Air Gap Systems: A way to secure our data

Introduction

Since the begging of network creation, providing a secure area and preventing unauthorized access to our data has always been a big challenge for us.

It took a long time for computer and network engineers to find the ways to promote the network’s security to its highest levels. Despite the fact that there are many policies and practices which keep safe our network from the attackers and create a secure, highly protected, isolated network system; we see that it is not as its best form.

According to the statistics, although network administers pay fully attention to the security of their networks and continue using the newest ways, there are cyber-attacks at a high rate.

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

A report by “Cybersecurity Ventures”

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

In addition to losing the money, let’s think about it a little bit deeper. What would happens if the attackers have access to a country’s military database? or to the datebase of country’s nuclear organization? So is there any way to promote the network security to its best?   
The answer is No, but because of technology’s high development there is a way that we can actually reduce the chances of cyber-attacks.

Due to many threats by cyber-attack, **many organizations are now choosing to have air-gapped computers or networks.**

What is a Air-gap and what are the Air-gap systems?

Air-gapping is a way for creating a “roadblock” that is made by a blank space. It’s a technology used by network admins to protect network/computer systems from the malicious programming code that hackers send.   
Air gapping technology is based on the theory that without a WIFI connection or cable, malware or viruses cannot travel further than the network’s physical boundary. Hence, if you disconnect the network or computer from the internet, an air gap is created.

Air-gap systems refers to computers or networks that aren’t connected directly or indirectly to the internet.

A true air gapped computer is physically isolated, **meaning that the data can be only passed through it physically** (via USB, removable media or a firewire with another machine).  
Air-gap creates a buffer in network systems connections, so in case of being hacked, the hacker doesn’t get the access to all of our systems. **Keeping away our important data from the rest of the network is what it does.**

Thus, the only way of getting access to this system is physically and nothing more, you should work manually with the computers and get the information by yourself. It’s so easy, but how does this makes our network secure?

How does it make a network secure?

By using Air-Gap Defense Technology.Essentially, an ‘Air Gap Defense Technology’ refers to the absence of a wireless connection into a network connections or computer systems. It means that a hacker cannot hijack your network, computer systems, smartphone, laptop, or the WI-FI router ‘wirelessly’. They will need to have access to wired connections where you can install security software that acts as a firewall.

When the connection between backup and live data is removed physically, you get to what is called as an air-gap in network architecture. An air gap similar to this assures that your backup data stays offline and hence inaccessible to any outside party -making it unreachable for attackers or hackers.

To clear this subject, let’s show some usages of this technology.

What are Air-gap usages?

Here’s a good example from pop culture. Do you remember the scene of the movie *“Mission Impossible”* where *“Tom Cruise”* rappels down from the ceiling? It’s one of the most famous scenes in this series movies. 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. The computer in that scene was an **air gapped computer**. As you saw, the computer was not directly connected 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 infrastructures.

Also in:

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

Considering the benefits of air-gapping, a lot of organizations are now deploying apps in air gapped environments. Such apps or systems are managed by being physically plugged into the internal network.   
Apps that are deployed in an air-gapped environment are invisible to the internet, and hence the attackers. Security operations teams create this type of network for incident responses.

But that’s not all, there are also other reasons why some businesses opt-out of having an external network connectivity, here some:

* Edge computing for organizations that wish to conserve bandwidth.
* Apps can be deployed in areas with poor internet connection or no connectivity as we explained.
* Sales people in the field can demo their latest n-tier applications without internet access.

Flaws of air gap systems!

With all of the good things we said about air-gap system, yet 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 for air gapping, it would be silly if you pretend that nothing can go wrong. Air gapped computers can be breached too.   
Granted that this is true it’s a hell of a lot harder to do when a computer is air gapped, but methods exist.

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

More recently, evidence has shown that air-gapped systems can also be attacked through radio waves; Researchers in Israel showed how they could [**siphon data from an air-gapped machine using radio frequency signals**](https://www.wired.com/2014/11/airhopper-hack/)and a nearby mobile phone.   
The proof-of-concept hack involves radio signals generated and transmitted by an infected machine's video card, which are used to send passwords and other data over the air to the FM radio receiver in a mobile phone.

This, and the use of attacks via USB flash drives, effectively mean that no air-gapped system is beyond the reach of attackers.

But they are not the only ways of hacking. If you look at it scientifically, there are other way channels to extract data from an air gapped computer, they include:

* 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.

Conclusion!

For some of the cyber security experts, an air gapped network is not the most practical defense, but it certainly works as an ultimate cyber security measure.   
That explains why most of the high-security industries rely on air gapped systems such as military applications, financial institutions, power plants, aviation systems, and payment networks to name a few.

Creating an air gap sounds easy theoretically (just unplug it).   
However, the real implementation of this solution is not as easy as it seems on the paper. It is much much more complicated.   
Having said that, we are not ruling out the potential security and bandwidth effectiveness of an air gap network or computer, we’d in fact encourage you to take consideration of the cost, constraints and administrative requirements.  
Advanced technology that offers stringent defense against cyber-attacks is the need-of-the-hour since data theft is becoming one of the major issues for business.   
Once an intruder finds a way into your organization’s sensitive data, your businesses can take weeks or even months to recover because all the networked data is infected and encrypted, making it useless.

So if you or your business use an air-gapped system, you must assess or monitor your network to assure your system is correctly air-gapped. Monitoring includes looking for new data coming in from removable media,   
transient devices, or external network connections which are being set up with modems or VPNs.   
And also, you should never forget **social engineering**.

Thanks for your attention.