Operating Systems Security

Raj Jain

Washington University in Saint Louis

Saint Louis, MO 63130

Jain@cse.wustl.edu

Audio/video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-09/

Overview

❑ Layers of Security

❑ 10 Immutable Laws of Security

❑ Malware

❑ Defenses

❑ Passwords

❑ Application Security: Email, Browsing

Layers of Security

| Application Security |
| Network Security |
| **OS Security** |
| User Security |
| Physical Security |

❑ *A lock is as strong as the weakest door.*

Common Operating Systems

❑ Windows (9x, XP, Vista)

❑ Windows Server (NT, 2000, 2003)

❑ Linux

❑ Linux Server

❑ Unix

❑ Solaris

❑ HPUX

Multiple books on security issues of each one.

Most malware exploits windows – due to popularity.
  ⇒ We will mostly concentrate on Windows
  We cover only a very small subset of issues.

10 Immutable Laws of Security

1. *If a bad guy can persuade you to run his program on your computer, it's not your computer anymore*

2. *If a bad guy can alter the operating system on your computer, it's not your computer anymore*

3. *If a bad guy has unrestricted physical access to your computer, it's not your computer anymore*

4. *If you allow a bad guy to upload programs to your website, it's not your website any more*

5. *Weak passwords trump strong security*

Laws of Security (Cont)

6. *A computer is only as secure as the administrator is trustworthy*

7. *Encrypted data is only as secure as the decryption key*

8. *An out of date virus scanner is only marginally better than no virus scanner at all*

9. *Absolute anonymity isn't practical, in real life or on the Web*

10. *Technology is not a panacea*

Ref:http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx?mfr=true

Where Malware Hides?

❑ Autoexec.bat or autoexec.nt can start malware before windows start

❑ Config.sys, config.nt

❑ Autorun.inf on CD-ROMs or even hard drives

❑ Boot.ini, bootsect.dos, command.com, dosstart.bat

❑ msdos.sys, io.sys

❑ Desktop.ini - Can be used to hide files and auto-launch programs when a folder is viewed

❑ Host, lmhost

❑ Manipulating SMTP server settings or the Host file and intercepting sent e-mail.

Malware (Cont)

- Nested archives (zip, rar, tar, cab)
  - detected only by recursive scanning

- Auto-run files in archives

- Embedded applications in Documents (word, PowerPoint, excel)

- Embedded macros in documents
  - Can secretly send a named doc to a remote sender

- OLE2 formatted documents can be executed

- Rasphone.pbk - Can modify dialup network setting including DNS and make long distance calls

Malware (Cont)

❑ Startup folder

❑ Web cache - malware dropped in by websites

❑ Path variable - illegitimate program will run then load legitimate program

❑ Trusted publishers - can execute programs w/o user approval

❑ Registry entries

❑ Embedded URLs in HTML Emails (can execute programs)

Malware Trends

❑ Moving from hobby to criminals
$\Rightarrow$ more attempts to gain financial information

❑ Viruses are distributed through compromised websites

❑ Compromised clients are then directed to download more malware

Magnitude of the Problem

❑ Messagelabs.com:
  ➢ 69% of all emails is spam. 1 in 43 contain virus
  ➢ 70% of all spam is sent from addresses of innocent users

❑ Antiphishing.org:
  ➢ Phishing email increasing 26% per month
  ➢ 2% to 15% of the phishing is successful

❑ Dell.com:
  ➢ Average PC has 50 to 70 spyware infections

❑ Secretservice.gov:
  ➢ 29% of all successful intrusions by insiders

Defenses

❑ Don't give users Admin access
⇒ Windows Vista requires "run as administrator" for Privileged operations:

- ➢ Install or uninstall programs
- ➢ Configure windows system settings
- ➢ View or change security permissions
- ➢ Change networking configuration
- ➢ Stop, start, load, or pause services
- ➢ Modify drivers
- ➢ Registry
- ➢ etc.

Defenses (Cont)

❑ Update often

❑ Use Personal firewall

❑ Use antivirus software - keep updated

❑ Use anti-spam

❑ Use anti-spyware

❑ Boot-up password

❑ Boot only from primary hard drive - Can't load NTFS4DOS

❑ Password protect the bios

Defenses (Cont)

❑ Disable guest account

❑ Rename administrator account - unlimited retries

❑ Rename guest account to administrator - helps catch hackers

❑ Run services on non-default ports https://x.com:3809

❑ Install software on non-default folders

❑ Use encrypted file system (EFS)

❑ Disable LM and NTLM authentication

❑ Enable account lockout after a certain number of tries $\Rightarrow$ Potential DoS Attack

Defenses (Cont)

❑ Use two factor authentication - biometric, smart card, USB token, etc.

❑ Disable Simple File Sharing. SFS removes most NTFS permissions to close to Share. All connecting users come in as administrator or guests

Passwords

❑ Most people use only alphabets with dictionary words $\Rightarrow$ Easily broken

❑ Common passwords: password, admin, 12345, ...

❑ Often leave manufacturer defined password unchanged

❑ Most people use the same passwords for all accounts $\Rightarrow$ Get their password in a less secure environment and use it in a more secure environment

Windows Login Passwords

❑ Windows 2000 allows 127 character passwords with 64k possible characters $\Rightarrow 4.9 \times 10^{611}$ passwords

❑ System managers can set policies: Requiring minimum length and types of characters

  ➢ Upper case alphabets

  ➢ Lower case alphabets

  ➢ Numerals

  ➢ symbols

  ➢ Unicode characters: Alt+nnnn 4 #s numeric keypad

❑ Most keyboards have 94 characters
  $\Rightarrow$ Most hackers will try 94 possibilities

Password Hashing

- Windows uses LAN Manager (LM) hashes or NT hashes.
- LM Hash is case insensitive and truncates password to 14 characters
- LM Has in not salted $\Rightarrow$ Results in the same output if two accounts use the same password
- Salted $\Rightarrow$ Random value is mathematically applied to the password before hashing
- Challenge-Response is used over the network

Password Attacks

❑ Password resetting - much easier than cracking

❑ Replace the Security Account Manager (SAM) files $\Rightarrow$ Nordhi boot diskette

❑ Net use drive mapping

❑ Brute force password guessing $\Rightarrow$ John the ripper exercise, Cain & Able, Brutus, TSGrinder (Terminal services and RDP connections)

❑ SQL Server authentication $\Rightarrow$ ForceSQL, MSSqlPwd, Swlbf, Sqlbf-all, and SWL Auditing Tool

Password Attacks (Cont)

❑ Password capturing via key loggers,

❑ Hardware key logger - PS2 like between the keyboards and the PC. Used by FBI, CIA, Bank robbers, Customers

❑ Sniffing authentication traffic on the network

❑ Share Message Block (SMB)/NetBIOS attack tools: ScoopLM captures authentication exchanges, BeatLM then does off-line brute force cracking. Similarly, SMBRelay, SMBGrind, SMB Auditing tool, SMB Downgrade Attacker.

❑ Share password attacks - Share password cracker

Password Attacks (Cont)

❑ Kerberos Authentication
   - KerbSniff and KerbCrack

❑ Password Cache: 10 user credentials are cached
   - CacheDump

❑ Passwords saved with Remote Desktop Protocol (RDP) – cracked by Cain & Able

❑ Older IE (before IE6) sent authenticated credentials to all IIS servers

Password Authentication Mistakes

❑ Dell XP PCs (2005) had an hidden ad account with blank password,

❑ MS Word password can be blanked by opening the document in an editor

NetBIOS/SMB Services

❑ Commonly Attacked Window Services

❑ Enumerate NetBIOS name table of any machine: nbtstat -A <IP address>

❑ NetBIOS name table service can be disabled

❑ Anonymous logins

Application Security

❑ Peer-to-Peer (P2P) Sharing programs allow users to share files, directories, and drives

❑ Deny-by-default software policy in many enterprises

Email

❑ Phishing

❑ Attachments

❑ HTML content (autopreview)

❑ Spam: Spamming tools to introduce misspellings to avoid detection, to harvest emails from web sites, usenet groups, chat channels

❑ Most email is plain text $\Rightarrow$ Can be read by any one

❑ Match the senders domain with IP address

❑ Set rate control on: Connections per client, emails per client, number of recipients per email

❑ Personal black and white lists

Browsing

❑ IE MIME type mismatch - Declare skin but send java script

❑ IE Plug-ins, Active X controls, Java scripts

❑ Password and form input saving in browsers and in-line auto complete

❑ Empty Temporary Internet Files folder when browser is closed

Web Servers

❑ Directory Traversal:

➢ http://hostdomain/../../../../../../windows/system32/cmd.exe?/c+dir+c

➢ will be converted to c:\windows\system32\cmd.exe in unpatched versions of IIS 5.

➢ Allows a command shell access to the hacker

Summary
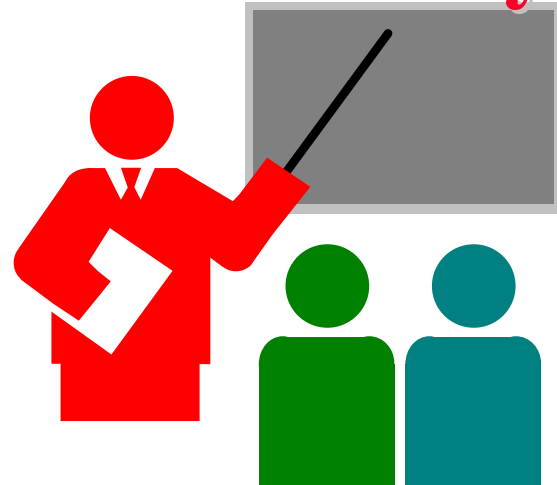
- Need to secure systems against theft of data
  – bios password, boot password
- Passwords must be strong.
  Use two-factor authentication for critical applications.
- 10 Immutable Laws of Security
- Secure email and browsing

Reference

- R.A. Grimes, "Professional Windows Desktop and Server Hardening," Wrox Press, 2006, 600 pages, ISBN:0764599909

- Michael O'Dea "Hacknotes:Windows Security Portable Reference," McGraw-Hill/Osborne, 2003, ISBN:0072227850

- Eric Maiwald, "Fundamentals of Network Security," McGraw-Hill, 2004, ISBN: 0072230932

- R. Bragg, et al, "Network Security: The complete Reference," McGraw-Hill/Osborne, 2004, ISBN:0072226978

- Jan L. Harrington, "Network Security: A practical Approach," Morgan-Kaufman, 2005, ISBN:01231163333

Lab Homework 4

❑ This homework requires two computers with OpenSSH and telnet client and servers installed. You can use CSE571XPC client and CSE571XPS server or your own computers.

❑ Start ethereal (or wire shark) on the client machine.

❑ telnet to the server and login with your username and password. Logout.

❑ ssh to the server and login with your username and password. Logout.

❑ Stop ethereal and read the trace.
Note the difference in the two logins?