6.915 Computer and Network Security	**Fall Term, 1995**
Lecture 2 : September 12, 1995	
Lecturer: Ron Rivest	*Scribe: Chia-Ying (David) Yang*

1 Physical Security

Physical security is the basis of computer security. We are going to discuss the two main uses of physical security: protection against natural risks and malicious attacks.

1.1 Natural Risks

These natural risks are the most common threats to computer physical security:

- **Power interruption**: Power interruption may be hard to recover from. Sometimes it may result in permanent system damage, since electronic components are not designed to absorb sudden power fluctuations. UPS (uninterrupted power supply), surge protectors, alternative power generators are possible security measures.
  example: Neumann p. 16. AT&T backup battery drain.

- **Fire**: Smoke detectors and sprinklers are possible security measures. Make sure that the water from the sprinklers will not wet the systems, as this may cause electrical fire and/or water damage (see below.)

- **Storm, flood:** There are two distinctions to be made between raising waters and falling waters. The first happen in case of flood for example. Systems should be placed in high stands and possibly in higher floors of buildings (not in the basement.) Falling waters may happen because of leakage during heavy storms or because of fire alarm sprinklers. The easiest form of protection in this case is lots of plastic sheets. Others advocate the use of foam fire extinguishers instead of water ones .
  example: Neumann p. 56. Passengers were stranded in Sydney's monorail due to water damage to control computer.

- **Earthquake, Meteor, War**: These risks may destroy a whole building. In order to quickly restart the computer system first of all we need up to date backups (see section on backups below). Of course the backups should be kept in a separate place possibly miles away. In some cases a *cold site* may be needed, i.e. a facility with power, cooling and network connections (i.e., at least phone lines), available to install a computer system. For more critical task *hot sites* may be required. A hot site is a facility with a computer system ready to run and be used. The cost of maintaining a hot site is high but companies usually share the services of a single hot site provider (given the very rarity of use) making the cost fairly affordable.
- **Communications interruption**: To protect against accidental severance of communication lines, duplicate lines at different sites are needed.
  example: Neumann p. 17. Beaver chews on cables.
- **Operator error**: Errors such as coffee spills and accidental file deletion are very common.
  example: Chernobyl accident, 1986.
- **Software/hardware error**
  example: Neumann p. 68. Therac-25 chemotherapy machine fried several patients due to software bugs.

Backups: The most effective solution to many of these natural risks is to create backups. Many types of backups are possible– daily, weekly, and monthly, as well as full, incremental, and differential. Backups can be used either for quick restart or restoration of damaged systems, as well as for record keeping and tracking purposes. Backups should be separately stored in a secure place away from the system. Backups should be regularly tested to make sure that the data on the backups are intact. Also backups may contain sensitive information so they should be protected since they provide an attacker with a potential entry point to private data other than the computer system itself.

1.2 Malicious Attacks

1.2.1 Physical access control

Walls and **fences** define the security perimeter, while **guards** and **locks** enforce access control policy. Only authorized users may enter the perimeter. Possible security leaks include:

- **Masquerading**: A person disguised as an authorized user. This can be done using forged IDs or pretending to be a repair man.
- **Piggy-backing**: A person who enters the security perimeter by following an authorized user.
- **Lock-picking**: Any locked can be picked. Sometimes there is substantial savings over combinatorial brute-force.
- **Visual/auditory access**: An unauthorized person can gain passwords using binoculars, telephone bugs, etc.

Possible solutions to these attacks include:

- **Safes, doors with special locks**
  example: Hotel doors with special access keys based on a sequence of random numbers.
- **Motion detectors**
  example: the movie *Sneakers*.

1.2.2 Protecting computer systems

To prevent theft, computers can be locked to desks or other immovable furnitures. In addition, locks on computers or on media readers can render a stolen computer unusable.

1.2.3 Protecting media

Possible security leaks include:

- **Dumpster diving**: Shredded documents may yield secrets such as passwords and confidential information.
- **Magnetic storage media**: Deleted information can often be undeleted.
  example: Oil company that reads consultants' tapes before writing on them.

Possible solutions to these attacks include:

- **Clearing, purging, destroying**: *Clearing* overwrites data multiple times with some character. *Purging* eradicates data using, for example, ultraviolet light for EEPROMs or degaussing for magnetic media. *Destroying* completely destroys the media by, for example, burning or melting.
- **Zeroize disk on memory allocation**

Another facet of media protection is protection against software piracy. United States piracy rate is estimated at 35%, which results in $15.2 billion in loss per year. Software companies have devised these copy protection methods:

- **Bad tracks at known places on disk**
- A **dongle** is a special hardware that attaches to, for example, the serial port. It contains circuitry which is needed to run the software.
- **Serial number/manual text check**
- **Network address/CPU check**

Often the most effective copy protection is no protection at all. By lowering the price of the software or by providing excellent support services, many users are willing to buy their own copy of the software.

1.2.4 Protecting devices and circuitry

A device or circuit can use a key for short-term protection or incorporate protection into the design for long-term protection. There are two protection techniques: passive (preventive) and active (counter measures).

1.2.4.1 Passive protection techniques

- **Potting circuitry in epoxy** makes it hard to remove components for study.
- **Special "connoisseur" coating**
  example: A layer of alumina, silicon bits, and even sodium coating may be on chip, making it hard to etch. The sodium is even reactive, causing further damage when it is exposed. These special coatings are usually expensive.

- **Special 3D geometry** makes it hard for etching or milling to etch down to the circuit evenly...
- **Stress glassed substrate** on which the circuitry is built can shatter when the enemy tries to remove components for study.
- **Fake circuits** that do nothing can confuse the enemy.
- **Programmable circuits** makes it hard for visual circuitry study (if programming is done with, say, ion implants or polysilicon fuses.

Possible security leaks for passive techniques include:

- **Diagnostic circuits** built into some circuits may give away its functions (e.g. the ability to scan out all registers on the chip).
- **Underside of chip** is often neglected, and may provide an access route (etch away from backside).
- **Optical or infrared viewing**

1.2.4.2 Active protection techniques

- **Pressurized containers**: circuitry can be disabled when a loss in pressure is sensed.
- **Wires through epoxy potting** can detect damage to epoxy potting.
- **Self-destruct device** can destroy the circuitry if its security is compromised.

Possible security leaks for active techniques include:

- **Fast attacks** by the enemy may destroy counter measures before they are activated.
- **Slow attacks** such as liquid nitrogen may disable circuitry while leaving the charges detectable.
- **Power usage** and **timing** may give away sensitive information about functionality of chip.
- **Zeroizing** memory may not be enough, since long-term charge storage may cause physical changes such as ion migration.

1.3 Electromagnetic Radiations

Computers (in particular their screens and their communication lines) emit the electromagnetic radiation. It is possible for an attacker to make use of such emissions in order to create privacy breaches.

Computer CRT signals can be picked up from afar with simple, cheap equipment. Communications cable active tapping can be detected, but inductive tapping is much harder. Fiber optic cables can be tapped through bending, nicking, or placing in high-refractive liquids, which may cause some light to escape. In addition, the power lines also radiate signal energy.

It is possible to shield a computer, but it is difficult and expensive to do it well. TEMPEST is the name of the program of the U.S. Government under which computer equipment is certified as not emitting detectable signals. One approach is to surround circuits with metal shielding. Shielding the whole computer is hard, since the shield should enclose everything (including the screen ...) A good compromise is to use a fine copper mesh in front of the screen. Sometimes entire computer rooms or entire buildings are shielded.

> *The best electromagnetic radiation security is afforded when the equipment is switched off.*
> Peter Swinbank

2 Principles

The following principles can be gathered from what we learned about physical security:

- *If information is in physical form, it can be accessed by the enemy.*
- *Physical protection is at the foundation of computer and network security.*

3 Readings

Chapter 12 of the textbook deals with physical security. Also Peter Neumann's book *Computer Related Risks* (which is quoted in these notes) is a good collection of computer risks due to lack of adequate physical protection.