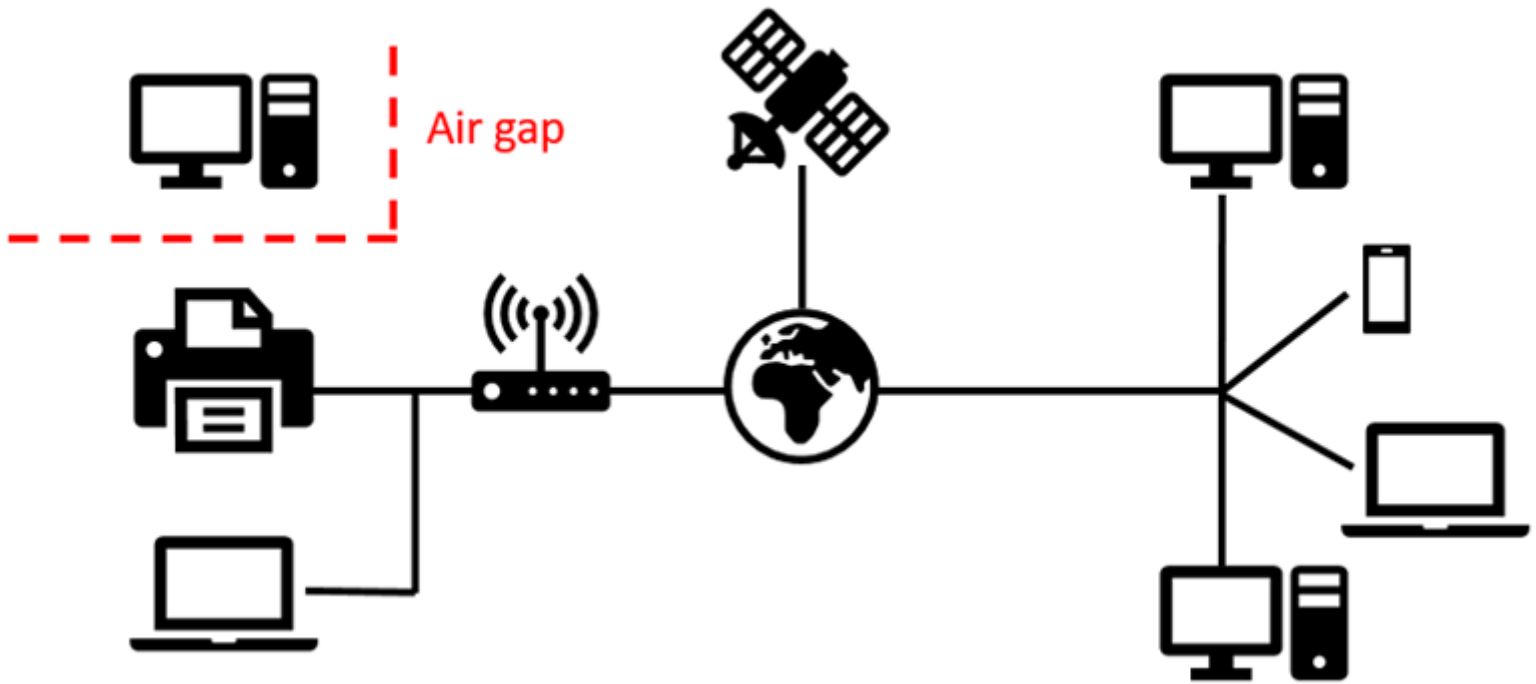
Hacking the Air Gap: Stealing Data from a Computer that isn't Connected to the Internet

An air-gapped computer is physically separated with no hardwired or wireless connection to the rest of the internet. It may still be part of an air-gapped network, and connected to other computers on a private network, but not the rest of the internet.



- Computers send information using binary code, a series of ones and zeroes (also called on/off, high/low, or true/false).
- Normally, whenever you download a song, view a website, or send an email, these ones and zeroes are sent as electronic signals through a wire like an ethernet cable, or as electromagnetic waves through a connection like Wi-Fi or Bluetooth.
- An air-gapped computer physically lacks the means to send signals over a wired or wireless connection.
- However, even without an internet connection, computers still transmit signals into the world around them. They make noise, they blink lights, they vibrate, and they get hot. Light, sound, vibration, and heat are all physical quantities that we can use to send information.

Types of Air-Gap

- **The total physical air gap**—This the salt mine type, which involves locking digital assets in a completely isolated physical environment, separated from any network-connected systems. A digital asset in a total physical air gap has no network connections. If anyone wants to get data from it or put data onto it, they must physically go to it, a process that usually involves going through physical security barriers.

- **Segregated in the same environment**—An air gap can be achieved by simply disconnecting a device from a network. One could have two servers on the same rack, for instance, but still air-gapped away from each other because one is not plugged into the network.

- **Logical air gap**—A logical air gap refers to the segregation and protection of a network-connected digital asset by means of logical processes. For example, through encryption and hashing, coupled with role-based access controls, it is possible to achieve the same security outcomes that are available through a physical air gap. Even if someone can access the digital asset, the asset cannot be understood, stolen, or modified.

Some popular sensors used for observing variations on air- gaped systems

- **Smartphone with a sensor app such as phyphox**
- **If you do not use a phone, you can also purchase a variety of sensors**
- **Infrared thermometer. Used to measure the temperature of a surface.**
  - **Decibel meter- Used to measure sound levels.**
  - **Lux meter- Used to measure light levels (not sensitive enough to detect individual LEDs, but can detect changes in screen brightness).**
  - **Electricity usage monitor.-Used to measure electrical power consumption.**
  - **Webcam or video camera- Used to observe blinking LEDs.**

Procedure

- Choose a physical quantity that you want to use to send a signal from your computer
- Find out how you will control that physical quantity on your computer. How you do this will depend on your computer and operating system. The controls could be built in to your computer's hardware (like buttons on the monitor to control the brightness) or operating system (like an icon in the taskbar to control the volume). Some quantities might require third-party software (like a program to control fan speed) or websites (like a site to play audio tones at different frequencies).

- Find out if you can send a binary signal from the computer to your sensor by changing the physical quantity you have selected. For example, if you change a computer's fan speed between 50% and 100% (do not set the fan speed to 0%, your computer will overheat!), can you detect the change while recording data with the microphone in your sensor app (audio amplitude function in phyphox)? If so, then you can send binary data, for example "1001" by setting the fan speed to either 100% (for 1) or 50% (for 0) in 1-second intervals?
- Determine the range of your signal. How far away can the sensor be? Does it require direct line-of-sight to the computer. Can it be in a different room? For example, if you are using a camera to watch an LED blink on the computer, how far away can the camera be before you can no longer see the LED.

- Examine how vulnerable your signal is to noise and interference. For example, if you are using an accelerometer to detect keyboard vibrations, what happens when people walk around the room or slam a desk drawer. If you are using a microphone to measure sound, what happens when people in the room talk.
- Figure out the bit rate of your signal, or how fast it can transmit data. How many 1's and 0's can you send per second, per minute, or per hour.For example, if you are running a CPU stress test to heat your computer up, how long does it take to notice a measurable increase in temperature of the computer's case with an infrared thermometer. How long does it take for the computer to cool back down.

- Investigate whether your signal would be detectable by a person using the computer or in the room. For example, fluctuating the monitor brightness between 0 and 100 might be very obvious to someone sitting right in front of it, but they might not notice if you change the brightness from 80 to 85. Can you send a signal that is below the threshold of human perception, but still detectable by the electronic sensor you are using.

Vulnerability

I. **Side Channel Attacks –Capture unintended leakage of information during operation .Can be exploited to extract key with relatively low effort.**
II. **FM and cellular radio waves to thermal and NFC signals that can carry up to 100 metre**
III. **EM emissions**
IV. **Power Consumption analysis (Ex- SPA,DPA)**
V. **Data Coupling**
VI. **Timing analysis**
VII. Hardware Trojans

Recommendation

- Installing Firewall
- Maintaining your system up to date
- Use Stronger authentication
- secure that machine either offsite or in a safeguarded room
- make sure all cables to the machine are properly shielded (don’t cut corners on cables here)
- plug unused USB slots with the USB Port Blocker
- turn the machine off when it is not in use (and unplug it from power);
- replace standard drives with SSD
- encrypt your data.

References:

- Air-gapped computers are no longer secure (TechRepublic)
- Interview with a hacker: Gh0s7, leader of Shad0wS3c (TechRepublic)
- Interview with a hacker: S1ege from Ghost Squad Hackers (TechRepublic)
- The 18 most frightening data breaches (TechRepublic)
- Experts predict 2017's biggest cybersecurity threats (TechRepublic)
- Security awareness and training policy (Tech Pro Research)