Security and Ethics

Lecture #10

Department of Computer Science and Technology
University of Bedfordshire

Written by David Goodwin,
based on the lecture series of Dayou Li
and the book *Understanding Operating Systems* 4^{th} *ed.*
by *I.M.Flynn and A.McIver McHoes* (2006).

Operating Systems, 2012

Role of OS in security

- OS has access to every part of the system.
- Vulnerability at OS level opens up the entire system to attack.
- The more complex and powerful the OS, the more likely it is to have vulnerability to attack.
- System administrators must be on guard to their OS with all available defences against attack and possible failures.
- OS role in security relates to system survivability, protection, backup and recovery.

System survivability

- The capability to fulfil its mission, in a timely manner, in the presence of attacks, failures and accidents
- Key properties
  - Resistance to attacks
  - Recognition of attacks and resulting damages
  - Recovery of essential services after an attack
  - Adaptation of system defence mechanisms to mitigate future attacks

Strategies for survivability

- Resistance to attack
  - strategies for repelling attacks
    - Authentication
    - Access controls
    - Encryption
    - Message filtering
    - System diversification
    - Functional isolation

Strategies for survivability

- Recognition of attacks and damages
    - Strategies for detecting attacks and evaluating damages
        - Intrusion detection
        - Integrity checking

Strategies for survivability

- Recovery of essential and full services after an attack
  - Strategies for limiting damages and restoring compromised information or functionality, maintaining or restoring essential services within mission time constraints, restoring full services
    - Redundant components
    - Data replication
    - System back up and restoration
    - Contingency planning

Strategies for survivability

- Adaptation and evolution to reduce effectiveness of future attacks
  - Strategies for improving system survivability based on knowledge gained from intrusions
    - Intrusion recognition patterns

Level of protection

configuration	ease of protection	relative risk	vulnerability
single computer without email or internet	high	low	compromised passowrds, viruses
LAN without internet	medium	medium	sniffers, spoofing (+viruses, passwords)
LAN with internet	low	high	Email, web services, FTP, Telnet (+sniffers,spoofing, passwords, viruses)

Backup and recovery

- Layered backup schedule – back up weekly entire system and daily only files changed on the day
- Copies saved for 3-6 months on a safe off-site location
- Backup becomes significant when a virus infects the computer – eradication software can be run and damaged files reloaded (though changes have to be regenerated)
- Safe off-site backup crucial to disaster recovery such as water, fire, malfunctioning sever, corrupted archival media and intrusion from unauthorised users
- Policies and procedures and regular user training are essential

Security breaches

- Unintentional intrusions
- Intentional attacks
    - Denial of services attacks
    - Making services not available (e.g. over the Internet)
    - Browsing
    - Directory or data in memory / disk from previous process / file
    - Wire tapping
    - Listening / collecting information (e.g. passwords for later access) bypassing authentication
    - Repeated trials (guessing authentic passwords)
    - Trap doors (including backdoor passwords)
    - Unspecified and undocumented entry points to systems
    - Trash collection / dumpster diving

Viruses and worms (1)

- Virus
  - a small program that alters the way a computer operates without the permission or knowledge of the user
  - Self-executing – often placing its own code in the path of another
  - Self-replicating – accomplished by copying itself from an infected file to a clean file
  - Targeting certain OS exploiting known vulnerability in the system software – hence important to correctly update the OS with patches

Viruses and worms (2)

- Types of virus
  - File infector
    Normally resident in memory and infect executive files in the OS
  - Boot sector
    Infect the boot sector (disks and hard drives) when the computer is booted up (powered on)
  - Master boot record
    Infect the boot record of a disk saving a legitimate copy of the master boot record in a different location on the volume
  - Multipartite
    Infect both boot record and program files making especially difficult to repair
  - Macro
    Infect data files such as word processing and spreadsheet

Viruses and worms (3)

- Worms
  - Memory-resident program that copies from one system to the next without requiring the aid of an infected program file
  - Immediate result – slower processing of legitimate work as the worm siphons off processing time and memory space
  - Particularly destructive on networks
  - Morris Worm – the first widely destructive worm infected more than 6000 systems over several days in 1988. It was installed from a university computer and spread overnight to hundreds of other universities.

Viruses and worms (4)

- Trojan Horses
  - A virus disguised as a legitimate / harmless program
  - Sometimes carries within itself the means to allow the program creator to secretly access the user system
  - Replaces the standard login with an identical fake login to capture the keystrokes
    - The user sees a login prompt and types in user ID
    - The user sees a password prompt and type in password
    - The rogue program records user ID and password and send a typical login failure message to the user, and returns to legitimate program
    - Now the user see the legitimate login and types in user ID
    - The user then sees the legitimate password prompt and types in password
    - Finally the user gains access, unaware that the ID and password were stored by the rogue program

Viruses and worms (5)

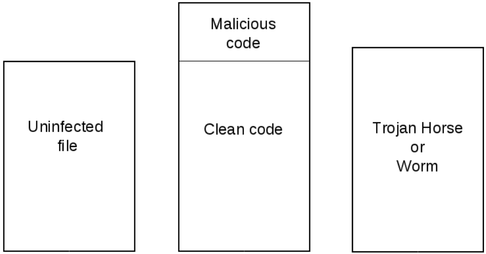
- Bombs
  - A logic bomb is a destructive program with a fuse – triggering event (e.g. keystroke or Internet connection).
  - A logic bomb often spreads unnoticed throughout a network until a predetermined event when it goes off and does the damage.
  - A time bomb is triggered by a specific time such as a day of the year.
  - Example –
    Michaelangelo discovered in 1991 was designed to execute on the birthday of Michaelangelo (6 March 1475) when a computer is booted up. It overwrote the first 17 sectors on heads 0-3 of the first 256 tracks of the disk making subsequent boot difficult.

Viruses and worms (6)

- Blended threats
  - Combines characteristics of other attacks
  - Harms the affected system
  - Spread to other systems using multiple methods
  - Attacks other systems from multiple points
  - Propagates without human intervention
  - Exploits vulnerabilities of target systems

Virus and worms (7)

- Antivirus software is capable of repairing files infected with a virus but it is generally unable to repair worms.



System protection

- Vulnerabilities – file downloads, email exchange, vulnerable firewalls, improperly configure Internet connections
- Regularly running antivirus software (preventive and diagnostic)
- Using up-to-date firewalls
- Authorised individual access only
- Using encryption where necessary

Antivirus software

website	**organisation**
csrc.nist.gov	Computer Security Division of the National Institute of Standards and Technology
www.cert.org	CERT Co-ordination Centre
www.ciac.org	U.S. DOE Computer Incident Advisory Capability
www.macfee.com	McFee, Inc.
www.sans.org	SANS Institute
www.symantec.com	Symantec Corp.
www.us-cert.gov	U.S. Computer Emergency Readiness Team

Firewalls (1)

- Firewall
  A set of hardware and/or software to protect systems by disguising its IP address from outsiders who have no authorised access or ask for information about it
- Typical tasks
  - Log activities that access the Internet
  - Maintain access control based on sender / receiver's IP address / services requested
  - Hide the internal network from unauthorised users
  - Verify that virus protection is installed and enforced
  - Perform authentication based on the source of request from the Internet

Firewalls (2)

- Fundamental mechanisms
  - Packet filtering
    The firewall reviews the header information for coming and outgoing Internet packets to verify that the source address, destination address and protocol are correct.
  - Proxy server
    It hides important network information from outsiders by making the network server invisible.

Authentication

- Verification that an individual trying to access a system is authorised to do so
- Kerberos – a network authentication protocol developed as part of the Athena project at MIT
- For password encryption for network security, Kerberos provides strong authentication (using strong cryptography – the science of coding messages) for client/server applications
- Free open-source implementation available at www.mit.edu/kerberos/

Encryption

- The most extreme protection for sensitive data
- Data put in a secret code
- Total network encryption – all communications within the systems are encrypted
- Partial encryption – may be used between the entry and exit points of a network, or other vulnerable parts
- Storage encryption – information stored in an encrypted form and decrypted when it is used
- Increased system overhead
- The key must be kept securely for decryption

Password management (1)

- Password
  - Most basic technique, needing careful user training, forgettable, unlikely to be changed frequently, commonly shared, considered bothersome, etc.
- Password construction
  - Stored in encrypted form for security reason
  - Contains a combination of characters and numbers – minimum length, use of misspelled words / joint bits of phrases, certain pattern on keyboard, acronyms, etc.
- Password alternatives
  - Smart card
  - Biometrics – face, fingerprints, iris, etc.

Password management (2)

- Dictionary attack
    - It is a method to break encrypted passwords, requiring a copy of the encrypted password file and the encryption algorithm.
- Social engineering
    - Looking in and around the user desktop for a written reminder, trying the user logon ID as the password, searching logon scripts, and even telephoning friends and co-workers to learn the names of a user's family members, pets, hobbies, etc.
- Phishing
    - Intruder pretends to be a legitimate entry to ask unwary users to confirm their personal and/or financial information via the Internet, email or telephone.

Ethics (1)

- Ethical behaviour – be good and do good.
- IEEE and ACM issued a standard of ethics for the global computing community in 1992.
- Unauthorised users can have severe consequences
  - Illegally copied software
  - Plagiarism / unauthorised copying of copyrighted work
  - Eavesdropping on email, data or voice communications
  - Cracking / hacking to gain access another system and monitor or change data
  - Unethical use of technology – unauthorised access to private/protected computer systems or electronic information (murky area of law though)

Ethics (2)

- Education of ethical behaviour
  - Publish polices that clearly state actions that should and should not be conducted
  - Run regular seminars on subject including real-life case histories
  - Conduct open discussions of ethical questions (e.g. it is ok to read someone else's email or is it ok for someone else to read your email?)
  - Useful information on Ethics and Professional Conduct from ACM at www.acm.org