International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)

ISSN: 2456-236X

Vol. 04 Issue 02 |2020

Air-Gap Malware Prevention Techniques

Anand V

MCA Scholar, Department of MCA, School of CS & IT, Jain (Deemed-to-be) University, Bangalore, Karnataka, India

ABSTRACT

Air-Gap is also a term used interchangeably, which means to isolate a system physically, i.e. Computer from all the other system, if that computer has more sensitive data and it should only be accessed by authorized personals only. This itself is a security measure but that is still not enough as frequencies and signal can go beyond walls. It has been found out the attackers can extract information even use mediums such as sound, light, vibrations, electromagnetic, heat, radio signals and frequency emitting from the computer. For this they use sensors and airgap covert channels This vulnerability is mostly found in modern computer systems such laptops as there are in-build microphones, speakers, Wi-Fi, Bluetooth which can emit information. The radiations and frequencies emitted from the computer can go up to a distance of 18-20 meters. Although the vulnerability of air-gap haven't yet been fully treated, there are some techniques can come in handy if it helps to prevent the leakage of a tiny bit of information. And also, this can be integrated with any other projects which helps in closing the vulnerability and giving a heads up against those attacks.

Keywords: **Air-Gap – Physical Isolation, Malware –A program malicious software created with the intention of damaging system or steal data, Ex-filtration – Unauthorized data transfer, Infiltration – Entry without authorization or permission, Channel – Path through signals flow**

1. INTRODUCTION

Up until the year 2014, it was believed that only data can only be transmitted or leaked using the frequencies of Wi-Fi and Bluetooth only. Then a researching team found out a malware named "AirHopper" [8], which technically was not a malware but an attack pattern which exfiltrates data from an 'Air-Gapped' computer to an Android device nearby. AirHopper used FM waves for exfiltrating the data.

Later in 2015, another researching team introduced a way for breaching Air Gapped Systems, they called it "BitWhisper" [9]. Here thermal sensors were used and heat emitted from the compromised system was monitored.

In that same year the researchers had introduced "GSMem" [9] which used GSM Frequency signals and data was successfully transmitted to a nearby cellphone in a range of 25-30 meters. The infected computer modulated and transmitted the signals in such a way that it was readable by the android device.

In 2016, a categorization was made as "OOB-CCs" [8] abbreviated as "Out of Band Covert Channels". In these malware communication channel,no, special hardware was required at both ends, the receiver and the transmitter. OOB-CCs didn't have higher bandwidth like the earlier ones but still data with small size like txt files, short record messages were able to be monitored.

1.1 Aftermath

Air-gapping a computer was practiced much before at the time of finding the vulnerability. Usually it was done to restrict unauthorized physical access and security issues. Even the use of removable storage was restricted on those systems. Air Gapping was done on various environments such as in Computers maintaining financial data, control systems, Life Critical Systems, Engine controls.

The Air gapping did not help much. Several malwares such as Stuxnet, agent.btz were introduced and thus they started to exploit vulnerabilities. The Stuxnet was infected to the nuclear Plant of Iran just by using a thumb drive. Although there have been incidents from time to time, it has been proved that these breaches are avoidable and feasible.

1.2 Suggested Solutions

This is the main problem and the suggested solution if it works, is to change the settings of the air gapped computer or any computer according to the situation in such a way that the data will not be leaked in any way possible especially though the mediums such as sound, light, vibrations, electromagnetic, heat, radio signals and frequency emitting from the computer.

2. STUDIES ON ATTACKS AND TECHNIQUES

The concept of exfiltrating information without any data transmitting seemed illogical. Seems illogical even today. That is where the black hat hackers win, make the victims believe that they are not victims at all. Although these was some studies on whether this is possible or not from time to time and it was found working.

2.1 TEMPEST [10]

Everyone knows that electronic devices produce electromagnetic fields, which can cause interference. For radio and television reception. However, intervention is not the only problem Electromagnetic radiation. In some cases, it is possible to get information about the codes used inside Equipment when the radiation is taken and the signals received. Especially in the case of digital devices pose a problem because of the remote reconstruction of signals inside the device can initiate the reconstruction of the data being processed.

TEMPEST works by capturing and reconstructing the electromagnetic radiation delivered by eavesdropping technology. Computer monitors display information by using an electron gun to manipulate pixels. The electron gun burns the pulses of the electrons, which cross the screen hitting pixels. Right and up and down several times per second. The electrons that are pushing the voltage level rise and fall based on it. Whether to make the pixel lighter or darker. This process produces an electromagnetic pulse, which releases the electromagnetic radiation or electromagnetic radiation, which oscillates out over great distances. There are other sources because the data is stored in binary code and processed as 1s and 0s, ON s and OFF s; the reason again is that the pulses and EMR from these radio waves are like fingerprints.

2.2 Air-Gap Covert Channels [1]

It has also been demonstrated to be hundreds of bits can be detected randomly without using FHSS modulation and delay between symbols under certain conditions. This result shows it
Steganographic capability when properly placed in a safe environment. The crypto-acoustic channel, if not eliminated, can be greatly reduced by a sound power detector for optimal bandwidth and active jamming technique. It is also estimated that some methods are not even requiring a physical channel.

There is only one jamming technique, effective against specific modulation schemes
It is not possible to give all the modulation schemes tested as useless. Without the use of jamming devices that produce a significant amount of wideband noise, that means jamming the barrage with enough electricity. Finally, an additional safety net and active jamming and passive monitoring are also recommended.

2.3 Air-Hopper

Infiltration into air-gapped networks has proven possible in recent years (e.g., Stuxnet), while data acceleration from air-gapped networks is still considered one of the most challenging phases of an advanced cyber-attack.

"Airhopper", a malware that uses FM signals to bridge the air-gap between a separate network and nearby infected mobile phones. While it is known that software can intentionally generate radio emissions from video display units, this is the first time that mobile phones have been considered in the aggression model as objective recipients of radio signals generated by an accident. Textual and binary data can be tied to a mobile phone from a physically separate computer at a distance of 1-7 meters, with an effective bandwidth of 13-60 bps (bytes per second).

2.4 Bit-Whisper and GSmem[9]

A team led by Mordechai Guri worked on a project using a named method on Air-Hopper, which uses FM waves for data exfoliation. A new research initiative called Bit-whisper is part of ongoing research on the topic of air-gap security at Ben-Gurion University's Cyber Security Research Center. Bit-Whisper is a display for an obscure two-way communication channel between two adjacent ones communicating heat through an air-wrapped computer. This method allows them to communicate using their body heat emitters and built-in thermal sensors, eliminating the air-gap between both physically adjacent and compromised computers.

2.5 Known air-gap covert channels

Type of Channel	Method of exfiltration	Emitting Hardware
Electromagnetic	TEMPEST	Video Card
	MAGNETO and ODINI	CPU
	USBee	USB Connector
	AirHopper	Video Card
	GSMem	RAM
Acoustic	Fansmitter	Laptop fans
	Ultrasonic	Microphones and Speakers
	DiskFiltration	Hard Disk Drives
Thermal	BitWhisper	GPU/CPU
Optical	LED it GO	HDD LED
	VisiSploit	Invisible pixels
	xLED	Router LEDs
	Air-Jumper	Invisible pixels

3. TECHNOLOGIES USED RELATED TO AIR-GAP MALWARE

3.1 TEMPEST SHIELDING

TEMPEST [5] shielding is the process of protecting sensitive devices from electromagnetic radiation (EMR), which can carry classified information. This is to prevent it from being interrupted by external organizations. It also refers to self-shielding, which is applied to electronic devices to interrupt EMR transmission. As a result of this defense, precautionary measures were taken during the Cold War to conceal secrets at the height of the political goon movement.

TEMPEST has since been regarded as an acronym of Transient Electromagnetic Pulse Monitoring Technology, which refers to devices and devices that emit or receive data from electromagnetic resonance, known as compromised emission.

Fig 1: TEMPEST Attack

3.2AUTORUN ATTACKS USING USB

The most obvious and simplest of all attacks is the using od thumb drives to insert malware inside a system. The malware will work in such a way that it will transmit without the knowledge of the user. If the attacker has a momentary chance of getting the infected USB device into an air-gapped machine, they can do a lot of damage. Stuxnet provided the first and foremost examples of threats from USB autorun attacks. It is now widely known that US Intelligence can use Stuxnet to compromise air-gap Iran nuclear reactors through the USB. With the use of USB ports, the possibilities are endless. Cottonmouth, developed by the NSA and leaked to the public in 2014, is a USB hardware hack that provides software persistence and over-the-air communication via RF links to prevent air gaps.

Black Hats now a days know how to harm firmware on a compromised USB device so that no computer can perform without hardware modification and forensic detection at the system level.

Fig 2: Autorun attack by inserting thumb drives

3.3 MAGNETO: Using Android phones to monitor Electromagnetic Signals from the CPU [12]

It is obvious that electromagnetic signals will get leaked out on the CPU while working. But it can it be monitored and Decrypted Malware that controls magnetic fields controls the workload of CPU core. Sensitive data such as encryption keys Password or keying data is encoded and transmitted on magnetic signals. Smartphone nearby the computer receives secret signals with its magnet Enrollment Device. The secret channel worked through the user process, without the need for privileges.

Apart from cellular, Wi-Fi, Bluetooth and NFC, the hardware and magnetic sensors are not considered communications interface. As such, you can access them with basic permissions. The Android mobile captured the data, thus finding that experiment successful.

Fig 3: Monitoring using Android

3.4 LIGHT FROM LED STATUS INDICATOR

Transferring files to a computer with a USB drive is also dangerous in some circumstances, but thanks to some LED lights that hackers made on his own drive, this attack vector is low on it. Using a USB drive with a single LED illuminated during read or write operations, but this is very common, as it is possible to accidentally transfer malware through a USB drive, especially writing task. There is a dedicated LED for which any user is alerted to write anything. Operations trying to travel under the radar. A recent article by Bruce Schneier highlighted a flaw in the USB drive. Their creation gives users more control over when their drives are accessed and in what ways, which can also be used to discover the specific uniqueness of the chosen operating system.

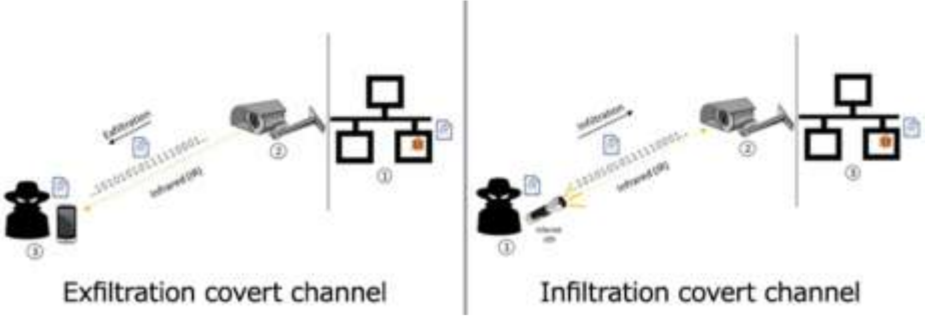


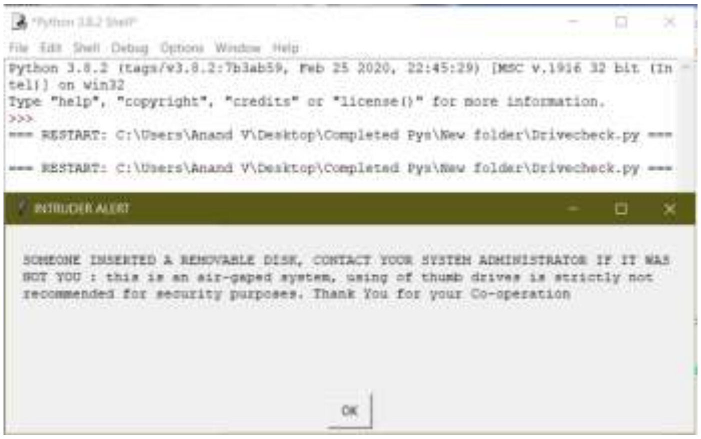
Fig 4: Exfiltration and Infiltration using LED

4.HOW TO PREVENT IT?

There can be some techniques that can be used and tools that can be built to prevent data leakage from the system. Building tool in Python language is recommended as it has more libraries and repositories that can be implemented on the computer hardware. Some techniques and an example model of how it can be implemented is also given below.

4.1 By checking for any thumb drives and prevent it from ever being inserted

A hacker can insert thumb drives and can do autorun attacks, which can manipulate the computer to send out data in the form of signals. To prevent this, a tool can be created which will display a warning message whenever someone tries to insert a thumb drive and will continue to display until the thumb drive is ejected from the system.



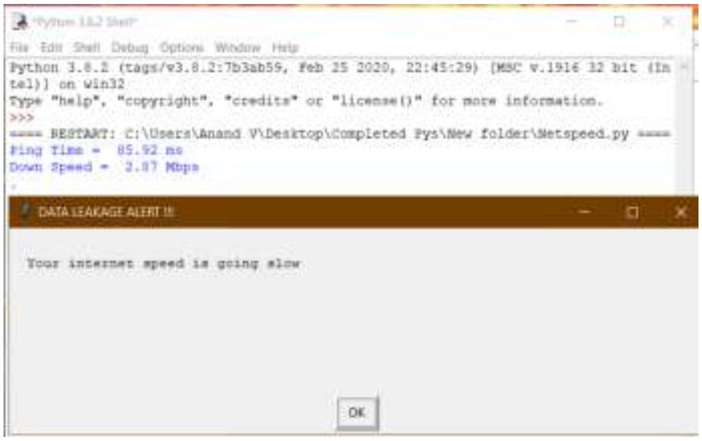
```
Python 3.8.2 (tags/v3.8.2:7b3ab59, Feb 25 2020, 22:45:29) [MSC v.1916 32 bit (In
tel)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
=== RESTART: C:\Users\Anand V\Desktop\Completed Pys\New folder\Drivecheck.py ===

=== RESTART: C:\Users\Anand V\Desktop\Completed Pys\New folder\Drivecheck.py ===
```

```
SOMEONE INSERTED A REMOVABLE DISK, CONTACT YOUR SYSTEM ADMINISTRATOR IF IT WAS
NOT YOU : this is an air-gaped system, using of thumb drives is strictly not
recommended for security purposes. Thank You for your Co-operation
```

Fig 5: Warning message

4.2 By checking the bandwidth speed

Proper monitoring of internet speed is always recommended. If some leakage of information is happening, then definitely the speed of internet will go down. The ping speed should also be monitored. Lower the Ping speed, Higher the bandwidth. A tool can be created will inform the user if the bandwidth speed goes beyond a specified limit.



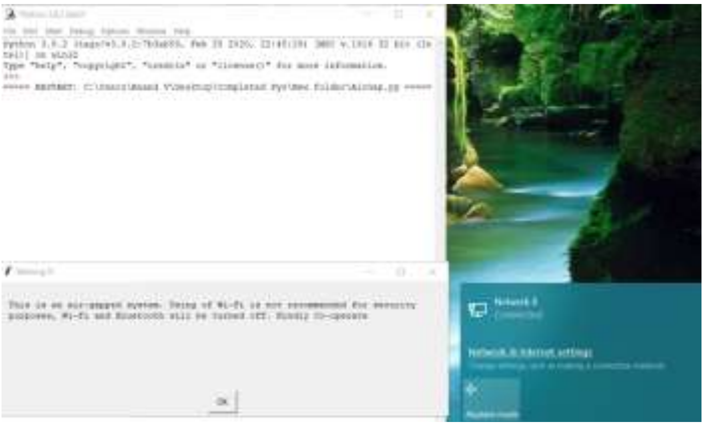
```
Python 3.8.2 (tags/v3.8.2:7b3ab59, Feb 25 2020, 22:45:29) [MSC v.1916 32 bit (In
tel)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
==== RESTART: C:\Users\Anand V\Desktop\Completed Pys\New folder\Netspeed.py ====
Ping Time =  85.92 ms
Down Speed =  2.87 Mbps
```

```
Your internet speed is going slow
```

Fig 6: Bandwidth speed is monitored in Realtime

4.3 Turning off the Wi-Fi and Bluetooth connectivity

Air-gapped computers are not supposed to have connectivity over Wi-Fi and Bluetooth. Wi-Fi and Bluetooth are inbuilt in almost all the laptops these days. Data has high risk for getting breached through these mediums. This tool will silence those medium until the user until the user wishes to access the internet. Although it is thoroughly not recommended to access internet from an air-gapped system.



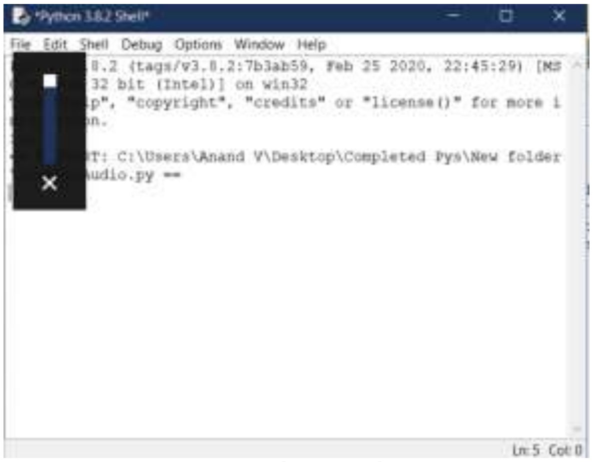
```
Python 3.8.2 (tags/v3.8.2:7b3ab59, Feb 25 2020, 22:45:29) [MSC v.1916 32 bit (In
tel)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:\Users\Anand V\Desktop\Completed Pys\New folder\[illegible].py =====
```

```
This is an air-gapped system. Using of Wi-Fi is not recommended for security
purposes, Wi-Fi and Bluetooth will be turned off. Kindly Co-operate
```

Fig 7: Wi-Fi and Bluetooth are turned off

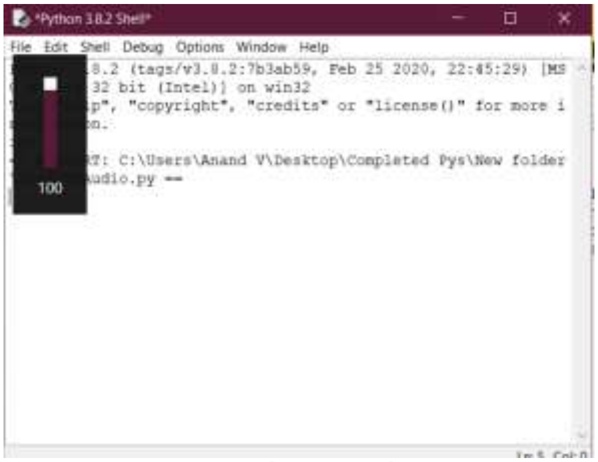
4.4 Bydistorting the audio

Audio waves were also used to track the information. Simply muting the audio may not help. Best option is to distort the audio i.e. turning the audio off and on from time to time. Suppose if the computer is being affected by a malware which causes it to transmit data by using audio signals, the data may get transmitted but will be distorted and meaningless if the audio is fluctuated. Thus, it can reduce this vulnerability.



```
8.2 (tags/v3.8.2:7b3ab59, Feb 25 2020, 22:45:29) [MS
 32 bit (Intel)] on win32
p", "copyright", "credits" or "license()" for more i
n.

T: C:\Users\Anand V\Desktop\Completed Pys\New folder
udio.py ==
```

Fig 8: Audio is Muted



```
8.2 (tags/v3.8.2:7b3ab59, Feb 25 2020, 22:45:29) [MS
 32 bit (Intel)] on win32
p", "copyright", "credits" or "license()" for more i
n.

T: C:\Users\Anand V\Desktop\Completed Pys\New folder
udio.py ==
```

Fig 9: Audio is Unmuted

5. CONCLUSION

Although the vulnerability of Air-Gap leakage is not 100% closable at the present scenario and the concept of Air-Gap malware seems illogical, the damage caused in real and the threat is also real. From time to these has been studies about this, some techniques can be definitely used to mitigate the loss caused due to this. There is a chance that this threat can get bigger in the future. These are only some techniques; however, I hope this will give a heads up to anyone who is willing to have an advanced research to find a close more vulnerabilities.

6. REFERENCES

[1]. Carrara, B. (2016). *Air-Gap Covert Channels.* Ottawa, Canada.

[2]. Chaouki Kasmi, J. L. (2015). Air-gap Limitations and Bypass Techniques: “Command and Control” using Smart Electromagnetic Interferences. *THE JOURNAL ON CYBERCRIME & DIGITAL INVESTIGATIONS, VOL. 1, NO. 1, DEC. 2015, BOTCONF 2015 PROCEEDINGS*, 7.

[3]. Dan Maloney, P. U. (n.d.). *HACKADAY Air Gap*. Retrieved from HACKADAY: https://hackaday.com/tag/air-gap/

[4]. Goetz, M. H. (2013). On Covert Acoustical Mesh Networks in Air. *Journal of Communications Vol. 8, No. 11, November 2013*, 10. Retrieved from http://www.jocm.us/uploadfile/2013/1125/20131125103803901.pdf

[5]. Goodman, C. (2020). *Sans Instutute Reading Room.* Retrieved from An Introduction to TEMPEST: https://www.sans.org/reading-room/whitepapers/privacy/introduction-tempest-981

[6]. Guri, M. K. (2014, Nov 2). *Cryptography and Security*. Retrieved from arXiv: https://arxiv.org/abs/1411.0237

[7]. Guri, M., Kachlon, A., Hasson, O., Kedma, G., Mirsky, Y., & Elovici, Y. (2015, August). *24th USENIX Security Symposium.* Retrieved from USENIX: http://blogs.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/guri

[8]. Guri, M., Kedma, G., Kachlon, A., & Elovici, Y. (2014, November). *AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies*. Retrieved from https://arxiv.org/abs/1411.0237

[9]. Guri, M., Monitz, M., Mirski, Y., & Elovici, Y. (2015). *BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations.* Beer-Sheva, Israel: Cornell University. Retrieved from https://cyber.bgu.ac.il/bitwhisper-heat-air-gap/

[10]. Guri, M., Zadov, B., Daidakulov, A., & Elovici, Y. (2018, February). *ODINI : Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields*. Retrieved from https://ui.adsabs.harvard.edu/abs/2018arXiv180202700G/abstract

[11]. Khandelwal, S. (2018, February 8). *The Hacker News*. Retrieved from https://thehackernews.com/2018/02/airgap-computer-hacking.html

[12]. Mordechai Guri, A. D. (n.d.). *arXiv*. Retrieved from MAGNETO: Covert Channel between Air-Gapped: https://arxiv.org/ftp/arxiv/papers/1802/1802.02317.pdf

[13]. Schneier, B. (2013, October 11). *Schneier on Security*. Retrieved from Air-Gaps: https://www.schneier.com/blog/archives/2013/10/air_gaps.html

[14]. Terdiman, D. (2012, April 12). *CNET*. Retrieved from http://news.cnet.com/8301-13772_3-57413329-52/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/

[15]. Visu, D., Chakkaravarthy, S., Kumar, K., Harish, A., & Kanmani. (2014, October). Retrieved from https://web.archive.org/web/20150322095128/http://www.veltechuniv.edu.in/Newsletter/cse_Oct2014_newsletter.pdf