



Information Security and Management

Arish Siddiqui

Introduction



Subject:



Information Security and Management



Lecture Content:



Information Security in Today's World

Protecting Your PC, Privacy and Self

“The minute you dial in to your Internet service provider or connect to a DSL or cable modem, you are casting your computer adrift in a sea of millions of other computers – all of which are sharing the world's largest computer network, the Internet. Most of those computers are cooperative and well behaved, but some are downright nasty. ***Only you can make sure your computer is ready for the experience.***”

Daniel Appleman, *Always Use Protection, A Teen's Guide to Safe Computing*, (2004 – Apress)

Purpose of This Discussion

- Provide an overview of:
 - What information security is
 - The challenges to InfoSec
 - The latest trends
 - Best practices to help protect your digital assets
 - The need for Information Security professionals
 - CyberWATCH

What Is Information Security?

- Process by which digital information assets are protected.
- Topic areas: Policies and procedures, authentication, attacks, remote access, E-mail, Web, wireless, devices, media/medium, secure architectures, IDSes/IPSes, operating systems, secure code, Cryptography, physical security, digital media analysis...

Understanding the Importance of Information Security



Prevents data theft



Avoids legal
consequences of not
securing information



Maintains
productivity



Foils cyberterrorism



Thwarts identity theft

Challenges

- A number of trends illustrate why security is becoming increasingly difficult:
 - Speed of attacks
 - increasing digital information
 - Sophistication of attacks
 - Faster detection of weaknesses
 - Distributed attacks
 - Difficulties of patching

Latest Trends



IDENTITY THEFT



MALWARE



PATCH MANAGEMENT
FAILURES



DISTRIBUTED DENIAL
OF SERVICE

Latest Trends - Identity Theft

Crime of the 21st century

Involves using someone's personal information, such as social security numbers, to establish bank or credit card accounts that are then left unpaid, leaving the victim with the debts and ruining their credit rating

National, state, and local legislation continues to be enacted to deal with this growing problem:

- **The Fair and Accurate Credit Transactions Act of 2003** is a federal law that addresses identity theft

Latest Trends - Identity Theft - continued



Phishing is a method used by identity thieves to obtain financial information from a computer user



The word “phishing” was made up by hackers as a cute word to use for the concept of *fishing for information*



One of the most lucrative forms of spamming



Often used in conjunction with spoofed Web sites

Latest Trends

- Identity Theft - continued



According to the Identity Theft Resource Center,



a victim of identity theft spends an average of more than 600 hours



and \$1,400 of out-of-pocket expenses restoring their credit by contacting credit bureaus, canceling credit cards, and negotiating with creditors

Latest Trends

- Malicious Software (Malware)



Designed to operate without the computer user's permission



May change or destroy data



May operate hardware without authorization



Can hijack your Web browser



Might steal information or otherwise aggravate a computer user or organization

Top 10 Malware Threats

Other notable ransomware threats that have successfully 'robbed' users during the past year are:

CryptoLocker

[Troldesh](#)

Bit Cryptor

[Tox Ransomware](#)

Alpha Crypt

Los Pollos Hermanos

[Locker](#)

Malware Trends



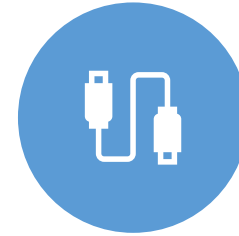
SPYWARE



KEYLOGGERS



ROOTKITS



MOBILE MALWARE



COMBINED ATTACK
MECHANISMS

Malware Trends - Spyware

Advertisement-focused applications that, much like computer worms, install themselves on systems with little or no user interaction

While such an application may be legal, it is usually installed without the user's knowledge or informed consent

A user in an organization could download and install a useful (often "free") application from the Internet and in doing so, unwittingly install a spyware component.

What will you do ?



If you get a message saying you have viruses on your system ?

Do you want to delete ? Yes/No



If you say yes- it is delete

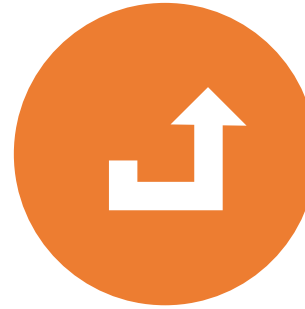


If you say no- it is delete



Think

CN4000 and CD4000



BEFORE WE CONTINUE



YOUR PRESENTATIONS
WILL TAKE PLACE ON W/C
09-DEC-2021



ANY DOUBTS OR
QUESTIONS ?

Malware Trends – Spyware - continued



Apart from privacy concerns, the greatest issue presented by spyware is its use of your computer's resources and bandwidth.



This translates into lost work as you wait for your computer to finish.



The time and money lost while eradicating spyware often exceeds all other forms of malware and spam combined

Malware Trends - Keyloggers



Used to capture user's keystrokes:

AKA Keystroke Logging



Hardware and software-based



Useful purposes:

Help determine sources of errors on system
Measure employee productivity on certain
clerical tasks

Malware Trends - Rootkits



Is a set of software tools intended to conceal running processes, files or system data, thereby helping an intruder to maintain access to a system while avoiding detection.



Often modify parts of the operating system or install themselves as drivers or kernel modules



Are known to exist for a variety of operating systems



Are difficult to detect

Malware Trends - Mobile Malware



Increase in the number of mobile phone viruses
being written



Insignificant compared to the much larger
number of viruses being written which target
Windows desktop computers

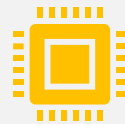
Malware Trends - Combined Attack Mechanisms



Speed at which malware can spread
combined w/a lethal payload



SPAM with spoofed Web sites



Trojans installing bot software



Trojans installing backdoors

Latest Trends - Patch Management Failures



Shift towards patching versus testing




In the next few years, it is estimated that 90% of cyber attacks will continue to exploit known security flaws for which a fix is available or a preventive measure known- A patch.

Latest Trends - Patch Management Failures - continued

- Why? Doesn't scale well and isn't cost-effective:
 - A survey by the Yankee Group found that the average annual cost of patching ranges from \$189-\$254 per patch for each computer
 - The cost is primarily a result of lost productivity while the patch is applied and for technician installation costs.
 - Patching costs in large organisations can exceed \$50 million per year

Latest Trends - SPAM

January 24, 2004 - Bill Gates predicted that spam would be “a thing of the past” in 15 years – the threat remains alive



No end in sight:

According to Ferris Research, by 2007, the percentage of spam E-mails will increase to 70% of the total E-mail messages sent

Latest Trends - Vulnerability Exploitation



Operating system attacks still in vogue:

Vista

Mac OS X



Increase in attacks taking advantage of security holes in other products:

Desktop tools

Alternative Web browsers

Media applications

Microsoft Office applications

Latest Trends - Ransomware



Type of malware that encrypts the victim's data, demanding ransom for its restoration.



Cryptovirology predates ransomware

Latest Trends - Distributed Denial of Service (DDoS)



Use hundreds of infected hosts on the Internet to attack the victim by flooding its link to the Internet or depriving it of resources.

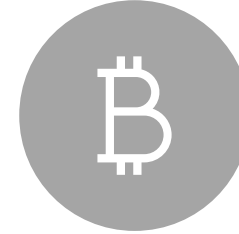


A PC becomes a zombie when a **bot**, or automated program, is installed on it, giving the attacker access and control and making the PC part of a zombie network, or **botnet**

Summary



WHAT INFORMATION
SECURITY IS



THE CHALLENGES TO
INFOSEC



THE LATEST TRENDS



BEST PRACTICES TO
HELP PROTECT YOUR
DIGITAL ASSETS



THE NEED FOR
INFORMATION SECURITY
PROFESSIONALS



PRECAUTIONS

Questions ?

