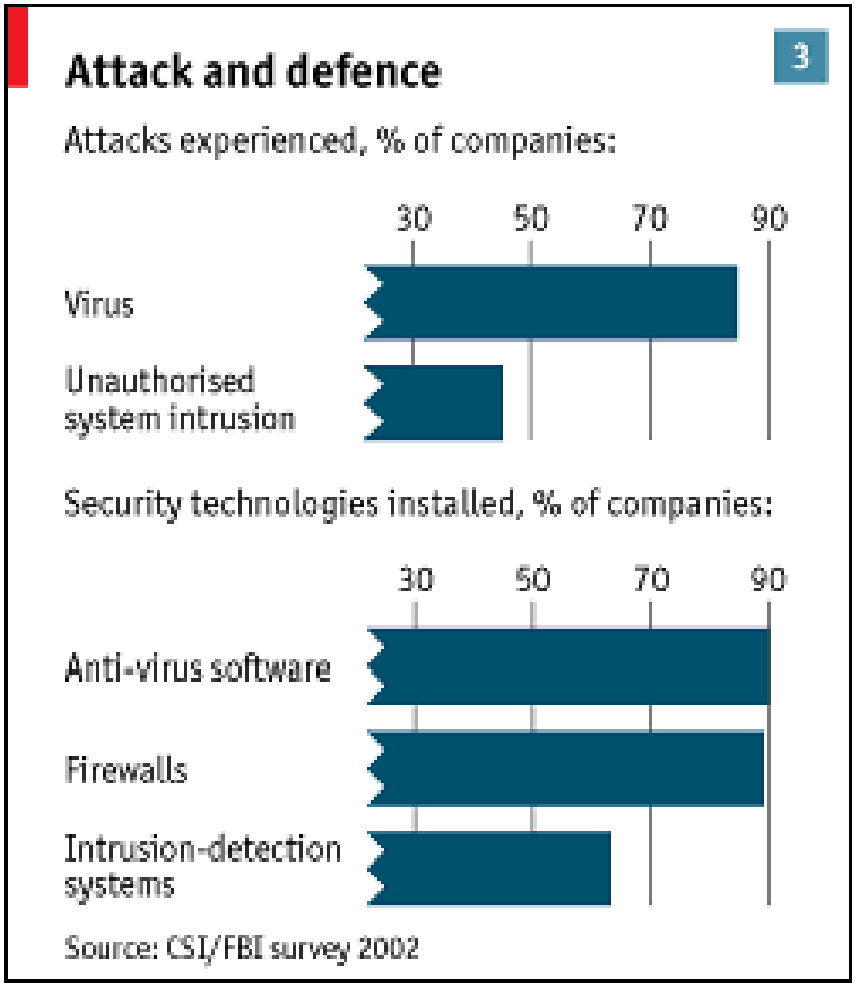
NEW YORK - Computer hackers infiltrated General Electric Co. computers connected to the Internet, according to a broadcast report by GE's local NBC television station here.

The computer breach, which was confirmed by a GE spokeswoman, gave the hackers access to research and proprietary information on GE computers in two cities, according to the report on WNBC-TV. The intruders, who managed to penetrate robust security barriers, known as "firewalls, and

How much money is being spent?



What are organizations doing about it?



Agenda

- Introduction
- **Security in distributed networks**
- Proven system and network security measures
- Security administration issues
- Getting the most return on investment (ROI)
- Status of cybersecurity legislation
- Conclusion

Major security challenges in distributed computing environments

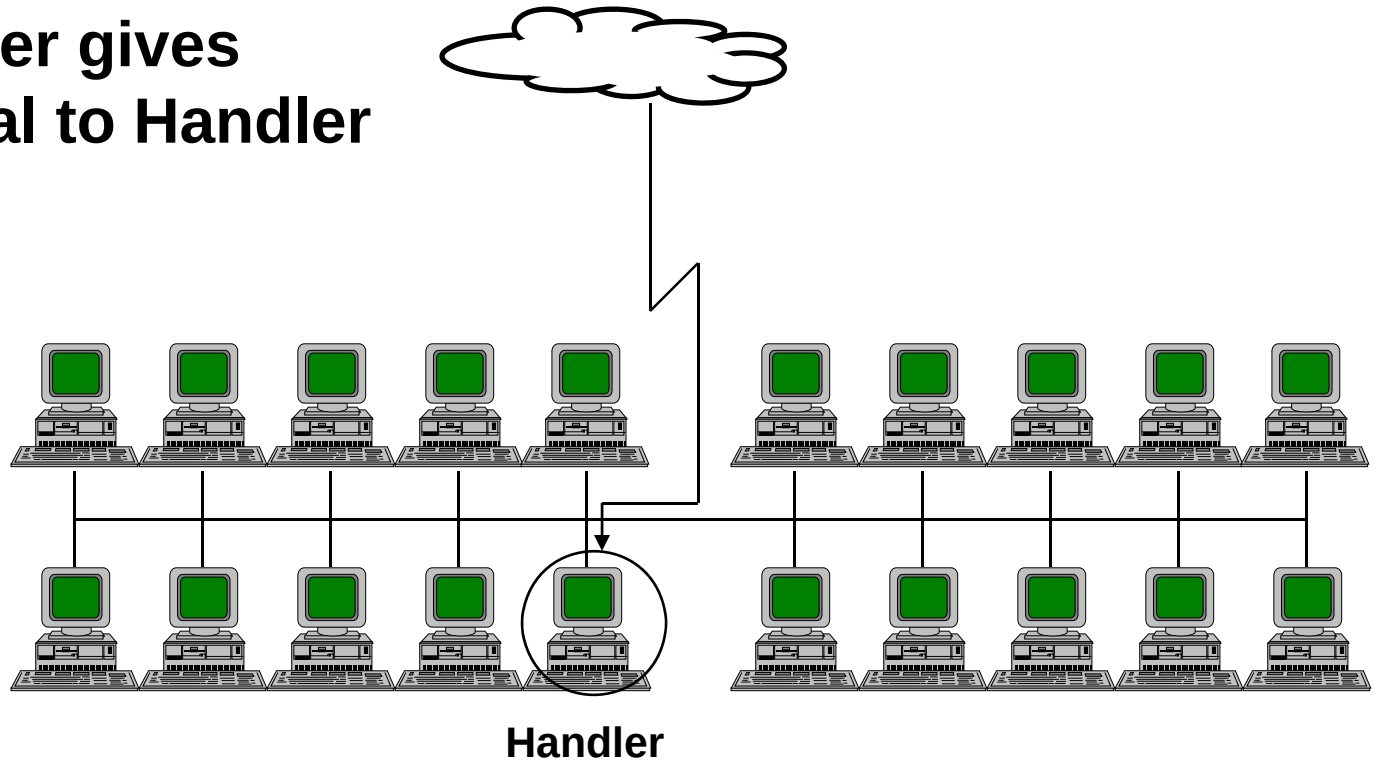
- It is difficult to centralize security (as opposed to mainframes)
- Clients create weak links in security
- Diversity of clients exacerbates the problem
- Just about every protocol used in client-server communications at every layer of the OSI model has inherent security-related weaknesses

Types of security threats in distributed computing environments

- Unauthorized users
- Misrepresentation or spoofing
- Unauthorized invocation of services
- Corruption of functions or operations
- Denial of service

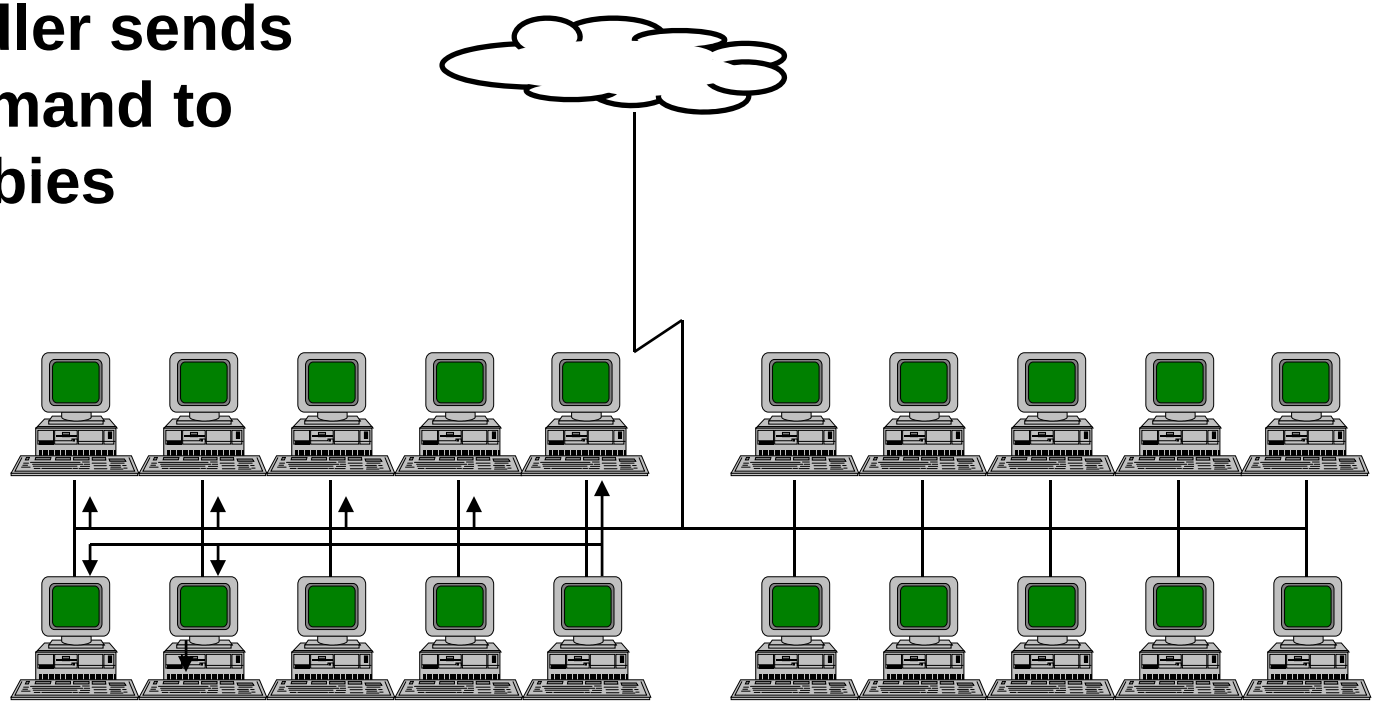
Distributed denial of service attacks

Master gives signal to Handler



Distributed denial of service attacks

Handler sends command to Zombies

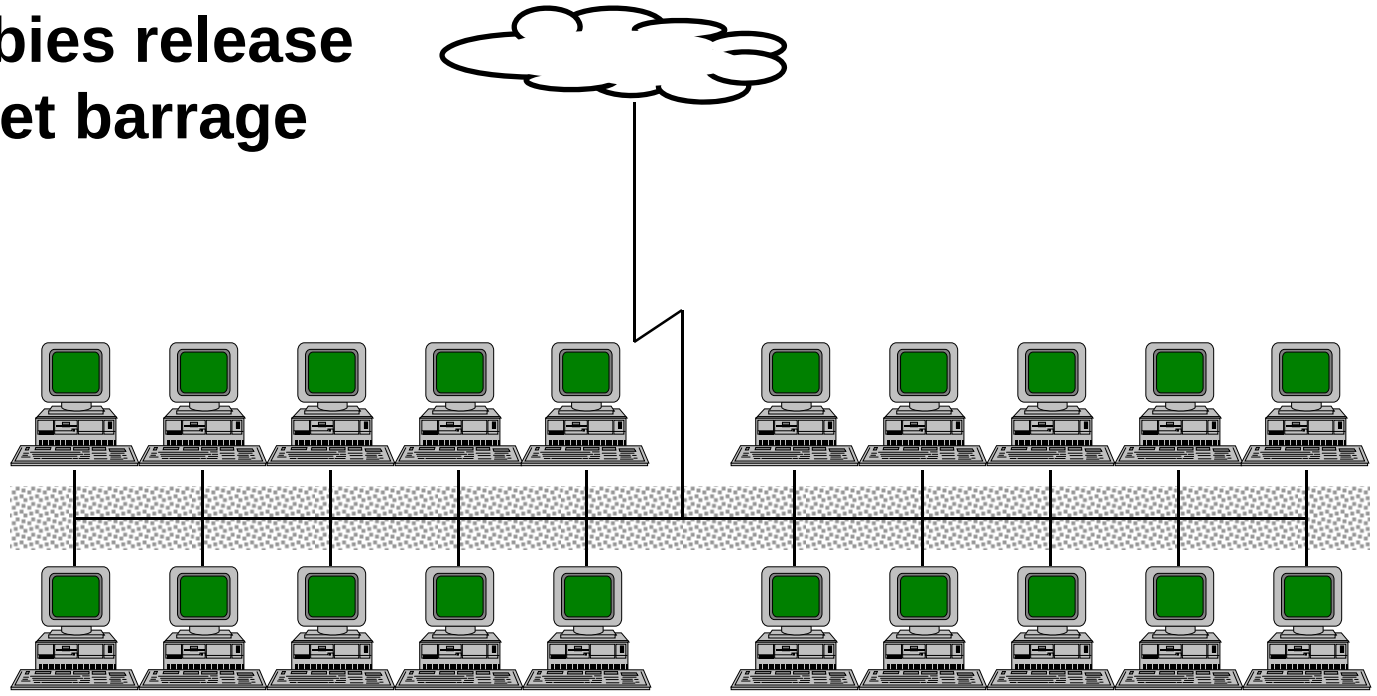


Handler

(continued from previous slide)

Distributed denial of service attacks

Zombies release packet barrage



Handler

(continued from previous slide)

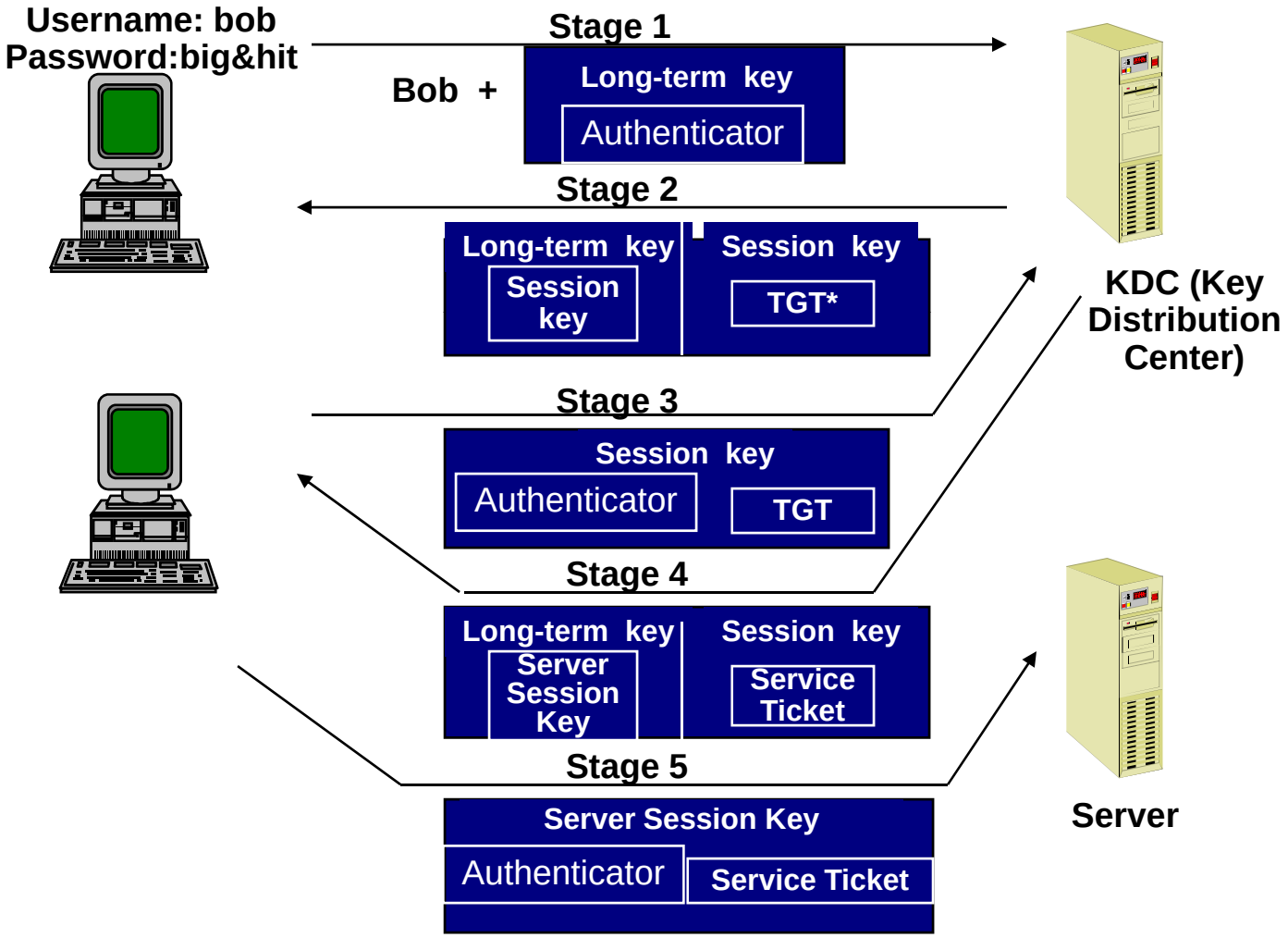
Major solutions

- Authentication--proving the identity of a person or system
- Access control--limiting who and what can gain access to
  - **Systems and their components**
  - **Network devices**
  - **Applications**
  - **Data**
- Encryption-- transforming data in a manner such that they cannot be meaningfully read because they are garbled
- Auditing and monitoring

Kerberos

- Designed to provide very strong authentication in distributed environments
- Uses a “very secure” host as a central authority
  - **Contains database of all network users**
  - **Holds passwords for all Kerberos users**
  - **Issues tickets (credentials)**
- Characteristics
  - **No passwords are ever sent over any network**
  - **Authenticates *every* session**
  - **Transparent to users during normal use**

Kerberos basics



* - Ticket Granting Ticket

Access control

- Many forms
  - **Selective blocking of network traffic**
  - **Selective access to individuals or hosts**
- Can be applied within
  - **Networks (e.g., firewalls)**
  - **Individual hosts (e.g., personal firewalls)**
  - **Applications**
  - **File systems (e.g., permissions)**

Agenda

- Introduction
- Security in distributed networks
- Proven system and network security measures
- Security administration issues
- Getting the most return on investment (ROI)
- Status of cybersecurity legislation
- Conclusion

Some proven system security measures

- Requiring everyone to select and use a good (guess-resistant) password
- Setting appropriate password aging parameters
- Using third-party authentication
- Running updated anti-virus software
- Setting restrictive file access permissions
- Limiting privileges to the minimum needed to get the job done
- Setting appropriate levels of auditing and inspecting logs frequently

Some proven system security measures

- Running personal firewalls
- Restricting dial-in access via modem
- Backing up critical computing systems as often as appropriate
- Creating and testing a plan to follow in case an attack causes a system to become unusable
- Encrypting files stored on hard drives
- Implementing appropriate physical security measures

(continued from previous slide)

Proven network security measures

- Firewalls
- Network authentication measures
- Appropriate network architectures
- Limiting services that run
- Intrusion detection
- Vulnerability scanning
- Encryption of network transmissions

Never underestimate the value of security training and awareness

- The Gartner Group found that training and awareness produces more dividends than any other single security-related measure
- Target audiences include
  - **Users**
  - **System and network administrators**
  - **Auditors**
  - **Management**
- For a sample curriculum, see http://www.lbl.gov/ITSD/Security/services/course-catalog.html

Agenda

- Introduction
- Security in distributed networks
- Proven system and network security measures
- **Security administration issues**
- Getting the most return on investment (ROI)
- Status of cybersecurity legislation
- Conclusion

Security administration issues

- Issues include
  - **Configuring systems to be secure right from the start**
  - **Installing patches as needed**
  - **Inspecting server configuration and settings to ensure that unauthorized changes have not occurred**
  - **Taking measures to minimize the likelihood of unauthorized changes in the future**
- Are extremely important because
  - **Machines are a target the minute they connect to the net**
  - **The time gap between the discovery of a vulnerability and the time it is exploited has narrowed considerably**
  - **Most security-related events involve some degree of unauthorized changes to systems and networks**

What if you don't patch vulnerabilities?

- You can always take a chance, but…
- Services in which vulnerabilities exist can be turned off
  - **Running as few services as possible is a good idea, anyway**
  - **Can result in denial or disruption of service, however**
- Firewalls and personal firewalls can compensate
  - **Can stop attacks intended to exploit unpatched vulnerabilities**
  - **Solution is anything but perfect**

Special concerns about patching

- Sheer number of patches
- Diversity of operating systems and applications that need to be patched
- Which patches really need to be installed?
- How fast must the ones that are genuinely necessary be installed?
- Has the patch been sufficiently tested?
- *Bottom line--develop procedures to be followed in evaluating/installing each new patch*

The lighter side of the problem

"Believe it or not, this is the latest Microsoft security patch."

Inspecting critical system properties

- Focus
  - **Accounts**
  - **Groups**
  - **Privileges**
  - **Ownerships**
  - **Permissions**
  - **Files and directories**
- Should be done regularly (every 1 - 2 months, at a minimum)
- Using tools (e.g., Tripwire) makes task manageable

Using Tripwire's siggen command

```
#siggen /etc/inetd.conf
sig0: nullsig  : 0
sig1: md5      : 28tGmgp.QsDF9REtUEhjJL
sig2: snefru   : 21dScGRRuDekfT2OQ7ab1d
sig3: crc32    : 1eB0TW
sig4: crc16    : 002Cs0
sig5: md4      : 1RynSTZ.WMon.1.Qsh3uTh
sig6: md2      : 0R2adEeDS2U2TYeC3bcTLo
sig7: sha      : Ec1Ujc45h.t1kt1rKsFy0pQ03rt
sig8: nullsig  : 0
sig9: nullsig  : 0
```

Agenda

- Introduction
- Security in distributed networks
- Proven system and network security measures
- Security administration issues
- Getting the most return on investment (ROI)
- Status of cybersecurity legislation
- Conclusion

Getting the most ROI

- Is an extremely elusive issue--security is like life insurance, after all
- Security as an *enabler*--the most effective approach (if possible)
- Basic principles
  - **Align security with business/operational drivers**
  - **Understand what risks are present and what their magnitude is**
  - **Implement security measures on a priority basis**
  - **Achieve a baseline level of security--avoid weak links**
  - **Systematically estimate and record the cost of security-related breaches**

Getting the most ROI

- Always consider costs versus benefits when considering implementing security measures
- Using metrics to show cost savings is the most effective way to communicate ROI to management

(continued from previous slide)

Agenda

- Introduction
- Security in distributed networks
- Proven system and network security measures
- Security administration issues
- Getting the most return on investment (ROI)
- Status of cybersecurity legislation
- Conclusion

Major U.S. computer security-related statutes

- Title 18 U.S. Code 1030, Computer Fraud and Abuse Act (as amended in 1996)
  - **States that unauthorized access to a "Federal interest computer" is a felony**
  - **Prescribes penalties for violation**
- Public Law 100-235, Computer Security Act of 1987
  - **Requires all "sensitive" information in Federal computers to be identified and covered by a protection plan**
  - **Requires contingency response plan for sensitive Federal systems**
  - **Requires computer security training for users of Federal computing systems**

Major U.S. computer security-related statutes

- Economic Espionage Act of 1996
  - **Strengthens protections against theft or misuse of proprietary business information, software piracy, and copyright infringement**
  - **Provides monetary penalties and prison sentences for defined acts of economic espionage or trade secret theft**
  - **Preserves the confidentiality of trade secrets in court proceedings**
- Electronic Theft Act of 1996
  - **Makes copyright violation punishable, regardless of intent to profit**
  - **Copyright violation must involve material worth at least $1,000**

(continued from previous slide)

Major U.S. computer security-related statutes

- Title 18 U.S. Code, Section 1462--Makes possession and transfer of indecent materials illegal
- Title 15 U.S. Code, Section 1693, Electronic Funds Transfer Act--prohibits tampering with systems that control electronic funds transfer
- 18 U.S. Code, Section 2500 et seq., Electronic Communications Privacy Act--forbids interception and disruption of electronic communications involved in interstate and/or foreign commerce
- Title 18 U.S. Code, Section 2252A--Forbids possession and transfer of child pornography

(continued from previous slide)

Major U.S. computer security-related statutes

- Title 18 U.S. Code, Section 2701 et. Seq., Stored Wire and Electronic Communications and Transactional Records Access Act--forbids unauthorized access to stored electronic communications
- Title 18 U.S. Code, Section 2703, allows law enforcement agencies to seize system logs and other data
- Federal Information Security Management Act of 2002--requires US government agencies to conform to a variety of provisions

(continued from previous slide)

Recently passed legislation that is already making a huge impact

- Sarbanes-Oxley Act--requires management to establish and maintain an adequate internal control structure and procedures

http://www.sarbanes-oxley.com/

- Health Insurance Portability and Accountability Act (HIPAA)—a complex set of federal regulations requiring that health care companies and every agency or organization that transmits protected health information electronically implement a wide set of security controls

http://www.hhs.gov/ocr/hipaa

Recently passed legislation that is already making a huge impact

- California SB 1386—requires that any business or agency that uses a computer to store confidential personal information about a California resident notify whoever may have had personal information (social security numbers, driver's license numbers, account numbers, and/or debit or credit card numbers) compromised

http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

(continued from previous slide)

What's on the horizon?

- Government Network Security Act--would greatly restrict peer-to-peer file sharing in US government systems
- Safeguard Against Privacy Invasions Act--would require companies using spyware to obtain computer users' consent before this software could be installed on their systems
- The Piracy Deterrence and Education Act--a calls for the FBI to assign federal agents to investigate and prosecute copyright violations, including online violations

What's on the horizon?

- Conyers-Berman Bill--would punish Internet users who permit others to copy (via peer-to-peer sharing and other methods) songs and movies from their computers
- Stop Pornography and Abusive Marketing (SPAM) Act and Reduction in Distribution of Spam Act--prescribe penalties for sending SPAM

(continued from previous slide)

Agenda

- Introduction
- Security in distributed networks
- Proven system and network security measures
- Security administration issues
- Getting the most return on investment (ROI)
- Status of cybersecurity legislation
- Conclusion

Conclusion

- Computer and information security continue to grow in importance
- The gap between attackers' capabilities and ability to defend against them is widening
- Neglecting security is the worst thing you can do
- Defense in depth (multi-tiered defenses) work best
- Always weigh costs versus benefits when considering security measures
- *Nobody ever said this was going to be easy!*