Air-Gapped Systems: Are They Really Air-Gapped? Current Cyber Security Threat and Defence Techniques for Air-Gapped systems

Bilgehan TURAN

bilgehan.turan@eurocontrol.int

EATM-CERT {European Air Traffic Management CERT}

***Abstract*—Generally, critical infrastructures are installed on the physically separated network in order to isolate them from the other part of the enterprise network. This type of isolated system are called Air-gapped systems. The physical separation gives us the wrong sense in terms of security that they are secure and attacks are not possible. On the other hands, today's technologies require more integration with each other to monitor, analyse and data transfer in both internal and external direction. The most of the Air-Gapped systems depends on the integration of other systems e.g. patching systems, maintenance by 3rd parties, data transfer like radar data, meteorology data, aeronautical data, etc. Even if the critical infrastructure is physically separated, there are attack types called side channels that can destroy all of the systems inside the Air-Gapped systems.**

The focus of this paper is the Air-Gapped or well isolated operational systems and based on real audits and penetration test results especially in aviation sector. Currently known attack types and what kind of APT groups are targeting to the Air-Gapped systems were inspected and proposed some attack scenarios with the combination of the typical attack types along with the recommendations to prevent attacks addressing the known threats.

***Index Terms*—Attacks to Air gapped systems, covert channels, mitigation**

I. INTRODUCTION

Air-gapped system or network is one that has no network interfaces, either wired or wireless, connected to outside networks. It is generally confused with the isolated systems that are not connecting to the Internet but there is a physical path connected to outside world even if it is fully blocked and there are many access control mechanisms.

What kind of attacks exists? There are some attacks to air-gapped systems even if there is no network interface, but interfacing with other attack vectors called side-channel attacks or covert channels.

A) Side Channel Attack:

In computer security, a side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs). Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited [1]

Side channel attacks can be categorized as follows:

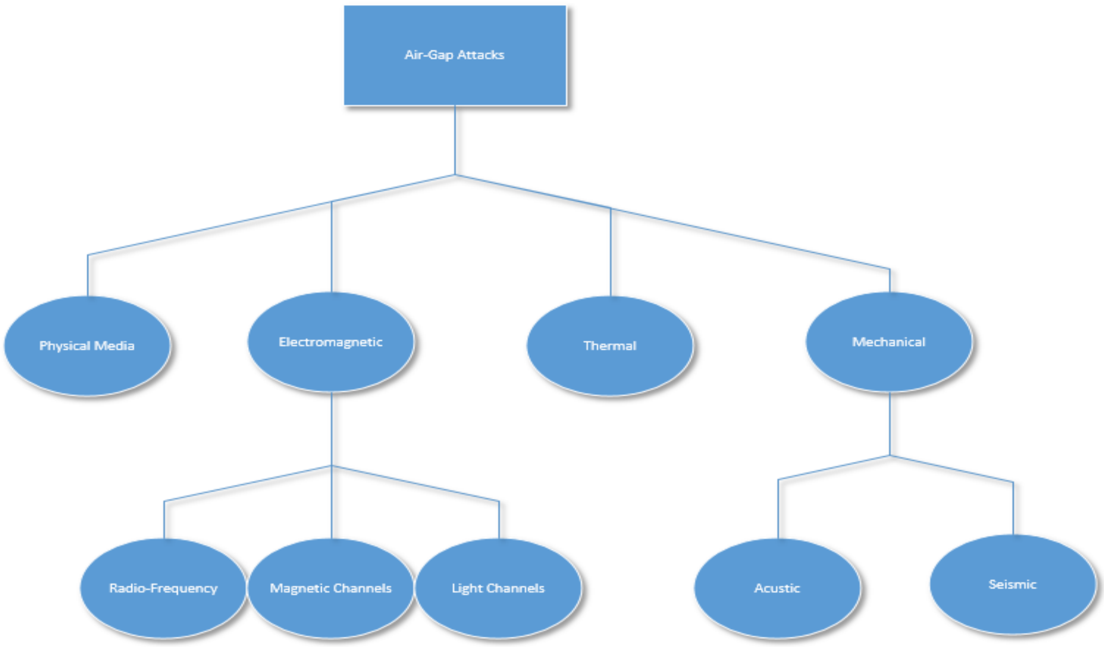

Figure 1 Side-channel attack types

Let us inspect the attack types in the diagram [2].

<u>*Physical Media Attacks:*</u> The most well-known attack type is the physical media. Generally, Advanced Persistent Threats (APT) which are focused on stealing information like intellectual property or destroying the system by using physical media like usb flash drive to infect the air-gapped systems. Here is the some samples of the APTs:

Adversaries	Other Names	Operated Since	Discovered	Media	Attack Air-Gapped	Main Purpose
Stuxnet	-	2005	2010	yes	yes	destruction
Flame	-	2010	2012	yes	yes	information stealing
Turla	Venomous Bear	2007	2015	yes	yes	information stealing
Miniduke	cosmicduke(new)	?	2013	yes	yes	information stealing
Redoctober	cloudatlas(new)	2010	2012	yes	yes	information stealing
APT28	fancybear,sofacy	2008	2014	yes	yes	information stealing
APT30	-	2005	2014	yes	yes	information stealing
HAmmerDrill	NSA tool	?	2016	yes	yes	information stealing
Brutal Kangaroo	NSA tool	?	2016	yes	yes	information stealing

Table 1 APT Groups Attacking Air-Gap Systems

As you see, there are many APT groups dealing with Air-Gapped systems generally dealing with information. If you check the APT's "*start operation*" and "*discovery date*" in the table, there is a huge gap between them. Since these groups use different techniques to become stealth, it is very hard to detect even if the detection methods are in place. However, never forget that when you defend your system, you should be perfect, but when the attackers penetrate into your system, they have to be perfect. They always make mistakes and the key idea is due diligence.

Thermal Attacks: There is an interesting attack that should be checked by using the thermal changes in the environment [3]. The attack based on hacked HVAC systems that resides between corporate and air-gapped networks and the malware inside the air-gapped systems is ready to sense the temperature increase and decrease. Although bit rate is very low which is approximately 1 byte/hour, it is enough to send the “Kill’m all” signal to the air-gapped system.

Electromagnetic Attacks:

Radio-Frequency Interference Attacks: (also known as Electromagnetic Interference (EMI)): in 2007, NSA declassified the document about electromagnetic interference [4]. This document is the first one that mentions about the term TEMPEST (Transmitted Electro-Magnetic Pulse / Energy Standard and Testing). Principle is simple: every electronic devices like PCs, monitors, cables, etc radiates the electromagnetic waves and it is possible to get these waves and demodulate it. CRT monitor could be captured from 1 km away [5]. There are many researches on this subject [6] [7].

Magnetic Attacks: The modulation of electromagnetic fields can be used for communication. The researchers succeeded to modulate and send data with electromagnetic fields with the help of modern mobile phones but only a few inches [8].

Light Attacks: Data can be easily modulated with LED [9] or IR. The researchers succeeded to send 4kb/s data transfer that is enough for exfiltration encryption keys, keystroke, text and binary files.

Acoustic Attacks: BadBIOS malware is the one sample for acoustic attack [10]. It sends the data with ultrasonic sounds by infecting the bios. There are also research about acoustically talking networks which are very effective to steal information [11].

Seismic Attacks: This attack is based on vibrations. For air-gapped systems, it is not a vector because it can be done for short distance just less than a meter [12].

The following table consolidates the side channels attack in terms of different aspects:

Covert Channel	**Channel Availability**	**Feasible**	**Stealth**	**Distance**	**Bitrate Range**	**Exfiltration**	**Destruction**	**Attack Probability**
Physical Media	If enabled in systems	yes	medium	N/A	~GB/x days	yes	yes	very high
Thermal	Depends on temperature changes.	no	low/high	40 cm - unlimited	low	not feasible	yes	very low
Magnetic	High	no	High	low	low	not feasible	not feasible	very low
Light	depends on user absence	yes	low/high	line of sight	15bit/s - 4Kb/s	yes	yes	medium
Acoustic	High	yes	High	~15 m	900bit/s - 10Kb/h	yes	yes	medium
Seismic	Low	no	low	~10cm	low	not feasible	not feasible	very low
Electromagnetic	High	yes	High	~50m-1km	48 bit/s - 5Kb/s	Yes	yes	high

Table 2 Side Channel Attacks Evaluation [13]

Attack probability shows that which one of the method is more probable for attacks. Do not forget that everyday there are new researches and side channel attacks are evolved and becoming more feasible for data exfiltration and destruction. As seen in the table that the most feasible attack for the attackers is the physical media if the target is exfiltration. On the other hand, if the attacker wants to become stealthier, the advanced side channel attacks shall be chosen like electromagnetic and acoustic. The destruction can be done with many of the side channel attacks. You can be one of the victim of these attacks by chance even if it is not targeting your systems like ransomwares.

B) Why air-gapping is not a long-term cybersecurity solution [14]

Nowadays, the integration of air-gapped systems with IT infrastructure is inevitable. This requirement pushes the air-gapped environments being opened to the outside world. The following is the list of why air-gapping is not a long-term cybersecurity solution:

1) It may give false sense of security. Attacks are evolving and APTs are realized the values behind this systems. New and creative methods are always in charge.
2) Air-gapped systems produce valuable data and they should be analysed to extract valuable information and published in anonymized way to the public.
3) Air-gapped systems cannot be managed by remotely. It requires more resources. What about if you have problem in a critical component that you are not the expert. There should be a way to connect from outside for system support for specific system that requires expertise.

Although air-gapped environments are opened connections to the outside world, they are not blindly opened. There are different precautions like strong access control mechanism, data diodes, data gateways, etc. In secret environment, for example data diodes can be used for only transmission into the more secret network but other way around is not allowed. Nevertheless, this time data transfer from secret networks is an issue and mostly usb drives are used with strong security checks. As seen so far, there is always a way to access to the well isolated systems. Let us inspect the anatomy of the attack executed on a well-isolated system [15].

Ukrania power grid attack is a good example of how attackers plan and executed a well-coordinated attack in a well-isolated system. Here is the summary of the attack steps:

- The attackers entered to the system before the destruction launched by phishing attack called blackenergy3. The network was well segmented and they cannot access to the SCADA systems initially. *For six months*, they conducted extensive reconnaissance, compromise Windows Domains, steal credentials for internal and VPN systems, understands how to access the ICS systems.
- The attackers reconfigured UPS systems, which are responsible for providing backup power to two of the control centers in order to increase the impact.
- The attackers studied the grid network since every implementation is different. They replace serial-to-Ethernet converters with malicious one that are used to send command from SCADA system to the substations.
- The attacker were ready to attack to the system at 3:30 pm December 23 2015.
  - They entered systems with the stolen VPN accounts and disabled the UPS systems first.
  - Before they started the attack, they have started a denial of service to telephone to the customer call centers to prevent customers from calling in to report the outage. The call center flooded with illegitimate calls. This shows very high sophistication of attack that attackers thinks every possibilities that prevent the system meltdown.
  - The attack started and all substations taken down and firmware was overwritten.
  - After 90 minutes, all computers were wiped with unrecoverable manner, converters and UPS were unusable.
- Recovery time took several months.

Here is the rough timeline depiction of the attack:

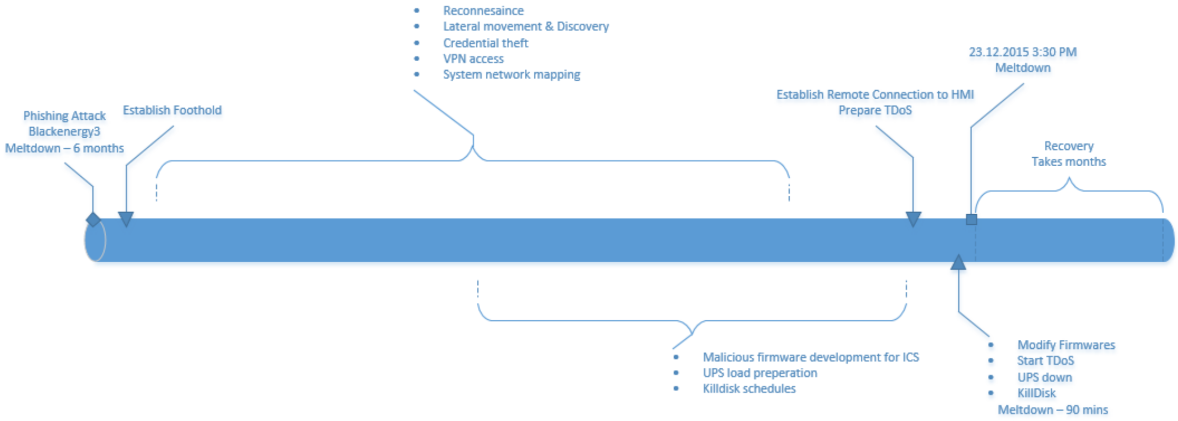

Figure 2 Timeline of Ukranian Power Grid APT Attack

This attack proves that if there is an access path to the critical operational systems, the attackers probably find out how to penetrate and it is only the matter of time. Of course, there are always ways to prevent this type of advance threats by providing defence in depth.

II. COMBINED SCENARIOS

A) Motivation

As seen so far, there are different types of side channel attacks for air gapped or strongly isolated systems. On the other hand, the success of attack types are depends on some conditions and special hardware. The most effective way is to implant a malware and try to find a communication medium. The problem is how to implant your malware into air-gapped systems. The most of the companies' physical security rely on physical access control system and that poses the risk of air-gapped system. The side channel attacks can be combined with other kind of attacks like bypassing the physical access control systems to implant the malware or device that contain malware and communication mediums that will interfere the outside world by means of related side channel.

B) Combined Attack Scenario - I

The first scenario is to implant the malware in to air gapped systems. In order to do that there are several ways:

- The proximity card that has the access to air gapped system rooms can be cloned. Proxmark is one of the tool for supporting variety of RFID cards. You can clone rfid cards with hi(13.65 Mhz) and low frequency(125 kHz).
- One insider can plug the usb flash drive containing malware into one of the machines. Rubber ducky and maldiuno are the well-known attacking tools. These tools have usb interface and are recognized as keyboard and they can run codes when inserted into computer. Anybody can insert into the computer and run a backdoor.
- One of the employer, who found the usb that look benign but its firmware modified, plugs into one of the system. There is a good analysis for baiting attacks presented in Blackhat conference [16].

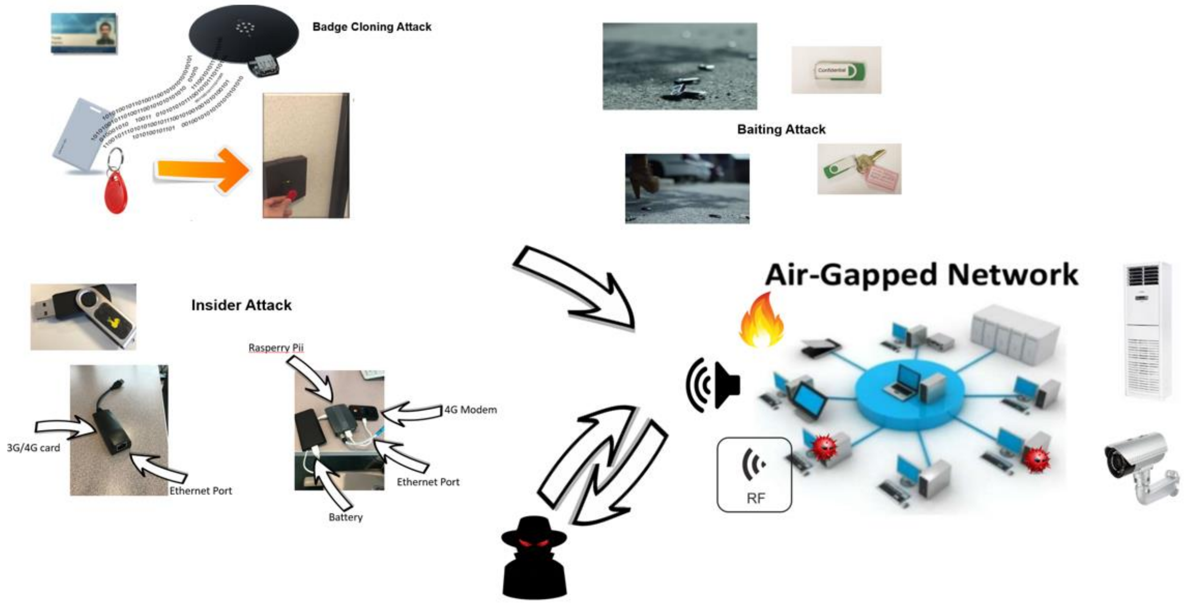

Figure 3 Combination of Physical Attack Methods with Side-Channel Attacks

One of the above method is enough to implant the malware. If the motivation is destruction, it is easy for the attacker to establish a scheduled time bomb that will be activated in a suitable time to wipe all systems in the air-gapped systems. On the other hand, if the motivation is information stealing, then the attacker shall be careful about being stealth and establish the communication channels, which require extra effort. If the implanted malware is used with hardware, which is able to establish wireless communication, then the attacker can have direct access to air gapped system. However, in many case, wireless communication signals may be poor because of the location and building type. Therefore, the attacker shall find other methods to exfiltrate data by compromising the supporting systems like the air ventilation system, CCTV, etc. mentioned in side-channel attacks.

Combined Attack Scenario - II

Air gapped systems turn out to be well isolated systems instead of physically segregated one. This is explained in the above section Why air-gapping is not a long-term cybersecurity solution.

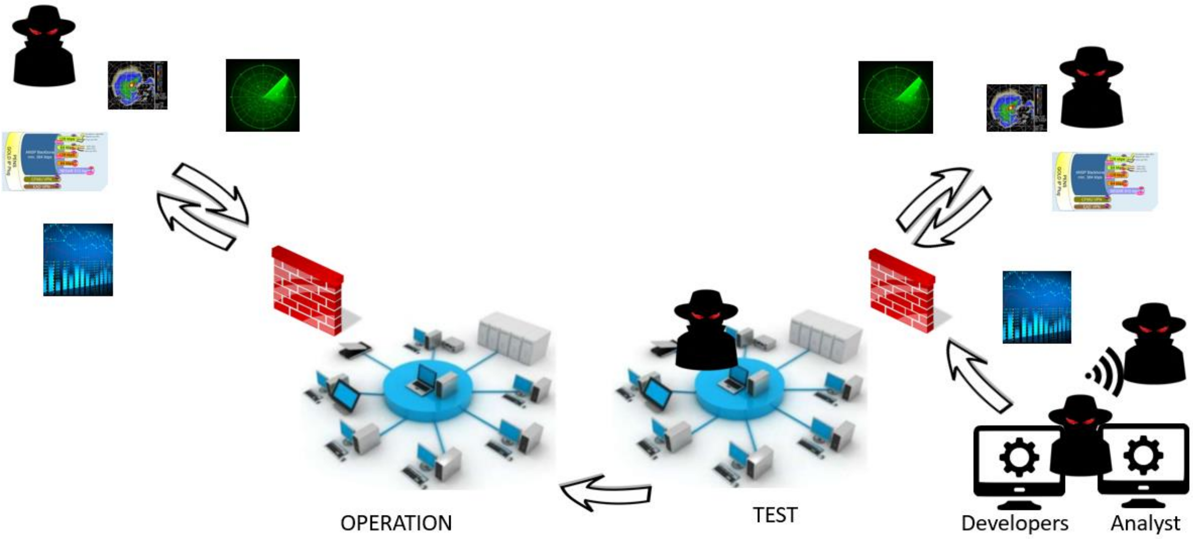

Figure 4 Attack Points in Sample Well-Isolated Environment

Any compromised trusted partner that connected to air gapped systems pose a risk. The attacker can compromise one of the partner and can try to bypass access restrictions for that connection. It is a fact that extranet connections are generally more relax than the others since the connections are from the trusted partners. Nowadays, there are attacks that first compromise the 3rd party connections and attacking the real target from there. The attackers think that why try to break the well-hardened and monitored systems instead of the backdoor that has less protection. In addition, test environments also have more relax access control rules, the attackers generally prefer these entry points. In real life, there may be entry points from test environment to the operation because of some misconfigurations and vulnerabilities.

III. COUNTERMEASURES

Here is the list of countermeasures that can be assumed as quick wins for defending your systems based on the penetration tests result conducted on the aviation sector.

A) Physical layer attacks prevention

- Use 2-factor Authentication along with Biometric checking in physical access control systems. Never rely on one factor authentication like badge or keypad access. 2-factor authentication prevents badge cloning, brute force password attacks to keypads. For biometric authentication prefer the method for better crossover error rate. There is an analysis for comparison of the biometric authentication [17].

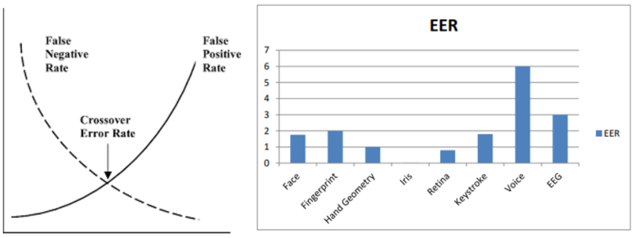

Figure 5 Two-Factor Authenticaion

- Disable usb storage ports on OS, prevent direct access to bios whenever possible. Physical usb port and cable blockers can be used for better protection. There are some attacking hardware that pretend like a keyboard or a mouse and runs malware on the systems when inserted into usb port.

Figure 6 Usb locks

- Disable other data transfers mediums like thunderbolt, cdrom, external sata. Any of these mediums are used for data transfer and they have the same level of criticality for transferring malwares into the air-gapped systems. There are tools for stealing information from air-gapped systems like HammerDrill and Brutal Kangaroo that were leaked by Shadow brokers hacker group [18]
- Remove or disable audio card in systems and remove any speaker to prevent acoustic side channel attacks.
- Protect support systems like HVAC, CCTV as like the main systems.
- Protect system rooms. Separate the rooms for different roles, compartmentalise the rack cabinets and also add biometric protection for accessing the rack cabinet.
- Don't allow anybody else access to the system without escorts including the stuff for cleaning and maintenance.

B) Network layer attacks prevention

- Protect External accesses. There shall be separate firewall that ended the connection from external trusted parties. Every connection shall be micro segmented that ensures that no parties can reach the others.
- 3rd party support company connections shall be done in controlled environment for maintenance purposes. The connection shall be available when there is a need. Physically, it shall be enabled and monitored during the maintenance.
- 2-factor authentication is the key element for securing the authentication. Whenever it is feasible, 2-factor authentication shall be applied such as in remote VPN access.
- Disable unattended network ports in your premises. If possible, 802.1x is a good implementation in the sense defence in depth.
- Disable wifi functionality in all devices like PCs, printers, TVs.

C) Application layer attacks prevention

- During the data transfers, always check the format and content of the data with content or protocol analyser.
- Format conversions prevents malwares to be exported to new format. Converting pdf and office formats into other format prevents malwares to be exported to new format.

D) Monitoring

- Test your system security periodically.
- Monitor physical access control systems.
- Mirror the important traffic into another network and monitor all incoming traffic with IDS sensors.
- Collect critical logs and monitor.
- Monitor regularly the RF signals especially GSM (900Mhz, 1800Mhz, 1900Mhz) and WIFI frequencies (2.4Ghz,5Ghz). Use spectrum analyser to analyse regularly for more broad range signals in your location.

IV. CONCLUSION & FUTURE WORKS

Air-gapped systems are indeed well isolated systems that has many access level protections. Every day new methods are discovered by both the attackers and the researches to bypass these security precautions. This paper is prepared for exploring what kind of attacks and threats exists to the well-isolated systems. Even with the simple combination of the other typical cybersecurity attack types with side-channels, the attacks magnitude and stealthiness will be higher. New different types of attacks will be monitored for future and will be analysed accordingly.

References

[1] wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Side-channel_attack.

[2] B. Carrara, “Air-Gap Covert Channels Phd Thesis”.

[3] Yisroel Mirsky, Mordechai Guri, and Yuval Elovici. , “Hvacker: Bridging the air-gap”.

[4] NSA, “TEMPEST:A signal problem,” [Online]. Available: https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf.

[5] W. V. Eck, “Electromagnetic radiation from video display units: an eavesdropping risk?,” [Online].

[6] M. G. Kuhn, “Electromagnetic eavesdropping risks of flat-panel displays,” [Online].

[7] Markus G. Kuhn and Ross J. Anderson, “Soft tempest: Hidden data transmission using electromagnetic emanations,” [Online].

[8] Ragib Hasan, Nitesh Saxena, Tzipora Haleviz, Shams Zawoad, and Dustin Rinehart, “Sensing-enabled channels for hard-to-detect command and control of mobile devices”.

[9] Mordechai Guri, Boris Zadov, Yuval Elovici, “LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED”.

[10] “https://en.wikipedia.org/wiki/BadBIOS,” [Online].

[11] M. Hanspach and M. Goetz, “On Covert Acoustical Mesh Networks in Air”.

[12] P. Marquardt, A. Verma, H. Carter and P. Traynor, “iPhone:Decoding vibrations from nearby keyboards using mobile phone accelerometers”.

[13] P. Mordechai Guri, “The Air-Gap Jumpers, Ben Gurion University Blackhat 2018 presentation”.

[14] https://3tsoln.com/blog/2018/05/29/why-air-gapping-is-not-a-long-term-cybersecurity-solution/. [Online].

[15] M. J. A. C. -. S. I. Robert M. Lee, “https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf,” [Online].

[16] Bursztein, “Does Dropping USB Drives in Parking Lots And Other Places Really Work, US Blackhat 2016”.

[17] P. T. I. V. R. K. H. BISMITA CHOUDHURY, “A Survey on Biometrics and Cancelable Biometrics Systems”.

[18] “http://en.wikipedia.org/wiki/The_Shadow_Brokers,” [Online].

Tables

Figures