Direct Attacks on Computational Devices

Environmental Attacks

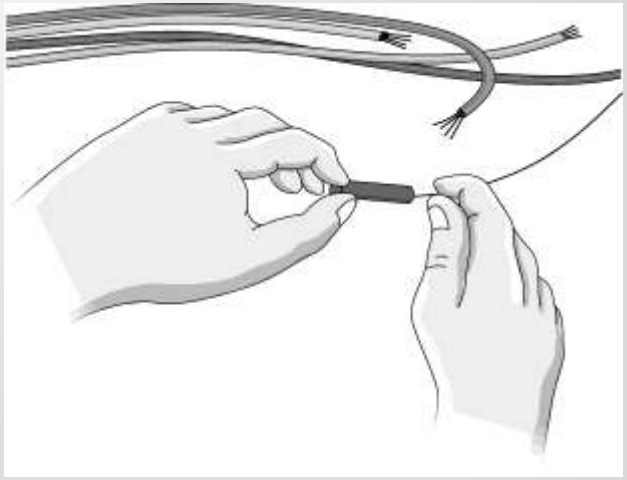
- **Electricity.** Computing equipment requires electricity to function; hence, it is vital that such equipment has a steady uninterrupted power supply.
- **Temperature.** Computer chips have a natural operating temperature and exceeding that temperature significantly can severely damage them.
- **Limited conductance.** Because computing equipment is electronic, it relies on there being limited conductance in its environment. If random parts of a computer are connected electronically, then that equipment could be damaged by a short circuit (e.g., in a flood).

Eavesdropping

- **Eavesdropping** is the process of secretly listening in on another person's conversation.
- Protection of sensitive information must go beyond computer security and extend to the **environment** in which this information is entered and read.
- Simple eavesdropping techniques include
  - Using social engineering to allow the attacker to read information over the victim's shoulder
  - Installing small cameras to capture the information as it is being read
  - Using binoculars to view a victim's monitor through an open window.
- These direct observation techniques are commonly referred to as **shoulder surfing.**

Wiretapping

- Many communication networks employ the use of inexpensive coaxial copper cables, where information is transmitted via electrical impulses that travel through the cables.
- Relatively inexpensive means exist that measure these impulses and can reconstruct the data being transferred through a tapped cable, allowing 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 extremely difficult to detect.

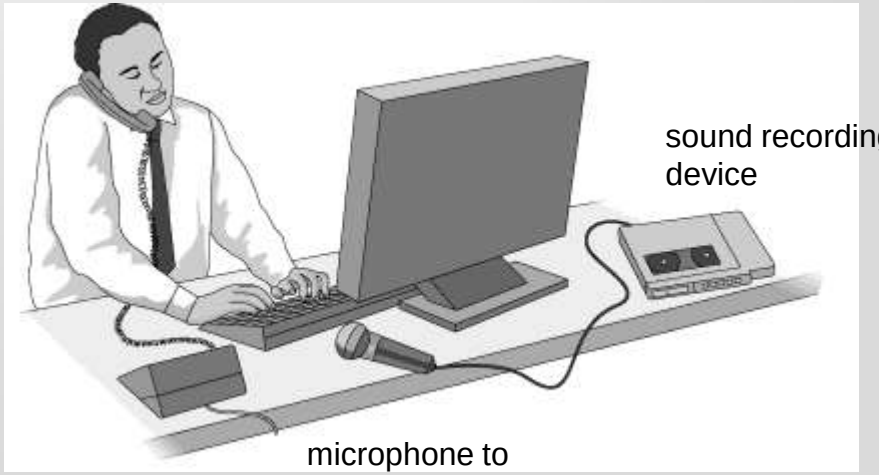


Signal Emanations

- Computer screens emit **radio frequencies** that can be used to detect what is being displayed.
- **Visible light** reflections can also be used to reconstruct a display from its reflection on a wall, coffee mug, or eyeglasses.
- Both of these require the attacker to have a receiver close enough to detect the signal.

Acoustic Emissions

- Dmitri Asonov and Rakesh Agrawal published a paper in 2004 detailing how an attacker could use an audio recording of a user typing on a keyboard to reconstruct what was typed.
  - Each keystroke has minute differences in the sound it produces, and certain keys are known to be pressed more often than others.
  - After training an advanced neural network to recognize individual keys, their software recognized an average 79% of all keystrokes.



Hardware Keyloggers

- A keylogger is any means of recording a victim's keystrokes, typically used to eavesdrop passwords or other sensitive information.
- Hardware keyloggers are typically small connectors that are installed between a keyboard and a computer.
- For example, a USB keylogger is a device containing male and female USB connectors, which allow it to be placed between a USB port on a computer and a USB cable coming from a keyboard.

TEMPEST

- **TEMPEST** is a U.S. government code word for a set of standards for limiting information-carrying electromagnetic emanations from computing equipment.
- TEMPEST establishes three zones or levels of protection:
  1. An attacker has almost direct contact with the equipment, such as in an adjacent 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.
  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

- To block visible light emanations, we can enclose sensitive equipment in a windowless room.
- To block acoustic emanations, we can enclose sensitive equipment in a room lined with sound-dampening materials.
- To block electromagnetic emanations in the electrical cords and cables, we can make sure every such cord and cable is well grounded and insulated.

Faraday Cages

- To block electromagnetic emanations in the air, we can surround sensitive equipment with metallic conductive shielding or a mesh of such material, where the holes in the mesh are smaller than the wavelengths of the electromagnetic radiation we wish to block.
- Such an enclosure is known as a **Faraday cage.**

Computer Forensics

- **Computer forensics** 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.

Computer Forensics

- Forensic analysis typically involves the physical inspection of the components of a computer, sometimes at the microscopic level, but it can also involve electronic inspection of a computer's parts as well.

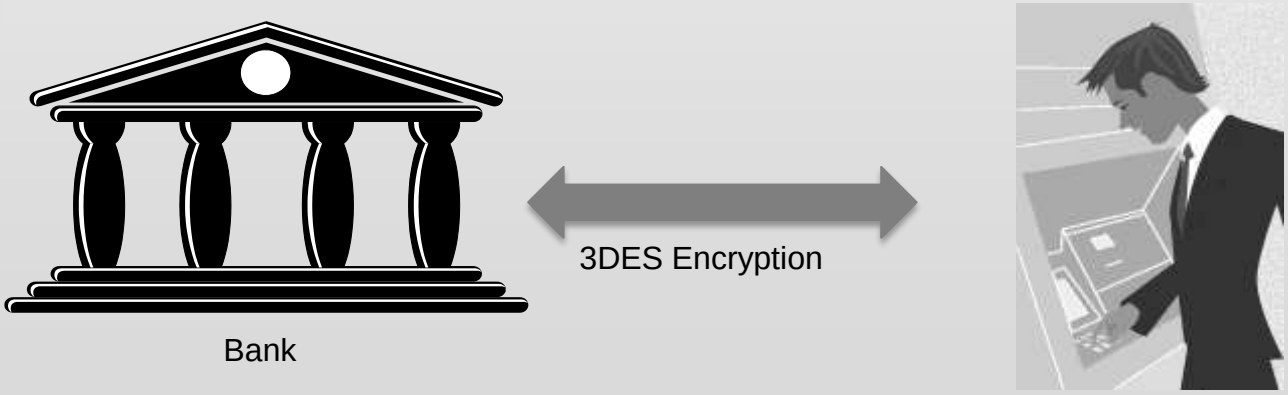
ATMs

- An **automatic teller machine (ATM)** is any device that allows customers of financial institutions to complete withdrawal and deposit transactions without human assistance.
- Typically, customers insert a magnetic stripe credit or debit card, enter a PIN, and then deposit or withdraw cash from their account.
- The ATM has an internal cryptographic processor that encrypts the entered PIN and compares it to an encrypted PIN stored on the card (only for older systems that are not connected to a network) or in a remote database.

ATM

ATMs

- To ensure the confidentiality of customer transactions, each ATM has a cryptographic processor that encrypts all incoming and outgoing information, starting the moment a customer enters their PIN.
- The current industry standard for ATM transactions is the **Triple DES (3DES) cryptosystem,** a legacy symmetric cryptosystem with up to 112 bits of security.
- The 3DES secret keys installed on an ATM are either loaded on-site by technicians or downloaded remotely from the ATM vendor.



Attacks on ATMs

- **Lebanese loop:** A perpetrator inserts this sleeve into the card slot of an ATM. When a customer attempts to make a transaction and inserts their credit card, it sits in the sleeve, out of sight from the customer, who thinks that the machine has malfunctioned. After the customer leaves, the perpetrator can then remove the sleeve with the victim's card.
- **Skimmer:** a device that reads and stores magnetic stripe information when a card is swiped. An attacker can install a skimmer over the card slot of an ATM and store customers' credit information without their knowledge. Later, this information can be retrieved and used to make duplicates of the original cards.
- **Fake ATMs:** capture both credit/debit cards and PINs at the same time.