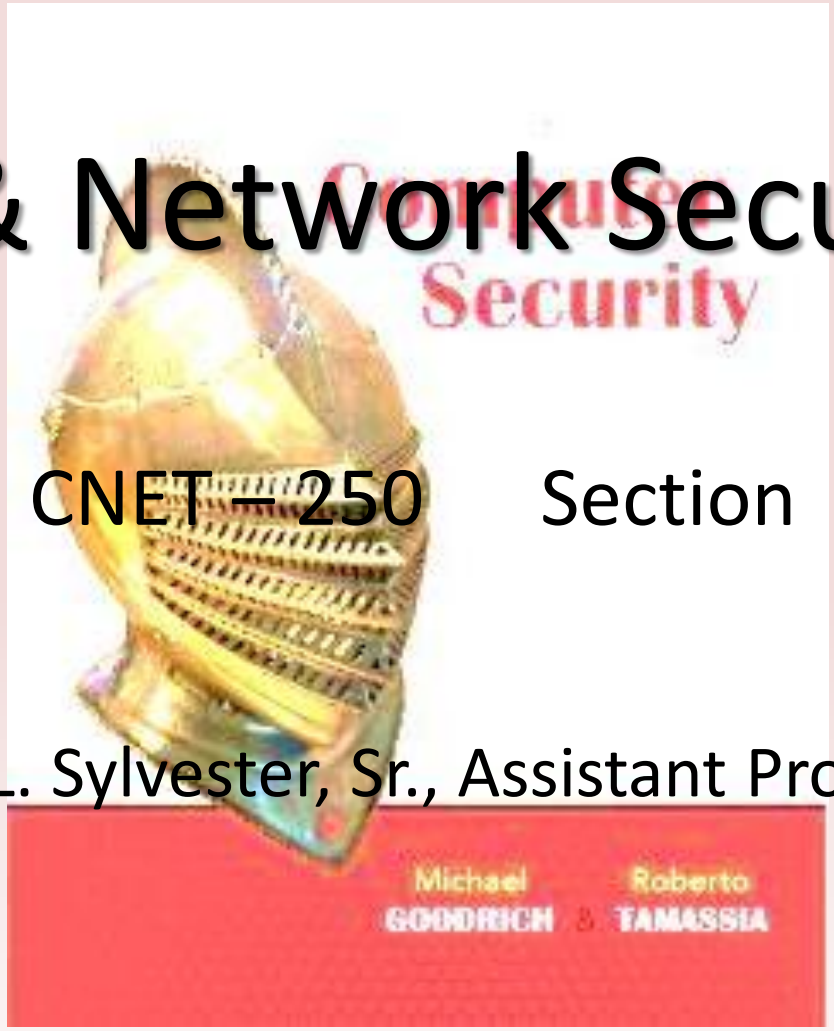
PC & Network Security

CNET – 250 Section



David L. Sylvester, Sr., Assistant Professor

Chapter 2

Physical Security

Physical Protection and Attacks

When thinking of computer security, we often think strictly in the digital context, where computers are accessed only over a network or through a well-specified digital interface and are never accessed in person or with physical tools, like a hammer, screwdriver, or container of liquid nitrogen.

Ultimately, digital information must reside somewhere physically, such as:

- In the state of electrons,
- Magnetic media, or
- Optical devices.

Accessing the information requires the use of an interface between the physical and digital worlds.

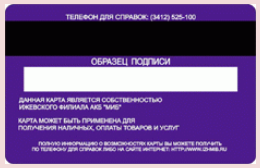
The protection of digital information must include methods of physically protecting this interface.

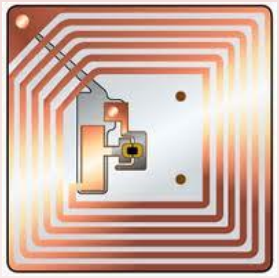
This is done through physical security, which is defined as the use of physical measures to protect valuables, information, or access to restricted resources.

- **Location protection:** the protection of the physical location where computer hardware resides, such as through the use of locks.
- **Physical intrusion detection:** the detection of unauthorized access to the physical location where computer hardware resides.
- **Hardware attacks:** methods that physically attack the hardware presentations of information or computations, such as hard drives, network adapters, memory chips, and microprocessors.
- **Eavesdropping:** attacks that monitor light, sound, radio, or other signals to detect communications or computations.
- **Physical interface attacks:** attacks that penetrate a system's security by exploiting a weakness in its physical interface.

Electronic combination locks is used to operate the lock using electromagnets or motors that are activated through an event that either turns on or turns off an electric current. An electronic lock can be open in the following ways:

- An **electronic combination:** the punching of an appropriate sequence of numbers on a keypad in a given amount of time.
- A **magnetic stripe card:** a plastic card with a magnetic stripe that contains an authorizing digital combination.
- A **smart card:** a small computational device contained in a card that performs an authorizing computation to open the lock.
- A **RFID tab:** a small radio frequency identification device that contains a computational element or memory that either performs an authorizing computation or transmits an electronic combination.
- A **biometric:** a biological characteristic that is read and matches a characteristic authorized to open the lock.



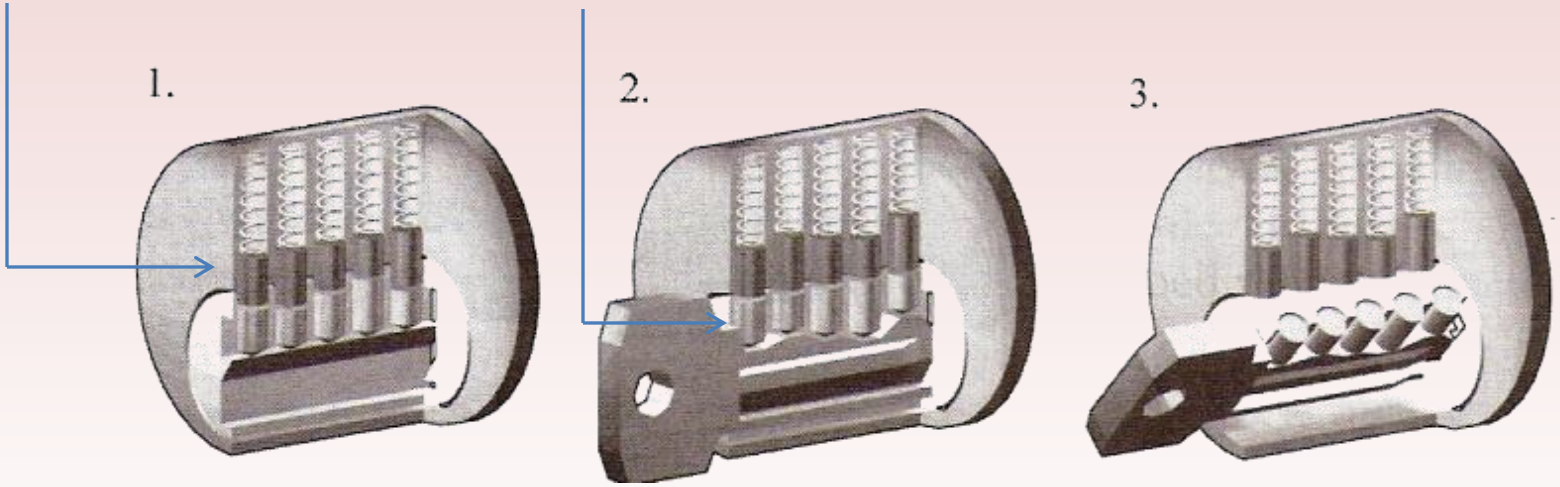


Locks and Safes

Pin Tumbler Locks

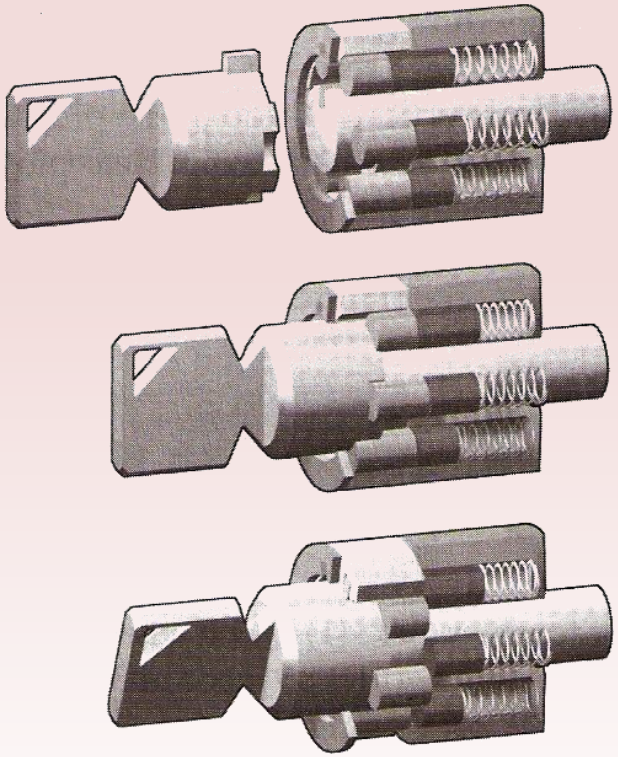
These are the more commonly used locks. In this design, a cylindrical plug is housed within an outer casting. The lock is opened when the plug rotates and releases a locking bolt, typically through a lever. When the lock is closed, the rotation of the plug is prevented by a series of pin stacks, which are housed in holes that have been drilled vertically through the plug and the outer casting.

Driver pins, key pins, shear line



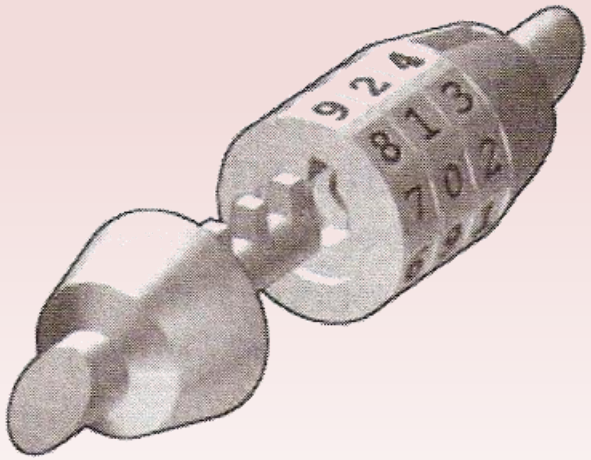
Tubular and Radial Locks

Rather than having pins located on a line parallel to the axis of the plug, as in the traditional pin tumbler lock, the pins of a tubular lock are arranged in a circle. As a result, keys are cylindrical in shape. These locks are most commonly used on laptops, vending machines, and bicycles.



Combination Locks

Combination locks typically come in one of three varieties, multiple dial, single dial, and electronic. Multiple-dial locks feature a sequence of notched disks around a toothed pin. When the disks are rotated to the correct combination, the notches line up with the teeth of the pin, allowing it to be removed. Multiple-dial combination locks are often used in briefcases, bicycle locks, and other low-security applications.



Safes

Valuables can be secured against theft by placing them in a safe. Safes can range from small lockboxes in homes to large, high-security safes in banks. Safes can feature any of the locking mechanisms discussed. Most high-security models employ a combination dial, with the possible addition of biometric authentication.

Attacks on Locks and Safes

Lockpicking

Lockpicking allow an attacker to replicate the effect of an authorized entry. The lock picker attempts to open a pad lock with a tension wrench by picking the pins individually.

Lock Bumping

Lock bumping became widespread through the media in 2006. To bump a lock, the bump key is inserted into the keyhole, then withdrawn a small amount so that each tooth rests immediately behind a pin. While applying a slight rotational force, the bump key is then reinserted by tapping it with a hammer or other object.

Key Duplication and Impressions

Duplication. A locksmith can easily create a key duplicate if the original is available. They can even make a duplicate from a photograph.

Impressioning. This is another bypass technique used. An attacker begins with a key blank matched to a specific lock brand. The top of the blank is polished, and then the key is inserted into the target lock.

High Security Locks

There are a number of innovations developed to make bypassing difficult.

1. incorporating the use of security pin
   - Spool pins
   - Serrated pin
   - Mushroom head pins

Security pins may defend ordinary picking, but do little to stop techniques such as bumping.

Authentication Technologies

Barcodes

Printed labels called barcodes were developed around the middle of the 20th century as a way to improve efficiency in grocery checkout.

one dimension bar code

two dimension bar code

Magnetic Stripe Cards

Developed in the late 1960's, the magnetic stripe card is one of the most pervasive means of electronic access control. Magnetic stripe cards are key components of many financial transactions, such as debit or credit card exchanges, and are the standard format for most forms of personal identification, including driver's licenses.

Magnetic Stripe Card Security

The stripe on the back of a credit card is a magnetic stripe, often called a magstripe. The magstripe is made up of tiny iron-based magnetic particles in a plastic-like film. Each particle is really a tiny bar magnet about 20-millionths of an inch long.

There are three tracks on the magstripe. Each track is about one-tenth of an inch wide.

The **first track** of a magnetic stripe card contains the cardholder's full name in addition to an account number, format information, and other data at the discretion of the issuer. The first track is often used by airlines when securing reservations with a credit card.

The **second track** is encoded using a 5-bit scheme (4bits of data and 1 parity bit per character), with a total of 40 characters. This tract may contain the account number, expiration date, information about the issuing bank, data specifying the exact format of the tract, and other discretionary data. It is most often used for financial transactions.

The **third track** is much less commonly used.

One vulnerability of the magnetic stripe medium is that it is easy to read and reproduce. Magnetic stripe readers can be purchases at relatively low cost, allowing attackers to read information of cards.

One effective deterrent against card fraud is a requirement for additional information know only to the owner, such as a personal identification number (PIN).

Smart Card

Smart cards incorporate an integrated circuit, optionally with an on-board microprocessor. The microprocessor features reading and writing capabilities, allowing the data on the card to be both accessed and altered. Smart card technology can provide secure authentication mechanisms that protect the information of the owner and are extremely difficult to duplicate.

Smartcards are commonly used in large companies and organizations as a means of strong authentication, often as part of a single sign-on scheme.

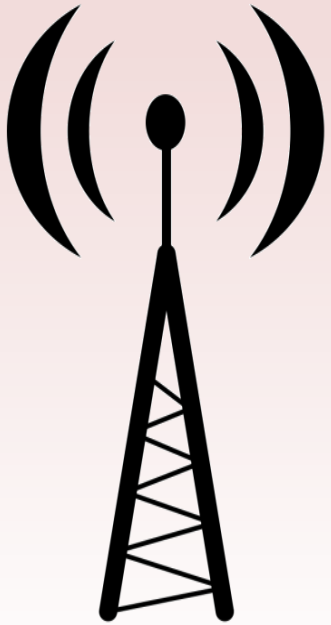
GSM Challenge-Response Protocol

When a cellphone wishes to join a cellular network to make and receive calls, the cellphone connects to a local base station owned by the network provider and transmits its IMSI to declare its identity. If the IMSI corresponds to a subscriber's record in the network provider's database, the base station transmits a 128-bit random number to the cellphone. This random number is then encoded by the cellphone with the subscriber's secret key stored in the SIM card using a proprietary encryption algorithm, resulting in a ciphertext block that is sent back to the base station.

Checks IMSI against network provider's DB →

← If IMSI matches, R = a 128 bit random number

→ $E_K(R)$ = the 128 bit random number encrypted using the subscriber's secret key K.



SIM (Subscriber Identity Module) Cards

Many mobile phones use a special smart card called a SIM card. The SIM card is issued by a network provider. It maintains personal and contact information for a user and allows the user to authenticate to the cellular network of the provider. Many phones allow the user to insert their own SIM card, making the process of switching phones simple and instantaneous.

SIM Card Security

A SIM card features an integrated circuit card ID (ICCID), which is a unique 18-digit number used for hardware identification. The SIM also contains a unique international mobile subscriber identity (IMSI), which identifies the owner's country, network, and personal identity. The card also contains a 128-bit secret key that is used for authenticating a phone to a mobile network.

RFIDs

The use of radio frequency identification, or RFID, is a rapidly emerging technology that relies on small transponders to transmit identification information via radio waves. RFID chips feature an integrated circuit for storing information, and a coiled antenna to transmit and receive a radio signal.

RFID Usage

- Vendors for consumer-product tracking (replacing barcodes)
  - Track best selling item
  - Tags for theft detection
  - Track animals in the wild
- Hopping Codes and Remote Automobile Entry
  - Lock/Unlock vehicle
  - Start vehicle

To prevent attackers from eavesdropping the controller chip in a key fob and the receiver in the vehicle uses what is known as a hopping code or rolling code. The controller uses the same pseudo-random number generator, so that each device produces the same sequence of unpredictable numbers.

Digital Signature Transponder

Several automobile key fobs and tags for automatic payment systems at gas stations use an RFID device called Digital Signature Transponder (DST), which is manufactured by Texas Instruments. A DST stores a 40-bit secret key and incorporates a proprietary encryption algorithm call DST40. The main use of DST is to execute a simple challenge-response protocol, where the reader asks the DST to encrypt a randomly generated challenge to demonstrate possession of the secret key. (*Similar to the GSM phone*)

Electronic Toll Systems

These systems allow motor vehicle owners to place an RFID tag near their dashboards and automatically pay tolls at designated collection sites. These systems provide great convenience, since they remove the hassle of dealing with cash and allow drivers to be tolled without coming to a stop.

Disadvantages

- Easily cloned
- Once cloned, it could be paced on another car in an attempt for a digital alibi (*a defense mechanism is photo camera: photo license plate*)

Passports

Passports contain an embedded RFID chip that contains information about the owner, including a digital facial photograph. In order to protect the sensitive information on the passport, all RFID communications are encrypted with a secret key. In may instances, however, this secret key is merely the passport number, the holder's date of birth, and the expiration date, in that order. All of this information is printed on the card , either in text or using a barcode or some other optical storage method.

Passport Vulnerabilities

- Person issuing passport may reconstruct the key
- Security key does not change
- May leak radio waves if slightly opened or if owner keeps documents of money inside of passport.

Biometrics

The term biometric in security refers to any measure used to uniquely identify a person based on biological or physiological traits. Biometric systems incorporate some sort of sensor or scanner to read in biometric information and then compare this information to stored templates of accepted users before granting access.

There are several requirements that must be met for a characteristic to be considered usable as biometric identification:

- **Universality** – Almost every person should have this characteristic. (preferably fingerprints not birthmarks)
- **Distinctiveness** – Each person should have noticeable differences in the characteristics. (retinal image, DNA, fingerprint)
- **Permanence** – The characteristics should not change significantly over time. (retinal image, DNA, fingerprint)
- **Collectability** – The characteristic should have the ability to be effectively determined and quantified.

Biometric Characteristics *(Person's Signature, Fingerprints, Voice Recognition, Eyes, Facial Recognition)*

Privacy Concerns for Biometrics Data

The storage of biometric data for authentication purposes poses a number of security and privacy concerns. Access to stored biometric data may allow an attacker to circumvent a biometric system or recover private information about an individual. Since biometric data does not change over time, once a person's biometric data is compromised, it is compromised forever. As such, encryption should be used to protect the confidentiality of biometric data, both in storage and transmission. However, this security requirement poses a unique problem, because biometric samples provided to a system by a user is not expected to match the stored template exactly. Therefore, the comparison of scanned or read data should be compared to the stored reference allowing for slight differences.

One approach proposed that support efficient biometric authentication, while preserving the privacy or the original biometric template of the user is that of approximate message authentication code (AMAC). This approach has the following properties:

- Given the AMACs of two messages, it is possible to determine efficiently whether the distance between the original messages is below a certain pre-established threshold.
- Given the AMAC of a message, it is computationally hard to find any message within distance from it.

Direct Attacks Against Computers

Acquiring physical access to a computer system opens up many avenues for compromising that machine. Several of these techniques are difficult to prevent, since hardware manufacturers generally assume that the user is a trusted party.

Environmental Attacks and Accidents

Computing equipment operates in a natural environment and if this environment is significantly altered, then the functionality of this computing equipment can be altered.

Three main components:

- **Electricity**: needed to uninterrupted power to operate
- **Temperature**: if overheated, computer chips can severely damaged
- **Limited Conductance**: given the fact that computing equipment is electronic, conductance should be limited

Eavesdropping

Wiretapping. Given physical access to the cables of a network or computer, it may be possible for an attacker to eavesdrop on all communications through those cables. Many communication networks employ the use of inexpensive coaxial copper cables, where information is transmitted via electrical impulses that travel through the cable. There are inexpensive way in which to capture these impulses and reconstruct the data being transferred through a tapped cable. This allows an attacker to eavesdrop on network traffic. These wiretapping attacks are passive, in that there is no alteration of the signal being transferred, making them very difficult to detect.

Defense Against Wiretapping.

- **Twisted pair**: copper that is entwined to eliminate electromagnetic interference.
- **Fiber Optic**: these cables transmit light rather than electricity, which prevents the signal leakage that occurs in coaxial cable

Hardware Keyloggers. A keylogger is any means of recording a victim's keystrokes, typically used to eavesdrop password or other sensitive information. Hardware keyloggers are typically small connections that are installed between a keyboard and a computer.

Tempest

Tempest is a U. S. government code word for a set of standards for limiting information-carrying electromagnetic emanations from computing equipment. In term of standards, TEMPEST establishes three zones or levels of protection:

1. An attacker has almost direct contact with the equipment, such as in the adjustment room or within a meter of the device in the same room.

2. An attacker can get no closer than 20 meters to the equipment or is blocked by a building to have an equivalent amount of attenuation (reduction of signal).

3. An attacker can get no closer than 100 meters to the equipment or is blocked by a building to have an equivalent amount of attenuation.

Emanation Blockage

This approach involves limiting the release of information from escaping into its general environment. Some examples of this type of emanation limitation include the following:

1. To block visible light emanation, (enclose sensitive equipment in windowless room)
2. To block acoustic emanation, (enclose sensitive equipment in room lined with sound-dampening material)
3. To block electromagnetic emanations in the electrical cords and cables, (have every cord and cable grounded, to dissipate any electric currents traveling in them)
4. To block electromagnetic emanations in the air, (surround sensitive equipment with metallic conductive shielding or a mesh of such material) *The holes in the mesh are smaller than the wavelengths of the electromagnetic radiation we wish to block.*

In order for these emanation blockage techniques to work, the sensitive computing equipment (including all its cables and junction boxes) have to be completely enclosed. Example of such enclosures range from a classified office building, which is completely enclosed in copper mesh and has two-pass copper doors for entering and exiting; metal-lined passport wallet, which encloses an RFID passport in a small Faraday cage so as to block unwanted reading of the RFID tag inside it.

Live CDs

A live CD is an operating system that can be booted from external media and resides in memory, without the need for installation. It can be stored on a CD, DVD, USB drive or any other removable drive from which the computer can boot. There are many legitimate uses for live CDs, including diagnostics and software repair purposes. Unfortunately, an attacker can boot from a live CD, mount the hard disk, and then read or write data, bypassing any operating system authentication mechanism. (*A native operating system can do nothing to prevent this, because it is never loaded. Therefore, preventative measures must be build into hardware.*)

- Protective Measures
  - BIOS (Basic Input/Output System) password

    The BOIS is firmware code that is executed immediately when a machine is turned on and before loading the operating system. By protecting the BIOS, an attacker is unable to boot the computer without a password. But, the actual information is still vulnerable if the attacker can remove the hard drive from that system and mounting it in another computer.

Computer Forensics

Computer forensic is the practice of obtaining information contained on an electronic medium, such as computer systems, hard drives, and optical disks, usually for gathering evidence to be used in legal proceedings.

Unfortunately, many of the advanced techniques used by forensic investigators for legal proceedings can also be employed by attackers to uncover sensitive information.

An important principle of computer forensics is to establish, maintain and document a chain of custody for the computer hardware being analyzed so that it can be shown that items collected remains unaltered throughout the forensic analysis process.

Security Concerns from Computer Forensics

Often, forensic analysis of a system, while it is turned on, can reveal information that would not be obtainable if it were powered off. For example, online analysis allows an investigator, even an attacker, the ability to use tools to examine or copy the contents of RAM, which is volatile and disappears when the computer is turned off. By examining RAM, an attacker could uncover recently entered passwords or other sensitive information that would be unavailable if the machine were off. Also, online attacks can often reveal information about a machine's presence on the network.

The process of backups (making copies of information), of entire hard drives or any other storage media is perform prior to analyzing its contents.

Forensic techniques also involves recovering data that a user has deleted. File operations on a computer, including reading, writing, and deleting files, are controlled by a portion of the operation system known as the filesystem. Many file systems only remove the file's metadata, information about the file, without actually overwriting the contents of the data on the disk.

Cold Boot Attacks

In 2008, a team of Princeton researchers presented a technique that can be used to access the contents of memory after a computer has been shut down. Dynamic random- access memory (DRAM) is the most common type of computer memory. DRAM modules are volatile storage, which means that their contents decay quickly after a computer is turned off. But, the study showed that by cooling DRAM modules to very low temperatures, the rate of decay can be slowed to the point where the contents of memory can be reconstructed several minutes after the machine has powered off.

In using this technique, the researchers were able to bypass several popular drive encryptions. Their cold boot attack consisted of freezing the DRAM modules of a running computer by using a canned refrigerant, powering off the computer, and booting it from a live CD equipped with a program that reconstructed the memory image and extracting the disk encryption key (which was stored in unencrypted form in memory).

Special Purpose Machines

Special purpose machines or computers are computers that are specialized to perform a particular job.

Two examples are:

- ATM (Automatic Teller Machine)
- Voting Machine

ATMs

These devices allow customers of financial institutions to complete withdrawal and deposit transactions without human assistance, using a magnetic stripe credit or debit card and entering a PIN. The ATM has an internal cryptographic processor that encrypts the entered PIN and compares it to an encrypted PIN stored on the card (older systems with no network connection) or a remote database. The PIN mechanism prevents an attacker with access to a stolen card from accessing account funds.

A technique know as ram-raiding is used by attackers whereby they use heavy construction equipment or large vehicles to uproot and remove entire ATMs. This can be prevented by installing vehicular obstructions such as bollards.

ATM Encryption

To ensure the confidentiality of customer transactions, each ATM has a cryptographic processor that encrypts all incoming and outgoing information, starting with the moment a customer enters their PIN. Triple DES (3DES) is the current standard cryptosystem for ATMs. 3DES is legacy symmetric cryptosystem with up to 112 bits of security.

Voting Machines

There are two types of electronic voting, paper-based and direct-recording. In a paper-based system, voters submit their votes on a piece of paper or a punchcard, after which it is counted either by hand or by an optical scanner designed to read and tally marked ballots.

Paper-based systems have several advantages, including the fact that most people are familiar with how they work and they allow for hand recounts.

The other type of voting machine, which is used by many countries, is the direct-recording system, where votes are submitted and tallied electronically, using touch-screen technology. These systems are faster, more environmentally friendly, more accessible to handicapped voters, and more accurate. But, these electronic voting systems are not as amenable to hand recounts (provides no paper audit trail).