Department of Computer Information System

Faculty of Information Technology

And Computer Science

Elements of Computer Security

Author: David Salomon

Yarmouk University

Chapter 01

Physical Security

2012/2013

Done by: Osama Alkhoun

Mobile: 0796484613

Contents:

1. Side-Channel Attacks

- Physical security is important but not enough.
- Behind locked doors, information can be leaked.
- An old idea, eavesdropping radiation for monitors.
- Modern monitors use LCDs or plasma screens that presumably don't radiate, but in the past, the only countermeasures to *side-channel attacks* were to either surround a computer room with a conductive material, to block any electromagnetic radiation from escaping, or to have a guarded, empty area around the entire building and move the parking lots away from the building.
- An important class of side-channel attacks is the so - called *timing attacks*.
    - A timing attack uses the fact that many important computational procedures take an amount of time that depends on the input.
- Thus, by measuring the time it takes to complete a procedure, a spy can learn something about the input to the procedure.
- An important example is the RSA encryption algorithm (see document on cryptography in the book's Web site).
- Part of this algorithm computes an expression of the form a^b where b is the encryption key.

1.2. Acoustic Keyboard Eavesdropping

1. A keystroke logger is a program that records every keystroke the user makes, and stores this data or transmits it to its owner (the spy).
2. A similar concept is a screen capture, a program that periodically takes a snapshot of the monitor screen and saves it or transmits it outside.
3. There are programs that identify and delete spyware, but spying on a computer can also be done physically.
4. A crude idea is to try to spy on a computer user by looking behind their shoulder, but a more practical, more sophisticated technique is to install a miniature radio transmitter inside a keyboard, to transmit keystrokes to a nearby spy.
5. Such a transmitter is a physical threat and cannot be detected by spyware -removal software.
6. The idea of *acoustic keyboard eavesdropping* is for a spy to hide a microphone as close as possible to a keyboard, to record the sound made by the keys when pressed, to digitize the sound, and to send the audio samples to a computer program controlled by the spy.
7. Experiments have demonstrated that a sensitive parabolic microphone can record keyboard sounds reliably from distances of up to 50 feet (about 17 meters) from the keyboard even in the presence of background noise.

2. Physical Threats

1. Surges in electrical power, often caused by lightning, may burn out electronic components in the computer.

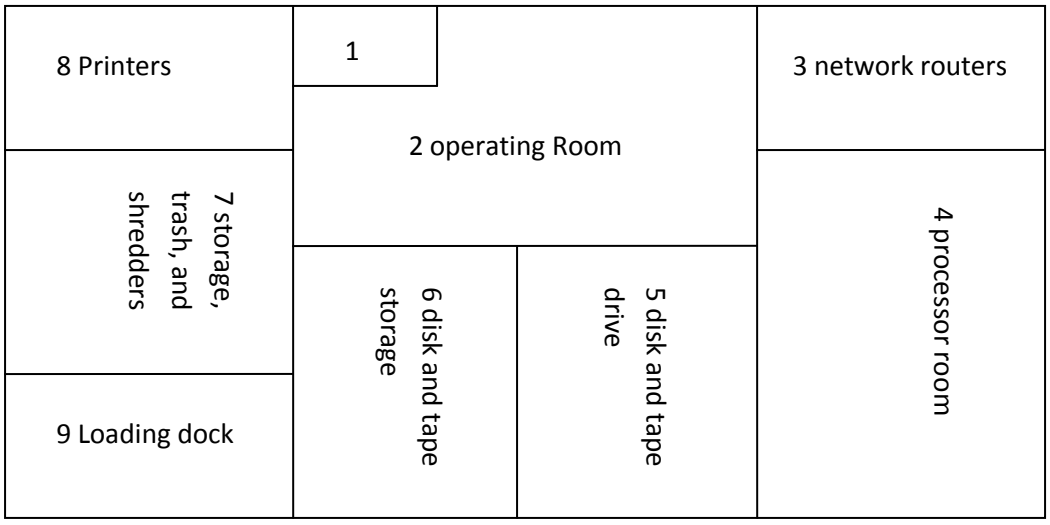
   Solution: Use an uninterruptible power supply (UPS).

   a. Such a device regulates the incoming voltage and produces a clean output signal. If the voltage gets high, the UPS trims it.
   b. If the voltage drops, the UPS uses its internal battery to supply the computer with power for a few minutes, enough to either turn off the computer (typical for a home computer) or to start a generator (typical in a large installation, especially an installation that has to operate continuously, such as a hospital or a telephone exchange).

2. The best virus protection software cannot prevent a home personal computer from being stolen.
3. Computer security starts by protecting the facilities that house computers and computer data. This problem is especially acute in industry.
   a. Many a company can be wiped out if its computers and especially if it's sensitive data are stolen or damaged.
4. Damage can be intentional, inflicted by a criminal or a disgruntled employee, or accidental, caused by fire, power failure, or broken air conditioning.
5. A facility using electronic locks and keys or other physical-identification
6. Devices to restrict access to certain areas should consider the following problem, known as piggybacking or tailgating.

7. An intruder may wait at a locked door, perhaps holding disks, paper or other innocuous - looking stuff with both hands, trying to look legitimate and waiting for the door to open.
8. When someone comes out of the restricted room, the intruder slips in while the door is still open.
9. A guard can prevent such a problem, but this is an expensive solution.
10. An alternative is to install a turnstile, or even a mantrap.
11. The latter device is a two-door entrance where a person has to pass through two doors in order to enter or exit a restricted room.
12. To enter, a person must pass through door A into a small space, the mantrap, and then open door B to the restricted room. The point is that door B will not open until door A is fully closed.

Design for Computer installation



- **Magnetic Fields.**
  1. Hard disks are magnetic storage. Data is recorded in small magnetic dots on the disk and is therefore sensitive to magnetic fields.
  2. (In contrast, CDs and DVDs are optical storage and are not sensitive to magnetism.) Experience shows that it is not enough to place a small magnet in your pocket and walk into a computer room, hoping to harm computers and data.
  3. Stronger fields are needed in order to adversely affect magnetic storage, but such fields exist.
  4. An old story, from the 1960s, tells of a computer tape storage room where tapes were always going bad. It took months until someone observed that the trouble affected only the tapes stored on the lower shelves. It turned out that the floor was cleaned periodically with a powerful vacuum cleaner that affected only those tapes.

- **User Tracking**

1. Imagine a facility with many computers and many workers, where a user may perform a task on a computer, move away to do something else, and then step to the nearest computer to perform another task.
2. A good example is a hospital with doctors and nurses treating patients and updating patient records all the time.
3. Another example is a lab where tests (perhaps blood tests or forensic tests) are performed by workers, and a worker has to enter the results of a test into a computer.
4. In such a situation, it is important to keep track of which employee used what computer, when and for what purpose. The simplest solution is to assign each user a password.
5. The user has to log into the computer, perform a task, and then log off. In the hospital example, where emergencies may and do occur often, such a procedure is too time consuming and unrealistic.

- **Physical Protection of Data**

1. Data is normally stored on devices that can easily be damaged or destroyed.
2. Paper, magnetic disks, CDs, and DVDs are sensitive to fire, magnetic fields, or scratches. Data stored on such devices deteriorates over time even under ideal storage conditions.
3. Thus, data has to be physically protected, and this can be achieved by backing up sensitive data periodically, so that a fresh backup is always at hand.
4. A home computer should have two external disks (or rewritable CDs or DVDs), one kept at home and the other kept in a different location, such as a friend's home.
5. Periodically, perhaps once a week, the computer owner should backup the data onto the external disk located at home, and swap the two backup disks.
6. This way, there is always a fresh (i.e., at most one week old) copy of the data kept at a remote location.
7. Disk drives may also be responsible for another serious security problem that few users are aware of. Since 2002, most copy machines (copiers or Xerox machines) are made with an integral hard disk drive built into the machine.
8. Every document copied is recorded on this drive in a proprietary, compressed format.
9. This gives the drive a capacity to store hundreds of thousands of documents.

10. When such a machine is sold by its owner, the (unknown or forgotten) drive often remains in the machine and may contribute to a new type of breach of security.
11. The short video at [copy machines 10] illustrates the gravity of this problem.

- **Hard copy**

1. The media has been touting the paperless office for several decades, but we still use paper. In fact, we use it more and more.
2. Security workers know that criminals often collect papers thrown away carelessly and scrutinize them for sensitive information such as credit card numbers and passwords to computer accounts.
3. This behavior is part of the general practice of dumpster diving.
4. The solution is to shred sensitive documents, and even not- so sensitive papers.

- **Spying**
  1. Spyware, an important threat, is the topic of Chapter 9, but spying can also be done in the traditional way, by person.
  2. Industrial espionage and spying conducted by governments are very real.
  3. A commercial organization often decides that spying on its competitors is the only way for it to stay active, healthy, and competitive.
  4. Spying on computer users can be done by looking over someone's shoulder, peeping through a keyhole, setting a small security camera, planting spyware in a computer, and also in other ways,

- **Data integrity**
  1. Digital data consists of bits. Text, images, sound, and movies can be digitized and converted to strings of zeros and ones.
  2. When data is stored, in memory or on a storage device, or when it is transmitted over a communication line, bits may get corrupted.
  3. Keeping each bit at its original value is referred to as data integrity and it is an aspect of computer security.

- **Security Management.**
  - Three simple principles can significantly reduce the security threats posed by employees in a large computer installation.
  - Perhaps the most important of the three is the separation of duties.

1. ***The first security management principle***, employed by many spy, anti-spy, and secret organizations, says that an employee should be provided only with the knowledge and data that are absolutely necessary for the performance of their duties.
    - What an employee does not know, cannot be disclosed by him or leaked to others.
2. ***The second security management principle*** is to rotate employees periodically. An employee should be assigned from time to time to different shifts, different work partners, and different jobs.
    - Also, regular annual vacations should always be mandatory for those in security-related positions.
3. ***The third security management principle*** is to have every security-related task performed by an employee and then checked by another person.
    - This way, no task becomes the sole responsibility of one person.
    - This principle allows one person to find mistakes (and also sabotage) made by another.
    - It slows down the overall work, but improves security.

3. Laptop Security

- A laptop computer is handy. Those thin, small, lightweight machines are truly portable and can increase a person's productivity.
- Unfortunately, they also increase the appetite of thieves. You may have asked yourself why so many people eye your laptop when you carry it in public.
- As many know from their misfortune, one common answer is: people consider a laptop a target. Thus, securing a laptop is a (physical) computer security problem.
- Perhaps the most secure solution is to chain the laptop to your wrist, so it becomes your Siamese twin. Although very safe, this solution is uncomfortable, especially during meals and bathroom visits, and may be rejected out of hand (out of wrist?) by most laptop users.
- The next best thing is to tie the laptop to a large, heavy object, often a desk, with a lock such as a bicycle lock
  (but if the lock opens with a combination instead of a key, make sure you set it to a random number and not to 123, 666, or another, easy to guess number).

- **Mac Hacking**
  - Traditionally, the Macintosh platform has suffered much less from hacking and security related problems (except theft) than computers running the Windows or UNIX operating systems.
  - One plausible explanation for this is that there are relatively few Macintosh computers (only 12–16% of the total number of personal computers, according to some estimates).
  - One reason for a hacker to spend time and effort on hacking activities is the satisfaction of breaking into many computers and being able to brag about it.
  - Macintosh hacking can never result in breaking into many computers, thereby giving hackers a disincentive. Another theory for the relative safety of the Macintosh is that its operating system has always been more secure than Windows and UNIX. This feature, if ever true, has changed since the introduction of the Macintosh OS X, which is based on UNIX.
  - Attacking version X of the Macintosh operating system isn't much different from UNIX hacking, and may attract intruders. A quick Internet search locates many items about hacking the Apple Macintosh.

4. **Disaster Recovery Planning**
    - A disaster recovery plan is an important part of any organization, whether commercial, charitable, or governmental. It details the steps required to quickly restore technical capabilities and services after a disruption or a disaster.
    - The idea in such a plan is to minimize the impact that a catastrophic event will have on the organization.
    - The details of such a plan depend on the nature of the organization and are different for different emergencies, but they have to touch upon the following aspects of the organization:
        - **Operation**: The plan should provide for continuous operation of the organization. In certain emergencies there may be periods where the organization will not function, but they should be minimized.
        - **Reputation**: The name, brand names, trademarks, products, and image of the organization should be preserved by the plan.
        - **Confidence**: A well-thought-of plan should increase the confidence of employees, clients, investors, and business partners of the organization.

- Developing such a plan consists of the following key steps:
    - The basic components of the organization, such as human resources, equipment, real estate, and data should be identified and assigned monetary values.
    - The basic components thus identified should be ranked according to importance and qualified personnel should be assigned to each element. Those people should develop recovery details for their component of the organization and should carry out the recovery plan in case of a disaster.
    - Once the plan is in place, it should be disseminated to all employees and should be practiced and rehearsed on a regular basis. Several times a year, management should reserve a day where a certain emergency will be simulated, and the recovery plan carried out as realistically as possible.

5. Privacy Protection

- This section describes two approaches to protecting privacy,
  - *The first is based on sophisticated lying* and
  - *The second is based on perturbing a random variable*.

- The first is based on sophisticated lying.
  - Just lying to a social researcher isn't very useful and may not serve any purpose. It may also sound wrong and may raise suspicion. Why would
  - Anyone agree to give out personal information and then invent wrong data about themselves?
  - The answer is, to receive a gift. No one is going to give away their household income level for a song, but many are willing to provide information on their online shopping habits for a free popular song or for large, free disk space on some company's computer.
  - Often, people provide wrong information, a habit which this author does not condone, but if you insist on lying, at least do it properly.

- The second is based on perturbing a random variable.
  - When we buy a product, it always includes a registration card that asks for our name, address, age (or age group), family income, and other personal information. People often fill out this card and mail it, or register online, lest they lose the product's warranty.
  - On the other hand, afraid to surrender their privacy, they often lie about their personal data.
  - The point is that the manufacturer doesn't need to know the age of every buyer and user of a product. All that the maker of a product would like to know is the statistical distribution of the ages; how many users are 18 years old, how many are 19, etc. This is the basis of the second approach.
  - The distribution of the random numbers is important, but knowing this distribution may help a hacker to break this method of privacy protection and to estimate the original data fairly accurately.