Windows NT Security

- Windows 95, 3.1, 3.11 are basically DOS and they have no security whatsoever.
- Windows NT has security features, especially as a computer in a network.
- Security of Windows NT should be understood correctly. In the USA DoD classification the Trusted Computing Standards Evaluation Criteria (the Orange Book) Windows NT has the classification C1 without any other features than login, passwords and file ownerships.
- With Windows NT Resource Kit the classification is C2, but only if the computer is not networked!!!!
- The Orange Book classification is from A1 (secure system) to D1 (no security, like DOS).
- To characterize C1 or C2, it is secure against your kid brother trying to break in. C2 is hard for any system to fill.

Windows NT Security

- Or to make it better sounding, C1 or C2 level of Windows NT is sufficient security against: (NT with a net connection is only C1)
  - a non-expert (who does not have inside knowledge of holes) with
  - insufficient time to find holes or to break passwords,
  - insufficient resources to break cryptographic mechanisms,
  - no ready-made tools (like a bootup floppy for a system which allows DOS-bootup),
  - no private access to the physical computer (so that he could open the computer and access the hard disc),
  - no access to the same LAN so that he could access with NetBIOS,
  - does not try to destroy the computer with a sledge hammer, or remotely with a HPM-weapon (High-Power Microwave).

Windows NT Security

- To summarize, C1 is fairly good and C2 quite good security and Windows NT can be considered as one of the most secure networked operating systems in common use today.
- This is because to be really secure a computer should not be connected to any network and it should be in protected locations where only trusted personnel can enter.
- We cannot require such security levels from a computer which is to be used in a normal environment.
- Class A1 is basically a computer in a totally secure locations with no network access used by one trusted person.
- Class B is not reached for instance by any Unix, there are e.g. requirements that privileged users cannot give access to nonprivileged users. In Unix root programs are run by non-root users and one can give access to others.

Windows NT Security

- Simple threats to Windows NT include:
- The standard PC is not a protected equipment against physical or electomagnetical attacks. (you need TEMPEST)
- If you do not prevent bootup from a floppy, it is possible to boot with a DOS-system floppy, read the content of the hard disc, modify the system files, for instance that they do not ask for a password, do anything as a superuser, restore the system to its original state so that no trace is left.
- The same goes if you have a double boot to Windows 95/DOS. Notice, Linux has the same vulnerability.
- If the intruder has some patience and NT system to try, he can disassemble say, CMD.EXE corresponding to DOS COMMAND.COM, and learn enough of the Virtual Device Drivers of NT to be able to write a native NT virus, which actually can do anything a DOS-virus can do.

Windows NT Security

- If the intruder gets to the same LAN he can use NetBIOS, SMB protocols. NetBIOS is a networking protocol for DOS PC networks and SMB is a protocol for file access on top of NetBIOS.
- These protocols have about the same level of security as NFS, that is almost no. With them you can access files in Windows NT.
- Macro viruses and DOS/Windows 3.1 viruses on DOS-boxes work under Windows NT. They have problems accessing protected files unless started by the administrator.
- Most Windows NT users probably are the only users of the machine and do not use the access controls (why should they). Then viruses could work well.

Windows NT Security

- After these starting comments which try to put Windows NT security to the correct framework for what can be expected from it, let us look at the security features.
- They are quite challenging to a remote hacker.
- **Logon**
- NT has a superuser called the administrator. Other users have access only to their directories and files.
- After turning on the power the user has to “boot” the machine with Crt-Alt-Del after which he gets the login prompt. This feature is intended to remove any Trojan horse (like BackOrifice).
- It is not boot of DOS, the sequence calls Windows NT security subsystem and stops all user programs.
- Why they use the DOS boot as Security Attention Sequence SAS is that all other key combinations were in use.

Windows NT Security

- One should consider whether it is necessary to remove the possibility of booting from a DOS-floppy and stopping the user from changing the set-up-data in CMOS. If you have so secure environment that nobody gets there, you do not need it.
- CMOS data can be put behind a password. However, remember the following fact. In many PC hardware types ‘ROM’ BIOS is not really ROM and there are parts that can be overwritten. To recover the computer from such problems such a PC has a crisis recovery floppy which has a bootup program. It is so e.g. in my digital venturis 575 pentium PC.
- To run the crisis recovery may require changing jumpers in the computer, so you have to open the computer, but the moral is that you always get in no matter what the CMOS settings are. Therefore do not trust the CMOS password unless you have checked the hardware.

Windows NT Security

- **Registry**
- In DOS there are files like CONFIG.SYS, AUTOEXEC.BAT, WIN.INI, SYSTEM.INI, PROTOCOL.INI.
- In Windows NT 4.0 all this is in Registry in
- %SystemRoot%\System32\Config - directory as files called hives. For a user (not a hacker) the hives look like one system, called the Registry.
- If your system allows boot from DOS-system floppy or allows dual boots, make at least the registry a NTFS-volume.
- NTFS is a new file system in Windows NT. In DOS and Windows 95 etc. the files are FAT (File Allocation Table) file formats. If you change the Registry to NTFS, then beginning hackers cannot change and read the files with DOS-tools.
- Naturally, it will not stop a more knowledgeable hacker. For instance, Linux can read NTFS files.

Windows NT Security

- The Registry should be made updateable only by the administrator. He can update it with regedit.exe or regedt32.exe. You can do this as an administrator from the File Permissions menu.
- Then a user cannot change the Registy, but notice, that if a user reinstalls Windows NT to another directory, there will not be any access restrictions by default and he will get access to the files of other users.
- If there are multiple operating systems in the disc, you can prevent causal users from booting from them by setting a time-out value to zero in the NT boot menu. To boot yourself you probably have to set the time back to some more reasonable value.
- While Windows NT is running Registry files are locked. If there are no bugs, this means that no hives can be modified.

Windows NT Security

- You should back up the Registry and pertinent files on a regular basis. There is a program Repair Disk (RDISK.EXE) or The Backup Utility (BACKUP.EXE) to do this.
- There is also Windows NT Emergency Repair disc. It is not a bootable disc but it restores the vital information. You have to run Windows NT 4 set-up to restore the system.
- Remote administration is possible with the RAS-system (Remote Administration System). It has a Registration Editor.
- You may set permissions on registry Keys so that a user cannot for instance delete a key.
- There are good auditing facilities for the Registry.
- As a summary: the Registry is an essential part of Windows NT security. Before making any changes to the registry, think over and save the original version.

Windows NT Security

- **Windows NT Security Subsystem**
- When you type in your password, WinLogon checks your password against SAM (Security Account Manager) hive in the Registry. If the password and user name matches, SAM creates an access token.
- This access token contains the rights to all operations in the session. It should be clear to the reader, that this is not a very strong way - it is similar to Unix - an intruder only has to cheat the SAM in the initial authentication. After that it is not cryptology. You may be able to change the binary in WinLogin and gain access thereafter.
- All processes of the user get this same access token. The administrator can audit the user actions with the access token. (Attack the access token, can you?)

Windows NT Security

- **GINA**
- The WinLogin with Crt-Alt-Del SAS button can be replaced by GINA (Graphical Identification and Authentication) under special conditions.
- This is to customize the login procedure as all may not like Crt-Alt-Del.
- **WinLogin tuning**
- You can fine tune WinLogon from the Registry or from the System Policy Editor. You can set the logon banner, enable shutdown or not, disable last login name, and whether Windows NT should wait for login to complete before running user shell.
- You can disable error messages from bootup errors, as it can be considered information relevant to an intruder.

Windows NT Security

- Changing banners may be useful in the States as they had a case of a hacker breaking into federal governments computers who claimed, that as the computer said Wellcome, he was only trying to accept the invitation.
- He was released (it is States, try - or preferably, do not - it here). So now you can put the banner to be less inviting.
- There are LegalNotice texts in Windows NT to do this.
- You can disable the login by AutoAdminLogon. If you do so, you will throw away security.
- As an ex-assembler programmer, I dislike all these options. they are in the code, so patching the binaries enables them easily. You may naively believe binaries cannot be patched with no access rights - right, but still. (for instance, as a principle, a virus only needs a short time to overwrite the bits before it is removed by antivirus program, system is changed.)

Windows NT Security

- **Locking Windows NT**
- This is a new feature: there is a menu by which a user can lock access to the computer with a password but processes can run in the computer. Only the user who locked the computer can remove the lock or the administrator can overrule the lock.
- This is an improvement to Windows 95 password option to a screen saver. In that solution anybody could turn off the power and reboot the machine. No process could run as the screen saver could eat all the CPU-time.
- Of course you can turn off the key but the lock reappears when the power is turned on. The processes running in the PC seem to be recovered in this case. Actually it seems to be that the power is still on and eats the batteries, so at least you can turn of computers and let them run out of batteries, then probably data is finally lost.

Windows NT Security

- **Firewalls**
- Windows NT has several mechanisms by which different firewall solutions can be realized.
- Packet firewall: Windows NT has an inbuilt packet filter.
- Application firewall: It is possible to obtain an application level firewall proxy system, called Catapult.
- Configuring a network router as a firewall is a common way to make a firewall.
- In this solution you restrict access to different ports using the packet filter from TCP/IP Properties Advanced Addressing IP and TCP/IP Security dialog boxes.
- One thing to remember is to disable access to SMB/NetBIOS from outside. These are in the ports TCP 139, UDP 137 and 138.

Windows NT Security

- With network bindings you can create a pseudo-firewall in Windows NT. It is recommended only for small networks. The purpose of a pseudo-firewall is to remove access to NetBIOS/SMB from outside.
- The recommended way to use a pseudo-firewall is to have a designated gateway machine running TCP/IP protocol services like WWW, Gopher, FTP, SMTP,Telnet.
- In the internal network TCP/IP client parts of these protocols are run in Windows NT computers, but not the server parts.
- Network bindings are enabled or disabled from the Network Applet in the Control Panel.
- Exercise, try setting up a firewall on Windows 2000 in the lab. Windows'2000 security differs at least in menus from that of NT but we will skip it now.

Windows NT Security

- **Vulnerability to viruses**
- NT replaces DOS interrupts and ROM BIOS interrupts by new devise drivers called Virtual Devise Drivers.
- But my library does not contain detailed knowledge of them, so all I can say is based on the good book (Internet Security) and the content of its floppy disc with 6 chapters on Windows NT.
- Usually a PC, or any Intel *86 series of computer has interrupts, hard and soft. It is part of the processor architecture.
- It seems that the interrupt routines are replaced by new routines, but whether their addresses are in the interrupt vector table (IVT), or if the table is also changes, is unclear.
- I assume there is the IVT. In that case interrupts cause a jump on a routine pointed out by that table.

Windows NT Security

- A floppy boot sector virus or a master boot sector virus will be executed before Windows NT is loaded. The processor is in the basic (normal 16 bit unprotected) mode.
- The virus routine can access anything and do anything.
- Fortunately what most boot viruses do is that they try to hook up to an interrupt (DOS or ROM BIOS) and stay as TSR-programs.
- This will totally fail as when Windows NT is loaded it will write over the interrupt vector table addresses and the virus TSR will never be called.
- A floppy boot sector virus may manage to write itself to the Master Boot Sector (MBS), but only before NT starts, since after that all writes to boot records on the hard disc are disabled.

Windows NT Security

- If the boot sector virus destroys files or changes Windows NT binaries while it has complete control over the system, it will manage to do so.
- A Partition Boot Virus could work just the same, but probably a DOS virus will not function correctly. A virus made for Windows NT should do just fine in the partition sector.
- There is a special concern of Windows 95/DOS partition boot sector viruses. If a user installs Windows NT with multiple boot to DOS, and there is an infected DOS with a viral partition boot sector, then this sector will be copied to another place by Windows NT set-up program and non-Windows NT aware antiviral programs cannot find the virus.
- The virus will still be viral if the user boots into DOS/Windows 95.

Windows NT Security

- Direct action DOS-viruses usually work fine in Windows NT from a DOS-window. This is because Windows NT emulated DOS interrupts do what the virus asks them to do. If the virus tired to use ROM BIOS interrupts, they would not work, but direct action viruses usually call DOS.
- A direct action file virus is such a file virus which does not try to make a TSR-program but when executed immediately finds another file and infects it. (These are the simple viruses to catch, you can easily figure out which file is viral from looking at the hard disc LED).
- A file virus trying to write itself into the boot sectors of the hard disc would not manage to do so in Windows NT. These writes are disabled. It could write itself on a boot sector of a floppy disc, this is allowed in NT.

Windows NT Security

- A virus in a DOS-window or a virus contained in a Windows 95/3.11 file will not be able to infect other files than those in that window.
- Provided that there are access controls used. A single person NT may not have any access controls set.
- DOS/Windows 3.11 file viruses trying to make a TSR-program will hook to a wrong interrupt routine. They will not be called ever. I am a bit confused by this - let us say, if a file virus tries to modify the code of DOS or ROM BIOS interrupt routine, that code will not be called as DOS or ROM BIOS services are not used. But, if the virus changes an entry in IVT, will it be called?
- Macro viruses work just fine in Windows NT.
- The bonus chapters of the good book state, that native Win32 viruses can write to the boot sectors.

Windows NT Security

- Let us make a thought experiment:
- If a macro virus is sent to the administrator, he starts it and the macro virus downloads, decrypts from an image or obtains in another way a Win32 virus and starts it.
- The virus establishes itself into a Virtual Devise Driver interrupt, I would suggest hooking the interrupt handling errors like memory protection.
- Then the virus tries to read memory outside its access limits forcing the memory protection interrupt to be executed.
- It writes a virus to the Master Boot Sector and makes an invalid operation causing the system to crash.
- The user reboots the system from the hard disc having disabled boot from floppy for security reasons.
- The MBS virus is executed and modifies the binaries of Windows NT enabling NetBIOS from outside. Are you in?

Windows NT Security

- Using bugs in Windows NT may not be so easy as in Unix :
- It has C2 classification, so the code is likely to be not so bad.
- The code is written with security in mind, not like Unix.
- Code is probably written in C++ with stronger type checking rather than C where there is no type checking.
- No open sources like Unix or detailed books like for DOS.
- (DOS and PC was nicely documented in many thick books)
- Disassembling takes time and work. Finding holes in version updates are more of a problem if no source is available.
- Still, it would be hard to believe that when reading from any configuration file etc. there would always be a check for the size of the parameter.
- As long as there are easier systems, Windows NT may not be the main target, so bugs will not be searched so much.

Windows NT Security

- **NTFS File system security**
- The old FAT (File Allocation Table) file system is still supported. In NT FAT file names can be long and contain spaces. For compatibility FAT is likely to be used also in Windows NT.
- If you use FAT file system, you still can boot to DOS and use the undelete command. Windows NT does not support undelete. This maybe leads some people to using FAT file systems in all but the Registry.
- However, FAT files cannot be protected by Window NT user-level security.
- You cannot turn off power while editing FAT-files, they may be left in corrupted state. NTFS does not have this problem.

Windows NT Security

- Why use NTFS file system?
- It is faster for large file systems (FAT uses an unordered linked list, NTFS has a binary tree)
- It can support much bigger files.
- On this course the reason is that NTFS has access controls given by permissions to files and directories.
- Permissions are not the same thing as rights given by the Registry. You cannot view permissions for a file like in Unix.
- NTFS files are not compatible with DOS, OS/2 or any other file system.
- The files are compressed.
- The files are too large to store on floppies.

Windows NT Security

- NTFS supports several streams in the files. This means, that you can have properties attached to a file. It is used by NT to support Macintosh files.
- Try the following as an administrator:
- echo This is data stream > Streamdemo.txt
- type Streamdemo.txt
- (types the text you wrote)
- echo This is hidden stream > Streamdemo.txt:NewStream
- type Streamdemo.txt
- (types the text This is data stream)
- more < Streamdemo.txt:NewStream
- (types the text This is hidden stream)
- What does this show? Files can contain hidden streams.

Windows NT Security

- NTFS files and directories have an owner. Usually the owner is the creator. FAT-files do not have owners.
- If the owner is an administrator, the files are co-owned by the whole administrator group.
- This is a good reason for a user not to use administrator rights in normal computer usage.
- You can review the ownership from network Properties menu.
- An administrator can change file ownership. Also the owner can grant permission to take ownership. The creator can remove administrator’s rights, but the administrator can take the ownership and then gain access.
- The file permissions are in Access Control List (ACL) as Access Control Entries. MicroSoft calls NT access control method discretionary access.

Windows NT Security

- When a user logs into the computer, SID and group SIDs are generated. They are in the access token created by Security Accounts Manager.
- If the user tries to access an NTFS resource, there is a loop through Access Control Entities. The loop stops if:
- There is an Deny for the SID,
- there is an Allow for the SID,
- or the end of ACL is encountered.
- Then the user gets a handle to the resource (file).
- It an intruder could change the order of ACEs so, that there is an Allow before Deny, then he would get access even if there is a Deny later in the list.
- All professionally sold Windows NT applications always put Deny ACEs to the beginning of the list.

Windows NT Security

- **Summary**
- Windows NT is a reasonably secure operating system for a remote hacker from an outside network, if configured correctly.
- Class C security is probably the best we can hope for from an operating system that runs on a standard PC and is not too difficult to use.
- There are many standard security mechanisms, login, access controls, firewall, some protection for most common viruses etc.
- Much of the security is created by unfamiliar services. like the Virtual Devise Drivers, NTFS file format etc. These can be reverse engineered and then we can expect more problems.
- However, if MicroSoft makes new versions with the same pace as before, a hacker may not have time to reverse engineer a system before a new improved totally different version comes.

Windows NT Security

- Windows NT can be quite insecure if configured poorly.
- Good login names should be selected.
- Booting from DOS and double boots are dangerous, maybe remove them and put CMOS settings behind a password.
- FAT-file system is not secure, use NTFS.
- Use restrictions to files to protect against viruses.
- Remove NetBIOS/SMB from outside, configure firewall capabilities.
- Do not open email attachments as an administrator, do not use administrator identity for every day operations.
- Use antivirus software, macro viruses and some DOS viruses still work, Windows NT viruses are sure to come.
- There is no detailed knowledge of bugs, there may be bugs.

Windows NT Security

- Exercise for the group working on Windows 2000:
- Using the bonus chapters on the CD of Internet Security of NT security features, or a book on Windows'2000 security.
- investigate the security features of Windows 2000,
- evaluate what security features are in use there,
- put the system to a more secure state,
- make some holes and try to use them from outside,
- report the configuration as it was, evaluate if it is secure, report the changes, report if your attack succeeded.

- Attacker: ask the Windows 2000 group to make some vulnerability, like NetBIOS/SMB to be available.Try to use this vulnerability.
- Find and try IIS (Internet Information System) vulnerabilities.