



TEKNILLINEN KORKEAKOULU

Malware, Intrusion Detection, E-mail Security



- Viruses and other malware
- Intrusion Detection Systems
- Securing e-mail



- A general term for all kinds of software with a malign purpose
 - Viruses, Trojan horses, worms etc.
 - Created on purpose
- Can
 - Prevent correct use of resources (DoS)
 - Cause general malfunctions
 - Destroy information
 - Modify information
 - Transmit information to unauthorized parties, also randomly
 - Enable others to have a complete control over a computer
- Secondary effects
 - Can disturb critical systems
 - Our society is controlled by computers



Types of Malware

- Trojan horses
 - Programs that promise something good, but instead or in addition do something nasty when you run them
 - Examples: root kits, games with backdoors, etc.
 - Do not spread automatically
 - Can open existing security vulnerabilities or create new ones
 - Some software allows complete control of the target host
- Spyware / Adware
 - Software, which the user installs and which sends information about the user's actions to a server
 - Often financed by advertising
 - Possibly legal, if the user is told of the privacy issues



...Types of Malware

- Viruses
 - Self-replicating software
 - Attach themselves to other executable content
 - Program files
 - Boot sectors on disks
 - Documents with macro instructions
 - Currently the biggest problem are macro viruses in various Windows software
 - MS Office macros, Visual Basic
- Worms
 - Network aware viruses that propagate as independent programs and usually use security vulnerabilities to enter different host computers



...Types of Malware

- Hostile Java applets and ActiveX components
 - User may not even notice he is running an active component on his computer
 - Component certification doesn't mean the component cannot be a Trojan, it is only intended to identify the source of the software component
 - Java's sandbox is in theory fairly secure, but vulnerabilities have been found
 - ActiveX does not limit the component in any way
- “Remote administration” programs
 - Examples: NetBus, Back Orifice
 - Can be packaged inside Trojan horses



How Does a Virus Spread?

- For example a simple MS-DOS virus:
 - Moves part of a program's binary code from the beginning of the file to the end and places itself in the beginning
 - When the program is run the virus activates and places its code into the computer's memory and hooks to the operating system so that the code is periodically activated
 - Then replaces the original program's code to the correct place in memory and allows the program to be executed
 - When the OS activates the virus in the memory, it infects other files and possibly performs some additional tasks



How Do Macro Viruses Spread?

- Macros are small application specific programs stored in the application's data files
 - The structured environment and high level services make life easier for the viruses
- The viral macro is stored among other macros and is configured to automatically activate when the document is opened by the application
 - After activation the macro can easily copy itself to other documents
 - The macro can also use other available services and for example send random documents using e-mail



Viruses for Purposes

- Viruses can be used to take over hosts in the network environment
 - E.g. the virus spreads as e-mail and inserts a small network server to the target system
- The captured servers can be used for various purposes
 - DoS attacks
 - E-mail spamming
- Spammers are actually doing this
 - An easy way to take over a large amount of hosts and to use them for sending e-mail
 - This is a business, with some money moving, also illegal in most countries
 - The spam mail is used to gather contact information about potential customers and sold to legitimate companies



How to Defeat Viruses?

- Avoid environments that actively support viruses
 - E.g. Microsoft Office tools
- Promote diversity by using less popular operating systems
 - Popular operating systems are more likely to attract viruses
- Use a virus scanner that knows the signatures of different viruses
 - The virus signature database needs to be updated frequently
 - Virus scanning program manufacturers currently share new viruses efficiently and focus on keeping the scanning programs up to date
 - Heuristic scanning that would recognize “bad intentions” of a program has been proposed frequently, but it does not yet work
 - The virus scanner can remove the virus from the host file or destroy the file
 - The scanning can be done for every file when it is opened
 - The scanning can also be done to file servers or at firewalls



Intrusion Detection (ID)

- E. Amoroso: Intrusion Detection is the process of identifying and responding to malicious activity targeted to computing and network resources.
- Houses may have surveillance cameras and burglar alarms; information systems may have intrusion detection
- Another analogy: network management systems (SNMP)
- Categories:
 - Attack detection
 - Intrusion detection
 - Misuse detection



Why Detect Intrusions?

- Knowledge of ID may scare intruders off (at least it keeps the honest people honest)
- Measured figures of actual attacks help establishing a budget for security administration
- A chance of reacting to the attack:
 - You may be able to stop the intrusion before anything catastrophic happens
 - You know what has happened so you can manage the damage
 - You can try to stop it from happening again
- Also for monitoring own staff
 - Likely to be illegal in many countries



How Intrusion Detection Works?

- The computers and/or the network traffic is monitored
- The data is collected and analyzed
 - Manually or automatically
 - Known attacks can be identified by their *signature*
 - If the *baseline behavior* of the system is known, anomalies can be identified
 - Sometimes the baseline is known exactly, e.g. between front end and database servers
- An operator can make decisions based on the data



Intrusion Detection Setup

- Typically there is sensor software in or near the firewall and other critical network points and in the server computers
- Information is collected to an analysis station
- Preferably the ID system uses an network of its own
- The attacker may be deceived by honeypots
 - Computers which look like worth breaking into, but are decoys
 - Even look-alike shells written in Perl exist



Criticism of Intrusion Detection

- Generally either produces many false positives or misses real attacks
 - Requires a trained (expensive) operator (24/7?)
- Automatic intrusion protection can be in effect automatized DoS service for attackers
 - prevention is always better than cure
- ID is by nature fail-open
- ID system may be used by crackers to create a diversion to camouflage the real attack
- Most anti-virus vendors have daily updates available from the Web; ID vendors issue updates a couple of times a year
 - The virus detection community shares signature information much more effectively than the ID community



Securing E-Mail Services

- The e-mail system is a good example of a service, which consists of several applications, protocols and hosts
- There are attacks towards the messages and the system itself
 - Eavesdropping, spoofing
 - Spam
 - Break-ins
- A comprehensive attitude is needed to protect the whole



The SMTP Protocol

- The basic SMTP (Simple Mail Transfer Protocol) used for transmitting mail messages over the Internet contains no security features:
 - It is possible to read your e-mail, as it travels in public networks and is stored in servers, that might be outside your control
 - It is generally easy to send e-mail messages with a forged sender address
- SSH and SSL can be used to protect the protocol sessions protecting messages in transit (but not in serveris)
- PGP and S/MIME can be used to encrypt and sign messages, providing end-to-end security



- Sendmail is usually delivered as a default SMTP server on UNIX boxes
 - Very powerful and difficult to understand configuration
- Hardening Sendmail
 - If no local delivery (e.g. relay only), can be run as non-root
 - Can be run chrooted
- Replacing Sendmail
 - One alternative for UNIX platforms would be qmail
- Most software (SMTP, POP and IMAP servers) have had major security problems
 - Buffer overflows etc.



- The SMTP server must be configured to avoid spam
 - No relaying by default
 - Nobody should be able to use our server to spam others
 - Sender domain must resolve from DNS
 - Sender addresses must be replyable
 - A whitelist or a blacklist of known good/bad addresses can be used
 - E.g. ADSL customers should not send e-mail directly, but use the operator's server
- Heuristic (Bayesian) analysis
 - A system which learns to recognize spam
 - Must be trained
 - Useful to analyze incoming mail



- Viruses exist
- Attacks exist
- Spam exists
- There is no brief solution to these problems, instead we should protect ourselves