Air Gap Systems: a way to secure our data

Introduction

Since the begging of network creation, having high security and protecting the data from being stolen, was a big challenge for us and computer users.

It took computer and network engineers a long time to find some ways to take the network security to its high levels. Despite the fact that there are thousands of solutions and ways to protect our network from attackers and create a safe, high protected, isolated network system; we see that network security is not at its best.

“*Ransomware is expected to attack a business every 11 seconds by the end of 2021*!”

Says a report by “Cybersecurity Ventures”

The cost of damages due to system security breaches is projected to cost over $6 trillion by 2021. The sad truth is, when sophisticated attackers want to get access to your data, they leave no stone unturned to find a way.

Although money is also important but let’s discus about this a little bit deeper. What happens if attackers find a way to access the data of a country’s military database?

Do these results leads us to not using networks?

So basically we are not able to protect our valuable data in anyways?

The answer is no, due to technology’s high development there is a way that we can actually reduce the chances of being attacked by hackers.

Because of these threats, **many organizations are now choosing to have air-gapped computers or networks.**

What is Air-gap systems?

Air-gap refers to computers or networks that are not connected directly to the internet or to any other computers that are connected to the internet.

A true air gapped computer is also physically isolated, **meaning data can only be passed to it physically** (via USB, removable media or a firewire with another machine).

So basically the only way to access this system is physically. You have to manually go to the system and get the information yourself.

Air-gap creates a buffer in network systems connections, so in case of being hacked, the hacker doesn’t have the access to all of our systems. **Keeping away our important data from the rest of network is what it does.**

Very simple. But how does this makes our network secure? Let’s reveal some usages of this technology.

What are Air-gap usages?

Here’s a good example from pop culture. Do you remember the scene from the movie *“Mission Impossible”* where *“Tom Cruise”* rappels down from the ceiling?

It’s one of the most famous scenes in movie history. In it, Cruise lowers himself from an air vent and dangles just feet above the floor as he steals a list from a computer in FBI headquarters.

That is an **air gapped computer**.

As you saw in that movie, the computer was not directly connect to network system. This made it almost impossible for attacker to get the data out of it.

Air gaps generally are implemented where the system or network requires extra **security**, such as **classified military networks**, **the payment networks** that process credit and debit card transactions for retailers, or **industrial control systems** that operate critical infrastructure.

Also in:

* Life-critical systems such as Medical Equipment
* Nuclear power plants
* Aviation Computers
* Government computer systems and networks

Flaws of air gap systems!

With all of the good things we said about air-gap system, still it is not totally secure. As we said it before, using air-gap systems decreases the chances of being attack by hackers, but it will not make it to zero. Still there are some ways to hack this system, but they cannot be done by any hackers.

Seriously though, while you definitely don’t need to freak out and go find an alternative to air gapping, it would be silly to pretend that nothing can go wrong. Air gapped computers can still be breached. Granted, it’s a hell of a lot harder to do when a computer is air gapped, but methods exist.

Cause this system needs a trustable people for managing it, there is a chance of being attach by the good old fashioned **social engineering**. That’s right, the easiest way to breach an air gapped computer is to find a human intermediary to wittingly (or possibly unwittingly) breach the computer. To do this they will need to access the computer themselves and attach a USB device like a flash drive or a Wi-Fi dongle.

But that’s not the only way to do this. If you want to get a bit more scientific, there are other way channels to extract data from an air gapped computer, they include:

* Electromagnetic (EM)
* Acoustic
* Thermal
* Optical

“Stuxnet”: the most famous infection of air gap systems

One of the most famous cases involving the infection of an air-gapped system is “*Stuxnet”*, the virus/worm designed to sabotage centrifuges used at a *uranium enrichment plant in Iran*.

Computer systems controlling the centrifuges were air-gapped, so the attackers designed “*Stuxnet”* to spread surreptitiously via USB flash drives. Outside contractors responsible for programming the systems in Iran were infected first and then became unwitting carriers for the malware when they brought their laptops into the plant and transferred data to the air-gapped systems with a flash drive.