Windows NT/2000/XP Security Mechanisms

Simon Myara
or « Is Windows really so unsecure and buggy as people think? »
Security Classes

US DoD (Department of Defense) Trusted Computer System Evaluation Criteria (Orange Book)

Range:
- D (minimal protection) to
- A (verified protection)
Security Classes (2)

- Common Criteria is a newer metering of computer system security, based on EALs (Evaluation Assurance Level)
  - “The Common Criteria represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the international community.”
- Ranges from EAL1 (-) to EAL7 (+)
Security Classes (3)

- Windows NT: C1
- Windows NT with resource kit: C2
- Windows 2000 with SP3 and networking hotfix: C2, EAL4 after lots of effort

- What does this mean?
Security Classes (4)

- C1 : fairly good security
- C2 : quite good security
- EAL4 : currently the best level that any « common use » OS can reach
Security Mechanisms

or « What are the secrets behind the desktop… »
Boot Process

Unlike in Windows 95/98, security begins in the very beginning

NT loader writes over the interrupt vector table

All writes to hard drive boot records are disabled

Interrupts protected by virtual devices
Logon Process
Logon Process (2)

- Ctrl-Alt-Del shows the logon prompt
- SAS (Secure Attention Sequence)
- Pressing these keys calls the security subsystem and stops all user programs
- Then, username and password are asked
- GINA (Graphical Identification and Authentication) can also be used
Logon Process (3)

- For local user, password is checked with SAM (Security Account Manager)
- For roaming user, password is checked in the domain server, using Kerberos
- If logon is allowed, user gets a token, describing his rights during the session
User Groups

Different rights are given to a user, depending on the group he belongs to:

- Administrators
- Backup Operators
- Power Users
- Users
- Guests
Computer Lock

This computer is in use and has been locked.

Only W2K-TEST\bgoode (Jonny B. Goode) or an administrator can unlock this computer.

Press Ctrl-Alt-Del to unlock this computer.
Computer Lock (2)

- Once a user is logged on, he can lock the computer.
- His processes are still running, but all user inputs are blocked.
- The user can resume the session by entering his password.
Computer Lock (3)

- An administrator can log off the user by entering his own credentials, but he cannot resume the session.
- If the computer is shut down when locked, the lock reappears when it is again powered.
FAT (File Allocation Table) format was developed in 1976 by Bill Gates, and is now supported by all Microsoft OSes.

- No security parameters in FAT

NTFS (New Technology File System) is supported by Windows NT, 2000, XP
NTFS Details

- NTFS has many advantages
  - Faster for large file systems
  - Supports bigger files
  - Supports access control given by permissions to files and directories
  - Supports file ownership and compression
  - Supports encryption and user quotas since Windows 2000
NTFS Details (2)

- File access rights can be given to a folder but also to a single file, and are related to a group or a single user.
- These permissions are stored in the ACL (Access Control List).
- User’s token contains a SID (security identifier) used in NTFS permissions.
NTFS Permissions

When a user tries to access a NTFS resource, there is a loop through ACEs (Access Control Entities). The loop stops if:

- there is a Deny for the SID
- there is an Allow for the SID
- or the end of ACL is encountered

If allowed, the user gets a handle to the resource
NTFS Encryption

- Uses the Encryption Certificates as keys for the expanded Data Encryption Standard (DESX) algorithm
- It is possible to encrypt single files, but also whole folders
- Only the user that encrypts a file can decrypt it
NTFS File Streams

- NTFS supports several streams in the files
- It makes possible, for example, to have properties attached to a file
- However, none of the programs shipped with Windows can make use of this property
- The stream may be accessed by typing FileName:StreamName
If you are curious, try this in a command window of your NT/2000/XP box:

- `echo Hidden stream > Test.txt:_hidden`
- `type Test.txt`  
  *doesn’t show anything*
- `more < Test.txt:_hidden`  
  *shows: Hidden stream*
- However, when you look at the file size, it says 0.

It is possible to store any kind of data in a stream… could you expect that a file that reports size 0 may contain a lot of things?
Windows Registry

- In DOS there are files like config.sys, autoexec.bat, win.ini, system.ini, protocol.ini
- Since Windows NT all this is in Registry in %SystemRoot%\System32\Config directory as files called hives
- For it’s own safety, it is recommended to install Windows on a NTFS partition, to avoid unwanted users to play with the registry files
Auditing

- Auditing allows the administrators to know almost everything that users are doing with the computer.

- Many resources can be audited, such as NTFS files and folders, printers, registry keys...

- One should avoid to over-audit, since it would report a really big amount of events.
Network security

Without going into details, Windows 2000 includes some useful network security features:

- IPsec
  - Explained on 8th of April
- Firewalling
  - Explained on 29th of April
Want more information?

- Last year’s lecture slides about Windows NT security
- US DoD Orange Book
- Evaluation Assurance Level
  - http://www.commoncriterias.org/
- NTFS encryption
  - http://www.brienposey.com/kb/working_with_ntfs_encryption.asp
- Microsoft Technet Security Resources
Thank You

Note: this work hasn’t been in any way sponsored by Bill Gates 😊