Air Gap Systems: a way to secure our data

Introduction

Since the begging of network creation, having a secure area and protecting our data from being stolen, was a big challenge for us.

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 yet.

The statistics shows that, although network administers pay attention to their network security and they use the newest solutions, but still cyber-attacks have a high rate.

“*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 think about this a little bit deeper. What happens if attackers find a way to access to a country’s military database?

Not every problem can be solved by money!

So basically there is no way to secure a network at its best?   
The answer is yes, but due to technology’s high development there is a way that we can actually reduce the chances of being attacked by hackers.

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

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

Air-gapping is a way for creating a “roadblock” made of air. 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 remove the network or computer from the internet, an air gap is created.

Air-gap systems 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 physically isolated, **meaning data can only be passed to 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 have the access to all of our systems. **Keeping away our important data from the rest of network is what it does.**

So basically the only way to access this system is physically and not in any other ways you can hack this system, you have to manually go to the system and get the information yourself.

Very simple. But how does this makes our network secure?

How does it make security?

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

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

To get this more clear 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

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 response.

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

* 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, 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 take 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.

Because 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.

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 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:

* 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 that rely on them: 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 difficult.   
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, you businesses can take weeks or even months to recover because all 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 sure your system is correctly air-gapped. Monitoring includes looking for new data coming in from removable media,   
transient devices, or external network connections being set up with modems or VPNs.   
And also, you should not neglect **social engineering**.

Thanks for your attention.