University of Padova

Department of Mathematics "Tullio Levi-Civita"

Master Thesis in Cybersecurity

Analysis of airgap security attack vectors and mitigating strategies

Supervisor
Asst. Prof. Alessandro Brighente
University of Padova

Co-supervisor
Prof. Mauro Conti
Co advisor University

Master Candidate
Naveen kumar Suresh Babu

Student ID
2004280

Academic Year
2021-2023

“Dedication or Quote”

“The internet is a battleground, and everyone is a potential target.” - Eric Schmidt

Abstract

We are aware that cyberattacks are a common threat to both information technology (IT) and operational technology (OT) today. As attackers continue to become increasingly capable of defeating current security appliances, organizations are moving towards air gap security. The term “air gap” relates to the idea that there is a vacuum in the connection that exists between the computer and other outside networks. The computer is not directly linked to the organizational network since there is a gap in the air; hence, it cannot be attacked via the network because it is not directly linked. Air gap has the goal to isolate the most vital systems from both the organization’s network and the outside world. The private organization’s concluded that airgap security is an effective option should be considered with caution, as it still presents vulnerabilities to some attacks, and there is no research existing with a consolidated view for the classification of air gap security attacks and the countermeasures for the air gap security attacks, despite numerous studies demonstrating that air gap security system is not completely safe since it is vulnerable to threats such as acoustic emanations, electromagnetic interference, and ultrasonic covert transmissions (Speaker-to-Speaker), etc. If practitioners want to deploy air gap security, they must have a comprehensive understanding of the security posture that we have provided in this thesis. We present unique consolidated threats and their corresponding countermeasures. Additionally, we analyze a workable semi-permeable air gap (SAG) technology solution and countermeasures.

Keywords: Air gap security, attack classification, countermeasure,

Contents

Listing of figures

Listing of tables

Listing of acronyms

FTC	Fundamental Theorem of Calculus
NSA	National security agency
DoD	Department of Défense
SIPR	Secure Internet Protocol Router
NIPR	Non-Secure Internet Protocol Router
NTI	Nuclear Threat Initiative
AG	Air Gap security
SATA	Serial Advanced Technology Attachment
EMR	Electromagnetic radiation
EMI	Electromagnetic interference
IOC	Indication of compromise
RFI	Radio frequency interference
SDR	software-defined radio
HZ	Hertz
OT	Operational Technology
IT	Information technology
SOC	security operation center
NPCIL	Nuclear Power Corporation of India
ICS	industrial control systems
SCADA	Supervisory Control and Data Acquisition Systems
ENISA	European Union Agency for Cyber security

NTI	Nuclear Threat Initiative
DoD	Department of Defense
SIPR	Secure Internet Protocol Router
NIPR	Non-Secure Internet Protocol Router
US	United States
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DOE	Department of Energy
RF	radio frequency
IPSs	Intrusion prevent system
IDSs	Intrusion Deduction system
WAN	Wide Area Network
ATM	Asynchronous Transfer Mode
LAN	Local Area Network
TEMPEST	Telecommunications Electronics Material Protected from Emanating Spurious Transmissions

1
Introduction

The term ”air gap security” refers to a method of protecting sensitive computer systems and data by logically and physically separating them from the internet and other external networks. The purpose of air gap security is to implement a (’air gap’) that is either physically or electromagnetically created between the protected system and any external networks. This ”gap” makes it more difficult for unauthorized users to access the protected system or steal information from it.

Traditional security measures, such as security operation center (SOC) 24/7 security monitoring with the help of industry-standard tools such as Splunk, IBM QRader, ArcSight, and network security device Firewalls, intrusion prevention systems (IPSs), and intrusion detection systems (IDSs), can be compromised by sophisticated hackers who are capable of exploiting vulnerabilities in the network. This is what drives the need for air gap security. Air gap security is a method that may provide an extra layer of safety to a system by isolating it physically from any external network or device. This makes it far more difficult for an intruder to penetrate the system.

Air gap security is often implemented in circumstances when the protection of sensitive information is of the highest significance. This may be the case in military or government operations, vital infrastructure, or other high-security settings. Nevertheless, it may also be applied in other contexts that need for a high degree of security to be maintained, such as in research centers, data centers, and financial organizations.

Even though air gap protection may be successful in preventing security breaches, it can also present difficulties for authenticated persons who need to move data between computers or access online services. These difficulties can be unpleasant. In order to overcome these obstacles, businesses can use customized hardware or software to offer restricted Internet access for certain purposes or to support safe data transmission between air-gapped systems. Overall, air gap security is a crucial tool for safeguarding sensitive data and systems from cyberattacks, However, it requires substantial design and administration in order to establish the correct balance between the needs of security and those of operations. Having said that, we have offered the consolidated airgap security attack categories as well as it countermeasures in order to develop airgap security that is immaculate.

Motivation: The adoption of diverse security methods to safeguard sensitive systems and data is a result of the rising relevance of information security in contemporary society. Traditional security solutions, however, have flaws and restrictions that make them vulnerable to online attacks and data breaches. Air gap security has become a crucial strategy for safeguarding high-security situations in response to this dilemma.
Physically separating a system or network from other networks to create a "air gap" that restricts access is known as "air gap security." Due to its distinctive strategy for reducing security concerns, this technique has grown in prominence recently, especially in military and government situations. Air gap security does have certain drawbacks, however, and work is still being done to increase its efficiency and fix any flaws that could exist.
In this thesis, we focus on the issue of air gap security due to the crucial role it plays in safeguarding sensitive systems and data as well as the continuing interest and advancement in this field. Through this study, I want to add to the current discussion on air gap security and provide some new perspectives on how to manage potential security challenges and maybe increase its efficacy.

An inventive and tireless attacker will ultimately discover a means to penetrate the network, eavesdrop [12], and send sensitive information outwards as longer as the local area network is connected with the outside world (for instance, the Internet (www)). When we categorize as critical infrastructure, or the operation is vital for the organization they may alternative way to secure is build AIR-GAP system. The connection with the outside world will be restricted by the airgap. which will protect from the internet and safeguard data and other misalliance information from an adversarial attack, in light of the changing threats in information technology (IT) and operational technology (OT). Fig 1.1, illustrates the fundamental design of the air-gapped system. Many Organizations maintain airgap security while processing their sensitive data, for instance. The United States government or organization has two kinds of information classified and non-classified [13].

Classified Information: Certain information that must be kept confidential in order to prevent its public release to unauthorized parties in order to preserve the United States' national defense and security or its international relations in accordance with a federal legislation or an executive order. This word refers to Restricted Data, National Security Information, and Previously Restricted Data. The degree to which each might compromise the nation's security is reflected in the level of classification it receives either Classified information, or Confidential.

Non- classified: Defense departments and security companies utilize this private and encrypted network to communicate and exchange information that is not classified but is nevertheless sensitive in order to protect people's privacy.

The United States (US) Military, Department of Défense (**DoD**), financial administration, National security agency (**NSA**), and other government entities are employing airgap security, e.g., [14], Secure Internet Protocol Router/Non-Secure Internet Protocol Router (**SIPR/NIPR**) to exchange the restricted and non-classified information.

Cyber-attacks are not exceptional for the OT platforms, particularly the nuclear power plant implementing the air-gaped network was secure but not anymore. As an example, [15] The Davis-Besse nuclear power station in Ohio fell victim to the Microsoft SQL Slammer worm in the year 2003. The worm corrupted the facility's computer network server. This virus caused a spike in the amount of data traffic in the site's network, which resulted in the plant's Security Parameter Monitoring System and process level systems being unavailable for many hours. Despite this, none of these devices posed a threat to the nuclear power plant's ability to function normally and safely. According to the findings of the inquiry, a contractor installed a computer link to its corporate network that was not safeguarded, and it was via this connection that the worm was able to access the plant network.

In the other hand, the statement released by Nuclear Threat Initiative (NTI) stated nuclear assets and building security had improved dramatically during the last decade. As important breakthroughs in physical security have been adopted, a possibly much more difficult threat is jeopardizing these gains: the cyber threat. Traditional cyber defensive tactics at nuclear sites, such as firewalls, antivirus technologies, and air gap security, are no longer adequate to counter today's dynamic attacks [16] Page number (4).

Most notably, The European Union Agency for Cybersecurity (ENISA) does not have adequate guidelines for airgap networks for industry.

As show in Fig, 1.1 Air-gap system Architecture, the term ”air gap network” relates to the idea that there is a vacuum in the connection that exists between the computer and other networks. The computer is not directly linked to the network since there is a gap in the air; hence, it cannot be attacked via the network because it is not directly linked. Because there is no other means to access the computer system via the Air-Gapped network, the hacker will need to ”cross the air gap” in order to bypass the Air gap computer security system. This can only be accomplished by physically sitting down in front of the computer.

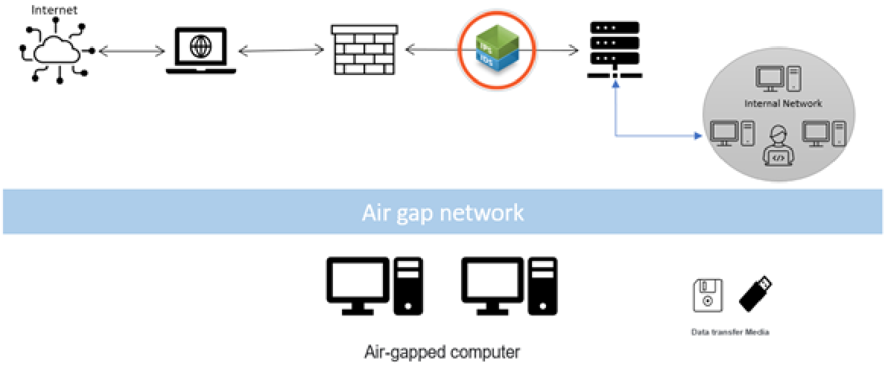


Figure 1.1: Air-gap system Architecture

Consider the following other instances of networks or systems that have the potential to be air-gapped:
1. Plants for producing nuclear electricity.
2. Computer networks and systems used by the military.
3. Control systems used in manufacturing, example Supervisory Control and Data Acquisition Systems (SCADA).
4. Information systems and network infrastructure operated by the government.
5. Systems and networks for the financial sector of the economy.

When the system requires an additional layer of protection, an air gap network or computer system will be established. Take, for instance, the payment networks that process transactions for shops, the military networks that are used to operate vital infrastructure, or the industrial control systems (ICS) that are used to operate such equipment. Consider the case of several types of infrastructure, such as power plants. The operation of the industrial systems of these power plants requires the use of computers. On the other hand, the internet cannot be accessed from these PCs. To put it another way, they have been ”air-gapped” with the goal of increasing the level of security. Because these systems are air gapped and not directly linked to the business network of the corporation, they are very effective at preventing intruders or hackers from gaining access to critical systems.

Data may only be transferred via external storage, like a USB drive or a firewire cable that connects two machines directly, when a computer or network is considered to be air-gapped for security. This indicates that the system is physically separated from the internet.

The finest aspect of the air-gapping technology is that it prevents almost all instances of virus attacks or hacking breaches caused by intruders while yet being a very inexpensive kind of technology. To deploy air gapping, all that is necessary is for you to unplug your computers from the rest of the world and then use the countermeasure that we have provided.

The preceding sections cover air gap security and how it is implemented; nevertheless, if we implement the airgap security outlined above, the adversarial will still be able to retrieve data from air-gapped machines. We presented some additional insight into various types of air-gap security threats, such as malware attacks, acoustic attacks, radio frequency attacks, and physical attacks. We broke down the potential dangers posed by each variety of cyberattack and outlined a variety of precautions that can be taken to avoid or lessen these dangers. These include the implementation of physical security controls, the implementation of routine software updates and patching, and the use of antivirus and other forms of security software. Also, we have emphasized the need of monitoring and safeguarding sound-sensitive equipment in addition to wireless communications as a means of preventing combination forms of assault, such as acoustic and malware attacks. I also brought attention to the possibility that radio frequency (RF) attacks may be used as a kind of physical attack, as well as the need of installing physical security measures to prevent against RF attacks as well as physical assaults. In general, I discussed the significance of installing a variety of technological and physical security measures in order to considerably cut down on the threat of air-gap security attacks and gave some valuable information into this topic

2
Real world Cyberattacks in Air-gap system

The air-gapped networks/system, which in theory offer the most robust strategy against cyber threats, have been shown to be vulnerable to intrusions in actual systems.

Firstly, an effective cyberattack against the Indian nuclear power plant Kudankulam was launched in 2019 and was successful the attack was confirmed by Nuclear Power Corporation of India (NPCIL) [17], the malware identified as Stuxnet was initially found in 2010 on a computer in Iran. Its intended purpose was to particularly damage the centrifuges at the Natanz nuclear power plant in Iran [18].

End of December 2020 SolarWinds attack,[19], the US cyber security community was discovered widespread security breach in both private and government networks. The event featured an evasive backdoor hidden within the firm's products, Consequently, it was the largest and most sophisticated attack the industry has ever witnessed. These methods enable attackers to deploy the desired virus into networks and surroundings that are extremely safeguarded. Even though the SolarWinds breach has been labeled as a cyber "attack" initial investigation suggests that its main objective was gathering intelligence rather than network disturbance, damage, or ruin.

The SolarWinds hack, which was developed with the intention of infecting countless networks in order to achieve prevalent access to sensitive interesting data and e-mails. It is known as a "supply-chain operation" because it utilized IT network operators to access the networks of its clients and used devious methods to avoid detection. As a result, it appears to lack the traits of focused, surgical espionage. Additionally, there does not appear to be any indication at this

time that it compromised restricted US networks.It is not as hazardous as a well-known Russian hack from 2008, which used an infected USB stick to access the AIR-GAP networks of the US Defense department. Ultimately, the SolarWinds attack appears to have been an intelligence ”fishing expedition” or recon operation launched on public networks, similar in goal to many previous state-sponsored cyberattacks, notably the 2013–2015 Chinese hack of the US Office of People Management.
The US intelligence community's top-secret data will be handled by the air-gapped Azure cloud area, according to a Microsoft announcement[20]

3
The Threat Model

The process of separating a computer or network from the world wide web or other unprotected connections in order to safeguard it from potential dangers originating from the outside world is referred to as air gap security. However, the protection provided by an air gap is not invulnerable and may be circumvented using a number of different attack techniques. The following is a list of some of the potential attack models for air gap security as shown in the Fig.3.1,

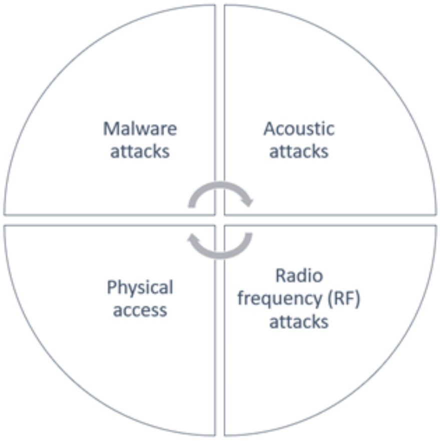


Figure 3.1: Air gap security threat model

Before we go into each individual threat model, we are going to look at the reasons why these arrows symbolize anything from malware attack to acoustic attacks.

An acoustic breach might be used to exploit weaknesses in a sound-sensitive device, such as a microphone or sensors, and obtain access to the air-gapped system. Once inside the machine, the attacker might install malware, such as a virus or trojan horse, which could then be used to launch other assaults or steal sensitive data.

This is frequently referred to as a ”badUSB” attack, in which a seemingly innocent USB device is really attacked with malware and may be used to corrupt a system. A badUSB attack might be conducted on a air-gapped computer by using a mic or other sound-sensitive equipment to transmit the information between the air-gapped system and an external source, such as a USB drive. [21]

To reduce the risk of a combined malware and acoustic attack on an air-gapped system, a variety of security measures must be implemented, such as physical security controls to prevent unauthorized access, regular software updates and patching to address known vulnerabilities, and the use of antivirus and other security software to detect and prevent malware attacks. Sound-sensitive equipment should also be securely secured and checked for evidence of manipulation or unexpected behavior.

Radio frequency (RF) attacks and physical attacks: may be connected in the sense that some types of RF attacks can be categorized as types of physical attacks. This suggests that there is a potential connection between the two types of intrusions. For instance, a radio frequency (RF) attack that makes use of a radio transmitter that is particularly powerful in order to affect or destroy electronic equipment or systems would be considered a physical attack since it makes use of a physical force in order to inflict harm.

When it comes to the security of an air-gapped computer, RF attacks and physical attacks are both viable options for breaching the system's defenses and gaining unauthorized access. For instance, an attacker may employ a radio frequency (RF) assault to collect wireless signals from a nearby device, such as a wireless keyboard or mouse, and exploit this to obtain access to the air-gapped system. This would allow the attacker to bypass the security measures. Instead, an adversary may conduct a physical assault to acquire physical access to the air-gapped machine. Once inside, they could then use this access to malicious program or carry out other kinds of attacks.

Physical Access

If a potential threat can get physical access to a computer or network that is protected by an air gap, they may be able to circumvent the security mechanisms that are in place. This may be accomplished by adding a USB drive or another external device that contains malware and has been compromised in some other way.

Radio frequency (RF) attacks

The use of radio waves to connect with a system that has air gaps is what is meant by a "RF attack." This may be accomplished by communicating with a neighboring air-gapped computer via the use of a device that sends out radio frequency (RF) signals, such as a mobile phone. This kind of attack is also classified as a "*covert channel*," which is a more technical term.

Acoustic attacks

Acoustic intrusions include the use of acoustic waves to interact with a system that has an air gap between it and the outside world. This may be accomplished by communicating with a nearby air-gapped system via the use of a device that sends out acoustic signals, such as a speaker or a microphone.

Malware attacks

Malware attacks against air-gapped systems require infecting an external device, such a Flash drive, that is linked to the air-gapped system with malicious code. After the device that has been infected with malware has been brought into contact with the air-gapped system, the virus may then be utilized to ex-filtrate data from the system.

There are a number of different forms of malicious software that may be used in air gap exploits, including the following:

Trojan horse: A Trojan virus is a kind of virus that is disguised as a legitimate software. Once it is placed on a computer, it may be exploited to grant an attacker the system's privilege. A Trojan horse is also known as a "*horse Trojan.*"

A worm is a self-replicating software that can move from one computer to another. Worms may also spread from network to network. After a worm has successfully infected a system that has hermetic security, it may be exploited to steal data from the system. A rootkit is a sort of malicious programs that is created with the intention of evading detection by security programs like as antivirus programs. Once an air-gapped machine has been infected with a rootkit, it is possible to exploit it to obtain access to the system and steal data from it.

Backdoor A backdoor is a concealed access point into a system that may be exploited to circumvent the security precautions that have been put in place. After an attacker has successfully placed a backdoor on a system that has been air-gapped, they are able to exploit it to steal data from the system.

When attempting to launch malware cyberattacks against air-gapped systems, one of the obstacles that must be overcome is the need of first introducing the virus into the system. Malware may be introduced into a system via a number of methods, including the use of virus is transmitted USB drives that are left in public locations or the use of social engineering methods to persuade a person to bring an infected device into an otherwise secure environment.

It is essential to make use of a variety of security measures in order to safeguard air-gapped computers against malware assaults. These measures include restricting access to USB devices, installing antivirus software, and performing routine security audits in order to identify any possible dangers.

Social engineering

Attacks involving social engineering against systems protected by air gaps consist on influencing humans in order to obtain access to the computer. Convincing someone to give access to the air-gapped computer may be accomplished via the use of a variety of strategies, such as phishing emails, phone calls, or even physical infiltration. These methods are all viable options. Once an attacker has gained access to a system, they can then use different attack models to exfiltrate data from the system. These attack models may include inserting an infected USB drive or connecting with the system via the use of electromagnetic radiation.

Here are a few concrete examples of social engineering approaches for breaching air-gapped systems.

Intrusion by physical means

An adversary might physically break into a building that encloses an air-gapped system and enter the building under the guise of an employee, a vendor, or a maintenance professional. Following this, the attacker may be successful in gaining access to the system via the use of a number of strategies, such as stealing a security badge or using a false ID. To avoid cyberattacks on air-gapped networks, educate workers to notice and report unusual behaviour, restrict physical access to buildings and devices, and implement strong authentication methods and access controls to prevent unauthorized access. It is also critical to perform frequent security audits to discover and remedy any possible security vulnerability.

Attacker motivation

Targeting air gap security systems may be motivated by a variety of factors for attackers, including the following:

Espionage: Air-gapped computers may be the target of cyberattacks sponsored by nation-states or business competitors that are looking to acquire sensitive information, such as intellectual property or trade secrets, that might provide them with an edge in the marketplace.

Cyberterrorism: Adversaries may utilize air-gapped computers as a target to conduct assaults on vital infrastructure, such as electric grids or rail networks, which could have significant repercussions for public safety if they are successful.

These are only some of the various reasons why attackers could target air gap security systems; there are likely many more. It is essential to have a solid understanding of the various types of dangers that may present themselves in air-gapped environments, as well as to take a holistic approach to security that incorporates logical and physical access controls, network segmentation, consistent security updates and backups, as well as employee training and security awareness.

4

Side channel attack Vs Airgap security

Side channel attacks and air gap security attacks are two separate forms of attacks that can be used to break security protocols; however, both have the capability to expose sensitive data or critical systems. Here's a breakdown of each.

Side channel attack: Side-channel attacks are a kind of attack used in cryptography. These attacks take use of information that is leaked from the physical implementation of a cryptographic system, rather than exploiting flaws in the mathematical techniques that are used to create the system. In other words, instead of directly attacking the encryption algorithm, a side-channel attack makes use of vulnerabilities in the physical implementation of the software, such as power consumption, electromagnetic waves, or timing information, in order to gain unauthorized access to sensitive information. This is accomplished rather than attacking the encryption algorithm directly.

Side-channel attacks may take many different forms; however, the following are some of the more prominent examples:

Power analysis: Analyzing the amount of power that is being consumed by a device while it is doing cryptographic operations in order to gather information about the secret key that is being utilized is one sort of side-channel attack. An adversary may occasionally extrapolate information about the activities being done by the device by watching the power utilized by the device over the course of time. The adversary can then use this knowledge to recover the key.

Electromagnetic analysis: Analysing the electromagnetic radiation that is released by a device while it is doing cryptographic operations is one sort of side-channel attack. This type of attack

may be used to infer information about the secret key that is being utilized. An adversary might occasionally extrapolate information about the operations that are being conducted by the device by watching the emission that is being emitted by the machine. They can then leverage this knowledge to retrieve the token.
Acoustic analysis: This sort of side-channel attack is examining the noise generated by a machine throughout cryptographic operations in order to gather details about the secret key being used. An adversary may occasionally extrapolate information about the processes being done and exploit this knowledge to acquire the key by capturing the noise generated by the machine.

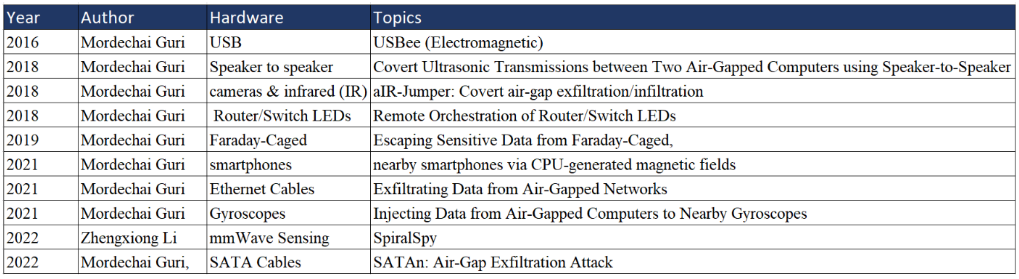
These are only a few examples of the many various kinds of side-channel attacks that may be used to breach the security of cryptographic systems. There are many more such attacks. It is essential for businesses that depend on encryption to be aware of these dangers and to take preventative measures against them.

Air Gap security (AG): Air gap security attacks are a particular approach that attempts to defeat the physical isolation mechanisms that isolate air-gapped systems from the outside world. These assaults often use a variety of ways to undermine the security of the air-gapped system and obtain access to sensitive information or vital systems, such as USB-based attacks, radio frequency (RF) attacks, malware-based attacks, and insider threats. Air gap security attacks are often used against high-security settings such as defense, government, or other situations where data security is a primary consideration. We have celebrated in the subsequent section the different types of cyberattacks and attack strategies.

Discussion of covert channels

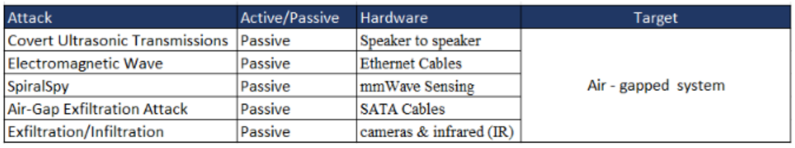
This section covers the most common air gap attacks currently in use. Overall, our goal is to highlight down sides of current responses and to encourage further research to develop more general defenses against air gap attacks.

Table 2 provides an overview of the attack categories, as well as the different types of hardware that have been used for the various forms of air gap security attacks. The attack pattern, as well as the types of techniques and the targeted system, are detailed out and in Table 3.



Year	Author	Hardware	Topics
2016	Mordechai Guri	USB	USBee (Electromagnetic)
2018	Mordechai Guri	Speaker to speaker	Covert Ultrasonic Transmissions between Two Air-Gapped Computers using Speaker-to-Speaker
2018	Mordechai Guri	cameras & infrared (IR)	aIR-Jumper: Covert air-gap exfiltration/infiltration
2018	Mordechai Guri	Router/Switch LEDs	Remote Orchestration of Router/Switch LEDs
2019	Mordechai Guri	Faraday-Caged	Escaping Sensitive Data from Faraday-Caged,
2021	Mordechai Guri	smartphones	nearby smartphones via CPU-generated magnetic fields
2021	Mordechai Guri	Ethernet Cables	Exfiltrating Data from Air-Gapped Networks
2021	Mordechai Guri	Gyroscopes	Injecting Data from Air-Gapped Computers to Nearby Gyroscopes
2022	Zhengxiong Li	mmWave Sensing	SpiralSpy
2022	Mordechai Guri,	SATA Cables	SATAn: Air-Gap Exfiltration Attack

Figure 4.1: TABLE. 2, SUMMARY OF SURVEYED ATTACKS



Attack	Active/Passive	Hardware	Target
Covert Ultrasonic Transmissions	Passive	Speaker to speaker	Air - gapped system
Electromagnetic Wave	Passive	Ethernet Cables	
SpiralSpy	Passive	mmWave Sensing	
Air-Gap Exfiltration Attack	Passive	SATA Cables	
Exfiltration/Infiltration	Passive	cameras & infrared (IR)	

Figure 4.2: TABLE. 3, SUMMARY OF ATTACKSTHE TARGETED SYSTEM

5 Air-Gap attack classification

In this section, we introduce the many categories of air gap security Covert channels, as well as the technological underpinnings of each attack and its tactics. In certain situations, we also describe feasible countermeasures.

5.1 Electromagnetic cover channel

Electromagnetic radiation: As we are aware, Personal computers, laptops, and mobile devices will release the inevitable electromagnetic wave or radiation, also known as compromising emanations or tempest radiation [22], but those radiations will carry the information that is processed in the system, Electromagnetic radiation travels across space as waves of electromagnetic energy. The frequency of these waves, which is defined in Hertz (Hz), and their amplitude, which is defined in decibel-milliwatts, are the two primary characteristics of these waves (dBm). When charged particles are propelled, electromagnetic frequencies are produced as a byproduct of the acceleration. In most cases, the presence of a change in currency in a metal wire results in the production of electromagnetic radiation.

Maxwell's equations and the Lorentz force law both explain the manner in which charges and currents react with the magnetic wave. EMR may be produced by a variety of electronic components, including computer displays, video cards, and connections. The frequency and amplitude are both determined by the current and voltage that are produced internally by the device [23]. Previous research has concentrated on harnessing EMR for eavesdropping uses and exploiting the deliberate and accidental EMR of various computer components in order to establish covert channels. In addition, EMR has been employed for the goal of creating covert channels. So, it certainly not only interferes with radio receivers also carry vital information. compromising emanations. The main piece of hardware used in this attack is Ethernet cable, which is commonly used for establishing a connection with other systems in a network. Before investigating the attack, it is important to understand how Ethernet cables are constructed because this will help us understand it better in upcoming sessions.

LANTENNA- is an innovative kind of electromagnetic covert channel that makes use of LAN networking connections in order to steal data via wireless through air-gapped networks. A piece of malicious software that is run on a hacked workstation or server has the potential to control the electromagnetic waves that are emitted from an Ethernet cable Fig 5.1, therefore using it as a broadcasting antenna. The author research demonstrates that any kind of binary data may be modulated on top of the radio waves that are created. The author also demonstrate that an ordinary software-defined radio (SDR) transmitter located in the location is able to decode the information and subsequently send it to the offender through the internet [1].

It is possible that the attacker will collect data from the affected systems as part of the exfiltration step. The data that has been stolen might include things like papers, records, access credentials, encryption techniques, and many other things.

Data transmission: After the data has been acquired, the virus will secretly transmit it utilizing the backdoor. In the case of LANTENNA, the data is modulated before being sent out in a wireless manner using the radio waves that are emitted by the Ethernet connections. [1]

Data reception: The covert signal is able to be picked up by a radio antenna in the nearby, where it is then decoded and forwarded to a potential attacker. It is possible for a malicious insider to carry the receiving gear or for it to be disguised in the location.

Ethernet cable classifications:

As depicted in *Fig. 5.2* below, multiple wires are twisted into four pairs to create an Ethernet cable. Ethernet cables can be categorized into the following categories:

Cat 5 & cat 5e: These cables allow 10 to 100 Mbps and the cat 5e allow up to 1000Mbps these network cables mostly employed in home network. [2]

Cat 6 & Cat 6a: This twisted pair cable was developed to handle situations with 10 Gigabit Ethernet and give networks more efficiency.The transmission speeds of Cat.6 and Cat.6a patched cables differ significantly. A Cat.6 network connection can already transmit data at a rate of 1000 Mbit/s (1 Gigabit/s), but a Cat.6a cable can do much more quickly.

Cat 7a: It's possible that category 7a cables were first developed as a future-proof measure to finish the anticipated broad adoption of the 40 Gbps Ethernet benchmark. However, a revised

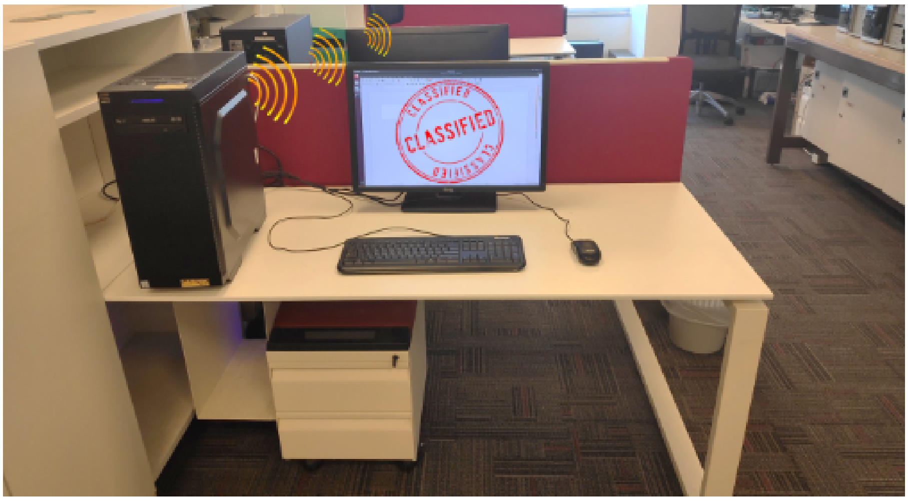


Figure 5.1: LANTENNA attack model [1]

authorization in 2016 meant that this responsibility was transferred to Cat8 cables designed for 2000 MHz. As a outcome, few computers officially support the cable Cat7a as a independent revision.

we have included the below table with all important information so that you may have a thorough understanding of all network cable kinds and capacities. Comparison of Cat cable in Table 5.3 [3]

The researcher Mordechai experiment proves that ether net cables emitting the electromagnetic waves. They employed spectrogram Fig. 5.4 and 5.5, to capture the waves and displaying the sequence values as 10101010..., this experiment was performed using air-gapped computer was transmitting the data using the network cable. the single was captured 200 cm away from Air-gap system.

Countermeasure

Countermeasure 1: Our study shows that fiber optics cable project more data security They are the best option for transmitting data since they are invulnerable to electromagnetic interferences. Since they use light pulses in glass threads to transfer signals, fiber optic cables are non-metallic. They can function without even being affected by electromagnetic interference and

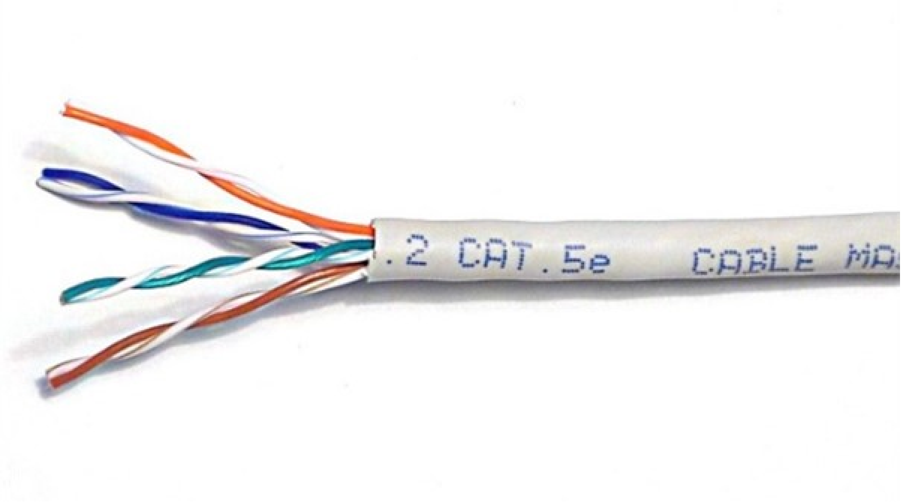


Figure 5.2: Ethernet cable I [2]

radio frequency interference (EMI/RFI). In other words, environmental and electrical noise does not impact the integrity of communications [**?**]

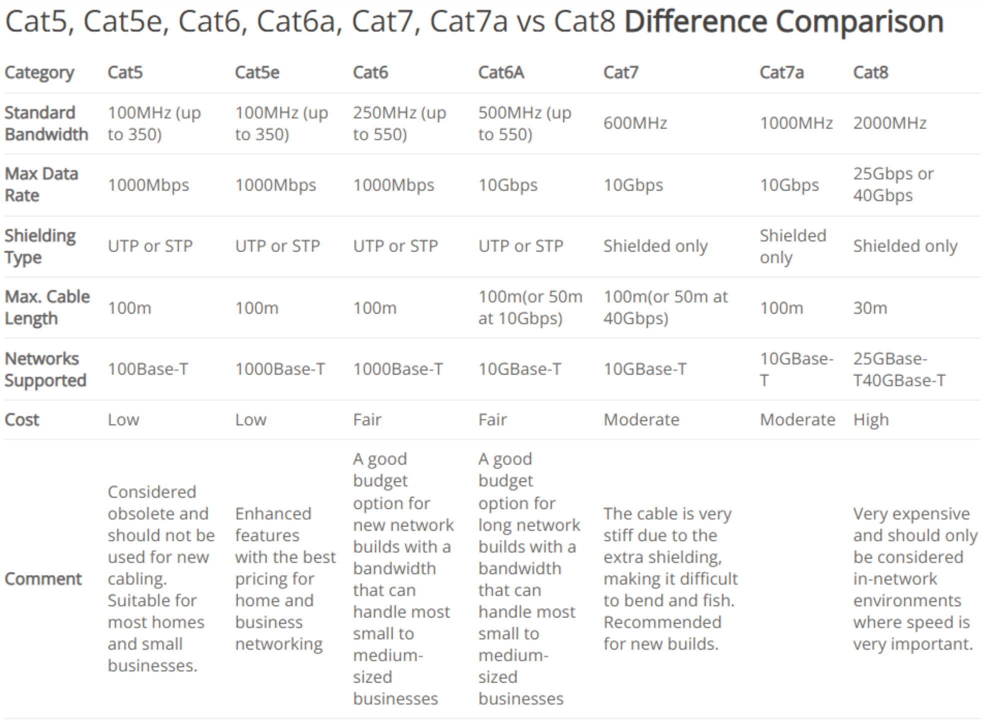
Countermeasure 2: Ethernet cable with Fig. 5.2, displays the shielding capacity highly recommended to avoid wide spread of the electromagnetic waves/radio frequency interference (EMI/RFI) which likely carry sensitive data into the space. To avoid this, we should utilize shielded ethernet cable. as shown in the blow figure 5.6.

Countermeasure 3: To safeguard air-gapped network environments against electromagnetic interference (EMI) through conducted emission. For example, EMI cyberattacks could be possible if the same power line that supplies an internet-connected computer also powers an air-gap system. The power source can be an indication of compromise (IOC).

Countermeasure 4: The network cable we use should be single grounded as shown in the below Fig. 7 in order block the electromagnetic waves to penetrate the network cable. [5]

5.2 Ultrasonic Speaker-to-Speaker covert channel

Research dissertation the researchers have demonstrated that more than two we show how air gapped computer nodes in the same location inculcated with electronic gadgets can stealthily swap information through ultrasonic moves [6]. The proposed process by the authors is related with the potential of a viral to develop precise frequencies scrap attribute in magnitude to backward the associated audio gadgets from product inclinations into stimulus devices - unremarkable interpreting them from input devices. The team has promised to render the optimal



Cat5, Cat5e, Cat6, Cat6a, Cat7, Cat7a vs Cat8 **Difference Comparison**

Category	Cat5	Cat5e	Cat6	Cat6A	Cat7	Cat7a	Cat8
Standard Bandwidth	100MHz (up to 350)	100MHz (up to 350)	250MHz (up to 550)	500MHz (up to 550)	600MHz	1000MHz	2000MHz
Max Data Rate	1000Mbps	1000Mbps	1000Mbps	10Gbps	10Gbps	10Gbps	25Gbps or 40Gbps
Shielding Type	UTP or STP	UTP or STP	UTP or STP	UTP or STP	Shielded only	Shielded only	Shielded only
Max. Cable Length	100m	100m	100m	100m(or 50m at 10Gbps)	100m(or 50m at 40Gbps)	100m	30m
Networks Supported	100Base-T	1000Base-T	1000Base-T	10GBase-T	10GBase-T	10GBase-T	25GBase-T40GBase-T
Cost	Low	Low	Fair	Fair	Moderate	Moderate	High
Comment	Considered obsolete and should not be used for new cabling. Suitable for most homes and small businesses.	Enhanced features with the best pricing for home and business networking	A good budget option for new network builds with a bandwidth that can handle most small to medium-sized businesses	A good budget option for long network builds with a bandwidth that can handle most small to medium-sized businesses	The cable is very stiff due to the extra shielding, making it difficult to bend and fish. Recommended for new builds.		Very expensive and should only be considered in-network environments where speed is very important.

Figure 5.3: CAT COMPARISON [3]

results of supersonic scope (18kHz to 24kHz). They too assessed the communicating transmission with diverse gadgets with the measuring parameters as distances and transmission speeds. They finally proved that speaker-to-output devices interlinked connection can be utilized to secretly broadcast information among two or more air-gapped nodes located at utmost of nine meters distance

Approach and Technical Background

The research contribution of this article is listed as follows

1. **Output Device -to-speaker communication** Attack model of connecting the airgap in between computer nodes. Apart from speakers the other electronic gadget's reaction to the ultrasonic series is also considered. The team also evaluated the acoustic reaction of passive gadgets to the optimal supersonic scope when changed into microphones. The computer nodes affected with viral has cardinal equipped components namely retasking by Jack, Synchronization and Transmission and reception. The communication may be unidirectional or bidirectional in the attack scenario. The workflow of malware is given below .

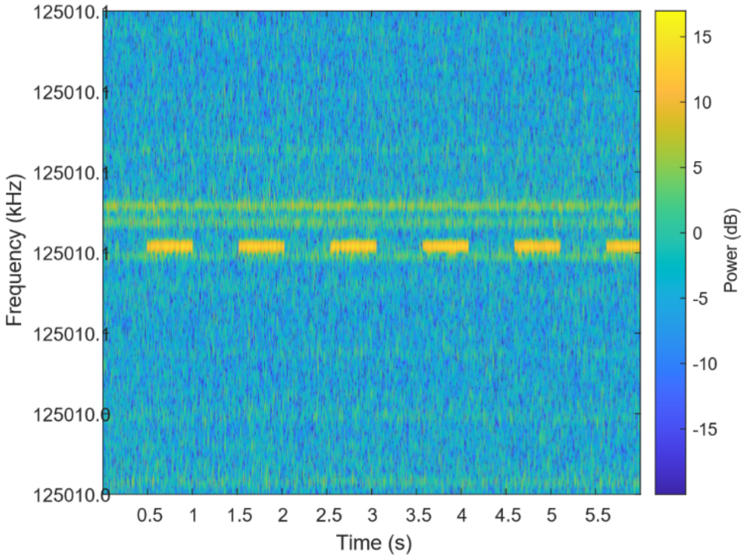


Figure 5.4: Spectrogram in Frequency waves [1]

The designing and execution of communication includes. A. Protocol Stack - Light, stripped-down speaker rules stack for the execution of the channel.
B. Near-Ultrasonic Range - frequency range of 18kHz to 24kHz standard for data transformation.
C. binary Set up – preamble header of six alternating bits the recipient to notice the commencement of the communication of each packet. Parity is the 32 bits of rough information which constitutes the real package. Eexception is detected if recipient ccomputes the CRC for the receiver payload, and if it varies from the receiver CRC.
D. Broadcast Message – Based on ID telecast, the node retasks its output device to a microphone. It remains for detection recognition note receive from further system. If a recognition notes aacknowledged, it stops propagating the discovery note. The acknowledgement note is of with the following quotes DISCOVERY ACQUIRE and RELEASE messages.

2. The novel approach of threads in speakers-to-headphones communication channel and vice-versa is evaluated.
3. Transmission protocol. In channel strategy, the two or more computer nodes must mutually

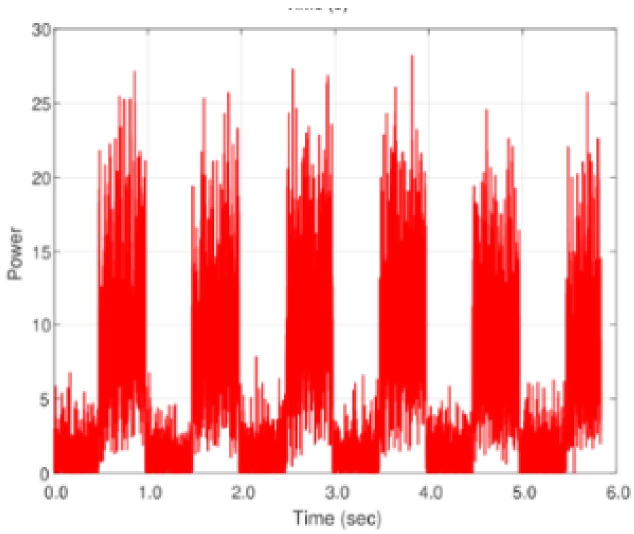


Figure 5.5: Spectrogram power [1]

transform the input devices roles to microphones role and in reverse during the communication.
The method that is adopted by other studies on the ultrasonic backdoor is to make use of the current implementation of protocol stacks that were first built for acoustic (communications that do not include ultrasonic waves)

The human ear is only sensitive to sound frequencies up to 20 kilohertz. When doing research on hidden channels, it is appropriate to consider frequencies over 18 kHz to be virtually barely audible to humans [24]. In 2016, a group of experts carried out an in-depth study on the growing danger posed by ultrasonic cross-device tracking (uXDT). They discovered that ultrasonic beacons (uBeacons) operating in the 18kHz to 20kHz frequency range are included into websites as well as television commercials [25]. After then, the beacons are picked up by applications that are loaded on cellphones in the immediate area. As a consequence of this, during the course of this article, we will refer to the frequency range of 18 kHz to 24 kHz as the permissible one for the covert communication as shown in the Figure 5.9.

Data Modulation - two different output frequencies f’0’ and f’1’in the range of 18kHz to 24kHz denote binary symbols Zero ’0’ and one ’1.’

4. Reversible speakers. Sound is produced by speakers by moving a diaphragm under the

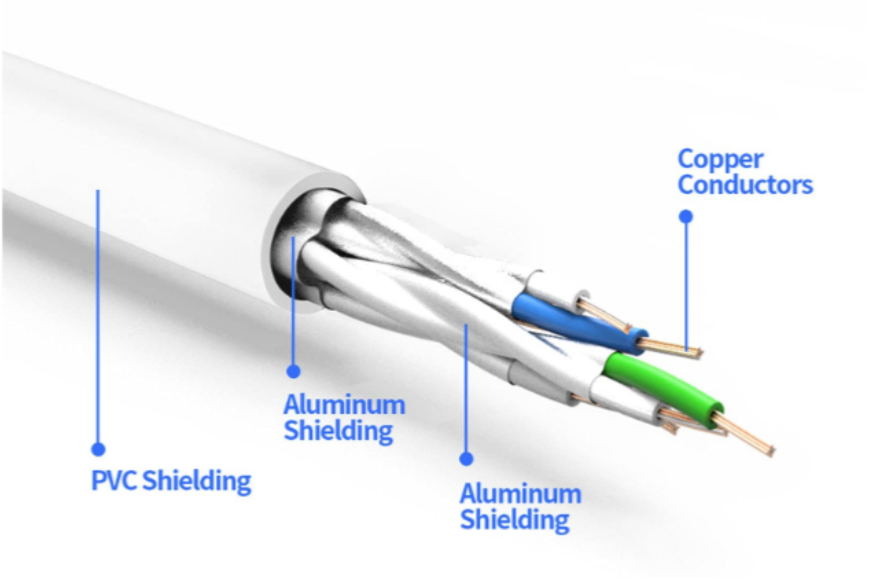


Figure 5.6: Shield Ethernet cable [4]

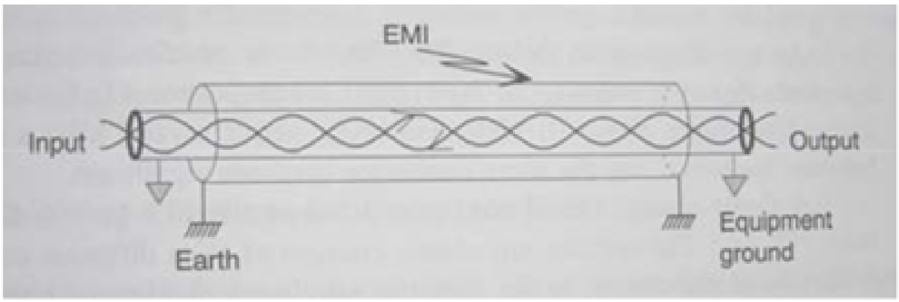


Figure 5.7: Cable Shielding to Minimize Electromagnetic Interference [5]

influence of a changing magnetic field that is influenced by electric impulses. In the same way, in input gadgets, a little mechanical device navigates through a magnetic field with protocols accordant to an air pressure in speaker. To be practical, outputs were not considered to execute as mike like input devices, and the registered signs will be of low value speakers utilize the varying magnetic field stimulated by electric signals to progress a membrane in sort to generate audio signs.

5. Jack Retasking. Chipsets in current internalboards and sound cards embrace a choice to modify the purpose of an output port at the firmware intensity integrated into PC motherboards. The associated output device can purpose as two registering microphones, thereby

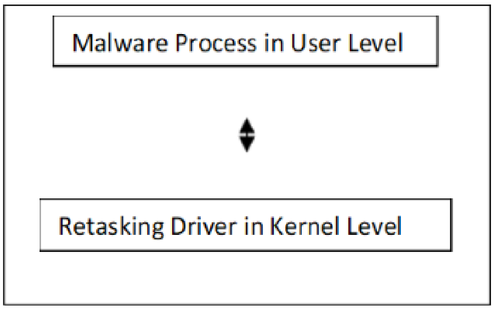

Malware Process in User Level
Retasking Driver in Kernel Level

Figure 5.8: The workflow of malware [6]

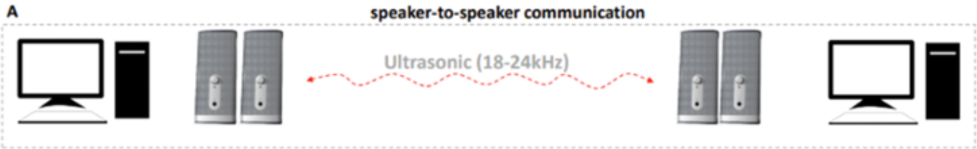


Figure 5.9: Speaker to speaker Protocol stack Cover channels[6]

representation the node a registering device - even while the node does not have a linked mike.

Test bed

As shown in the Figure 5.11, Channel capacity an evaluate parameter of the superior boundary on velocity at which data can conveyed over a channel. The proposed setup with channel capacity space difference of one, four and eight meters between the source and the destination. The passive loudspeakers considered as receivers for testing are Logitech Z523, Logitech Z213, and Philips SPA5300. The audio systems were linked to regrettable output output squad on an Optiplex 9020 desktop PC. The range up pointer was executed during a Logitech Z100 speaker linked to a Gigabyte GA-H97M-D3H server, (Intel Core i7-4790) operating Ubuntu OS 16.04.1 core 4.4.0. The indication is examined in consecutive Gaussian operating systems of 200 ms with 25 % partly cover on schedule. Assuming a random resolution of 100Hz for each and every band, ensuing in 250 examined ratios. The SNR is expected on every cardinal band, as the split of the acknowledged sign and calculated noise in this band.

Test results

A common explanation for every type of input and output gadgets is to employ the electronic equipment on-board, incorporating it surrounded by the micro chip of audio system. Diverse

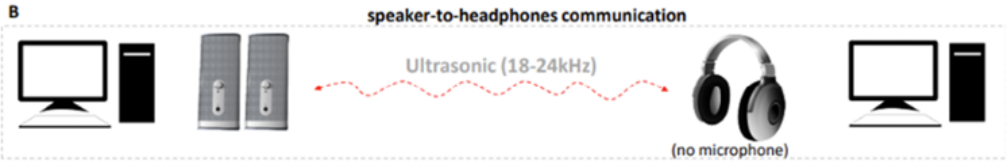


Figure 5.10: Speaker to headphone Cover channels[6]

concept is to facade supersonic broadcasts incoming assured region using supersonic jammers. Such plans produce supersonic setting disturbance intended at inquisitive with the communication signs. It is probably to display the audio for peculiarly up to the level of energy, in command to identify secret transactions in domain. This research article focuses on the supersonic frequency series scope greater than 18kHz is to be examine incessantly and scrutinized. Nevertheless, if the firmware instrumentation scrutinizing the supersonic range is remote from the source this proposed model is not impressive.

Countermeasures

As illustrated in Figure 5.12, there are three different categories that may be used to categorize countermeasures. These categories include software-based countermeasures, hardware-based countermeasures, and generic countermeasures.

Hardware-based countermeasures

It is standard practice to prohibit the use of any form of loudspeaker in high security facilities, regardless of whether the loudspeaker is either active or passive, in order to establish what is known as an ”audio-gap” separation with both computers [26]. The utilization of microphones is prohibited under the less stringent standards; however, the use of unidirectional loudspeakers is permitted. The NSTISSAM TEMPEST/2-95, RED/BLACK handbook recommended the implementation of such a rule [27]. This guide's section on protective measures includes the following recommendation: ”Amplifiers should be considered for speakers in higher classified locations in order to offer reverse isolation in order to prevent audio from being heard in lower classified areas.” As a result, certain TEMPEST-certified speakers come packaged with amplifiers and a fiber input that only goes in one direction. [27]

On the other hand, [28] the majority of contemporary earphones are not powered and are constructed without amplifiers, meaning that the above regulations and preventative countermeasures do not apply to these headphones. The implementation of the amplifiers on-board, where it is then integrated into the audio chip set, is a generic approach that can be used to all

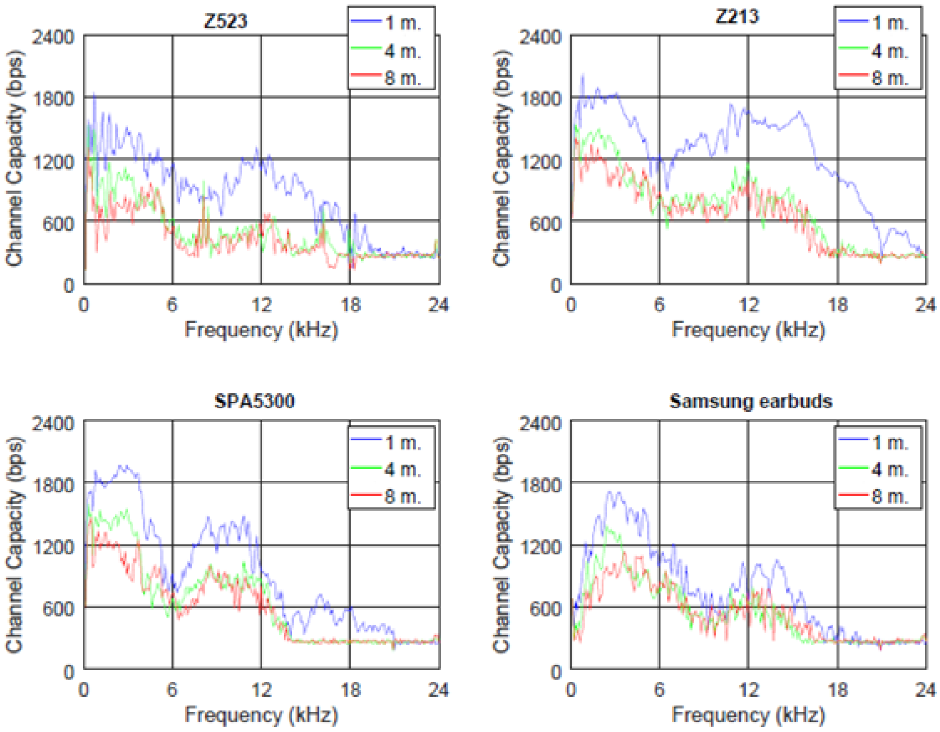


Figure 5.11: Channel Capacity [6]

different types of speakers headphones. Utilizing ultrasonic jammers device is another strategy, which may be used to conceal ultrasonic emissions in a particular region. These gadgets produce ultrasonic ambient noise with the intention of disrupting covert communication transmissions. [26] It is important to keep in mind that it is not an easy task to implement this kind of solution on a large scale since the jamming range is restricted to a radius ranging from a few meters up to a single room.

Software-Based countermeasures

One of the software defences is turning off the audio equipment entirely inside the UEFI and the BIOS. Because of this, malicious software may be unable to get access to the audio codec on the operating system level. On the other hand, since this configuration does not make use of the audio hardware (for example, to play audio), it is possible that it is not applicable in all circumstances. Installing an HD audio software that inhibits jack retasking or imposes a tight policy on jack retasking is an additional choice you have. Anti-malware and IDS may use a monitoring driver to offer broad software-level security. This driver can identify unwanted

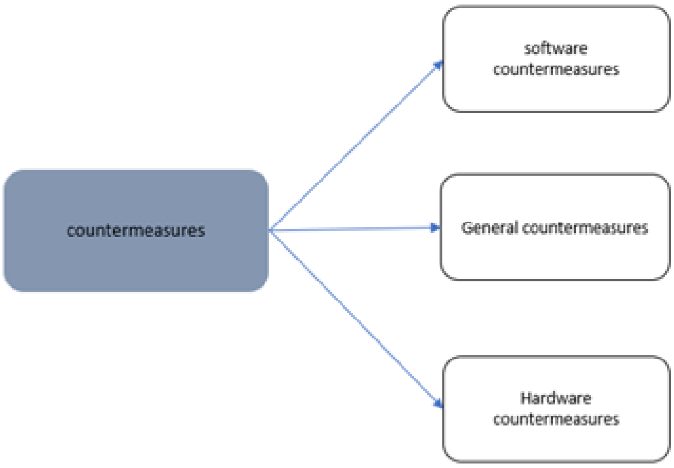


Figure 5.12: Types of countermeasures

speaker-to-mic retasking activities and prohibit them.
The second strategy that is suggested in [29] is to use a low-pass or band pass filter in order to remove the barely audible wavelengths that lie between 18 kHz and above on the frequency spectrum. Recent developments have resulted in the implementation of a software-based ultrasonic firewall for the Google Chrome web browser [30]. This firewall is known as *SilverDog*. This open-source project tries to restrict cross-device tracking via ultrasonic beacons, which is currently being done by companies *(uBeacons)*
The results of this paper experiment are as follows. The researcher's contribution in this study is concentrated on an attacker's capability to change a node's associated talker from an output device to a sign device. It quietly switches from being a speaker to a microphone. They also proved that though the inverted output gadgets are not intended to work as mike, they are quite responsive to oftenness scope of 18kHz to 24kHz sound range. Communications in series are almost infrasonic to fewest listeners, and therefore this model is analyzed covert. The authors finally concluded that via loudspeakers, Information may transmit through an air gap at efficient bit rates of 10 to 166 bits/sec from a distance of 8 meters

5.3 USBee: Air-Gap Covert-Channel

In the modern world, Fig, 5.13, researchers have confirmed how hackers can use external ports like USB to ex-filtrate the secured information from air-gaped computers through RF transmitters [7]. Such technique needs a instrumentation alteration of the USB port embedded with

RF transmitter.
USBee as seen in the Figure 5.13. A conventional, unmodified USB device (flash drive) (A) is transmitting data to a nearest receiver (B) via electromagnetic waves produced by its data bus. This transmission is taking place across an air gap.

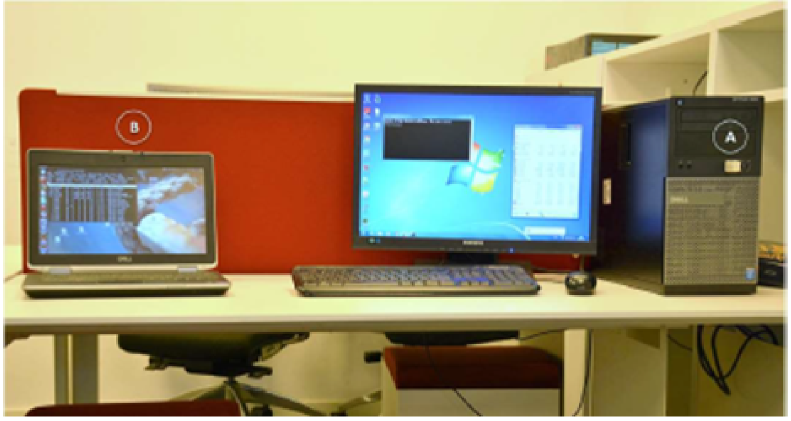


Figure 5.13: USBee [7]

The authors present the ‘USBee,’ firmware that can exploit an original USB port linked to a node as a RF transmitter. They also proved that software can deliberately produce dominated electromagnetic release from the information of a USB port. They too proved that the released RF signals can be automated with absolute multiple data and implemented a protocol of USBee with signal generation and modulation. Using GNU Radio modulator and demodulator is evaluated. The assessment demonstrates that USBee is utilized for transmittal binary information to nearby recipient at a bandwidth range of 20 to 80 BPS.

Technical background

USB port facilitates data transmission betwixt computers and peripheral devices. It is a combination of 4 shielded wires namely VBUS (+5v power), GND (for grounding), D+/D-(transmit differential data signals) with encoding scheme ’0’ for positive transition and ’1’ for no conversion of the sign level. For the proposed method the author utilizes USB 2.0 and USB 3.0 at the transferal charge of 480 M bits/s for the communication. In USB NRZI encryption, information is depicted in position of JK Flip Flop with ’1’ bit representation for D+ voltage level and ’0’ bit representation for D- voltage level. Bit padding is a system utilized to attain clock synchronization by insetting a ’0’ bit later all six successive ’1’ bits. Ssequence of 7 ’1’ bits is recognized as fault and assists to keep the clocks synchronal. The negative feedback is time consuming.

Electromagnetic emission (EMR) is a category of force released by convinced magnetic force procedure. It passes through gap in the descriptor of magnetic force waves with two primary attributes: (1) frequency (Hz) and (2) amplitude(dBm). Electromagnetic motions are produced whenever stimulating elements are accelerated. Charge emission in electromagnetic field was represented by Maxwell's formula and the Lorentz force law. The oftenness and magnitude depend on the interior actual and potential of the electronic gadgets which emits EMR. In USBee, information is operated in the USB's D+ and D- data cables to produce EMR.

Transmission

USB port scenario broadcast data in unidirectional. OUT key point is for carrying information from the host to the peripheral and IN key point is to act vice versa. It is found that the broadcast of a series of '0' bits to a USB gadget produces a noticeable production in the range between 240M*h*z - 480 M*h*z. This is comprehensible granted USB 2.0's timer velocity and the reality that '0' bits produce quick electric potential transform on each timer cycle as per the USB NRZI execution. Modulated data can then be decoded by RF receiver. The basic working model is based on the magnetic force sign at a needed frequency. This purpose obtains an indicator to a temp storage buffer in memory (buf), the range of buffer (size), and freq significance (freq) which is the objective secretion freq. in multiples of 100K*h*z. The purpose fills the transitory storage with a unique model which, as inherited over the information bus (D+ and D-), generates a magnetic force secretion at frequency f. Subsequently initializing buffet attributes x and y, set the variant t as double the percent among preferred release frequency and trial freq. 480Mbits/s. Bit representation is used to correspond the bearer motion and desired frequency respectively. For representation if the output series is of 24 bits, then it is stored as product frame will be a repetition form of 12 ones preceded by 12 zeros (1111111111000000000000...). Each 32 bits are added to the fender when printed to a file on a detachable storage device, will produce a signal at the preferred frequency. The buffer size (size) determines the duration of the signal. A buffer size of 6K, which makes a signal that, is strapping enough to be clearly noticed by the recipient. The happening of the bearer sign is switched between two values f1 and f2, consequent to a binary 0 or 1. According to the USB 2.0 stipulation, generalizing EMI by replication only a some oftenness isn't acceptable. It is probable to execute concise scrutinizing at the plan phase using numerous antennas that wrap dissimilar incidence ranges and get into description some flat and perpendicular points.

Countermeasures

The terms ”administrative,” ”software,” and ”physical” all refer to different types of countermeasures as show in the Fig.5.14

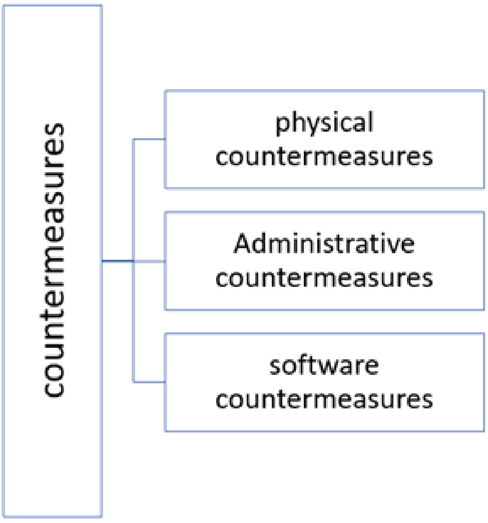


Figure 5.14: countermeasures

Administrative Countermeasures –The zones [31] technique may be employed in administrative countermeasures Fig.15, if necessary. In this method, sensitive computers are stored in regions that are off-limits to electrical equipment and are thus unable to be used. [31] [27] discusses the zones technique, often referred as the ”blackred separation” concept, as a method for mitigating several sorts of acoustical, electromagnetic, and visual dangers. On the other hand, it may not always be possible to adhere to a policy that mandates keeping RF receivers physically isolated from computers.

Software based Countermeasures – The software-based strategy entails making use of tools like anti-virus software and intrusion monitoring tools in order to identify potentially harmful behaviors. In order to detect USBee, it is possible to monitor the I/O activity of a process in order to recognize certain behaviors (for instance, behaviors that indicate frequent creation and writes to temporary files). These kind of behavioral detection systems have the potential to produce a significant number of false positives, which is mostly attributable to the nature of USBee’s activities (writing 6K of data to temporary files).
Physical Countermeasures Protecting against electromagnetic radiation (EMR) emitted by

USB components is an essential part of achieving physical isolation [32]. In most cases, electromagnetic shielding shielding are employed. However, there is another way that focuses on reducing the quantity of emissions that are produced. When testing for USB, the product must be scanned across frequencies as high as 1 GHz to detect whether or not there are any signal amplitudes that fall outside of the standard. The standards for USB 2.0 state that it is not permissible to infer EMI by scanning just a select number of frequencies. It is feasible to carry out some preliminary testing during the design phase using a number of antennas that span a variety of frequency bands and account for both horizontal and vertical orientations.
In this research report authors present USBee, a novel method that plays practically some USB connection into a short RF sender. The portfolio uses the data coach in a USB port connector to produce electromagnetic emission of a precise frequency. Code on a contaminated computer node can transform data and broadcast it to a close recipient, thus creating a type of communication transmission. Different prior covert channels founded on USB port; the proposed playing doesn't need firmware of the USB's component. The author presented the sign generation algorithm. This research article finally concludes that USBee can be used to efficiently convey information to a nearby recipient at a bandwidth of 80 bps.

5.4 SATA Cables covert channels

The researcher initiates a novel category of blast on separated, air-gapped server[8]. Though air-gap computer nodes have no radio communication, Fig. 5.15 [8] the authors demonstrated that afflictions can engage the SATA wire as a remote antenna to convey radio signals at the frequency range of 6 GHz. The Serial Advanced Technology Attachment (SATA) is a connector mediator to interconnect all major storage devices. The authors promised that the data transfer is highly secured in distant access level from internal a Virtual Machine (VM). [8]

Attack Model -

The major steps are the initial incursion, establishing foothold, lateral happening, data accumulation and extraction. Initial incursion is the initial layer where the malware software is installed in the target network. The information is a collection of data, images, and videos. The attacker may encrypt or hide the data at this phase. The malware places hosts in the network that holds active SATA middleware. The malware also uses a dedicated shellcode to reserve system action to produce signals from the SATA cables. The composed information is adapted, presented, and conveyed through covert channel. The recipient checks the 6 GHz spectrum for a possible communication, demodulates the information, codification it, and propels it to the assaulter.

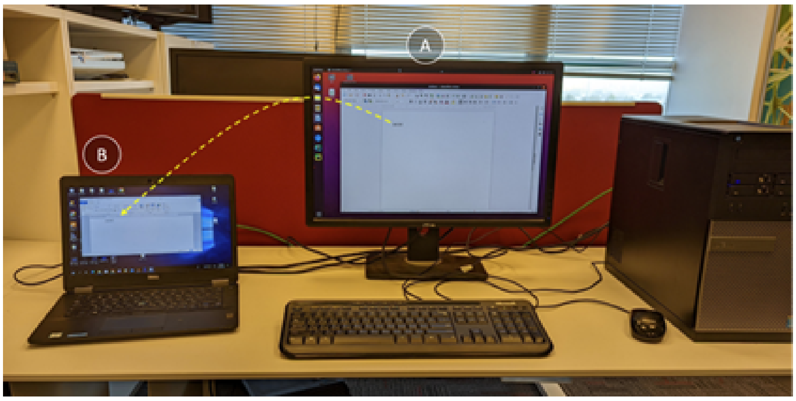


Figure 5.15: SATA cable covert channel

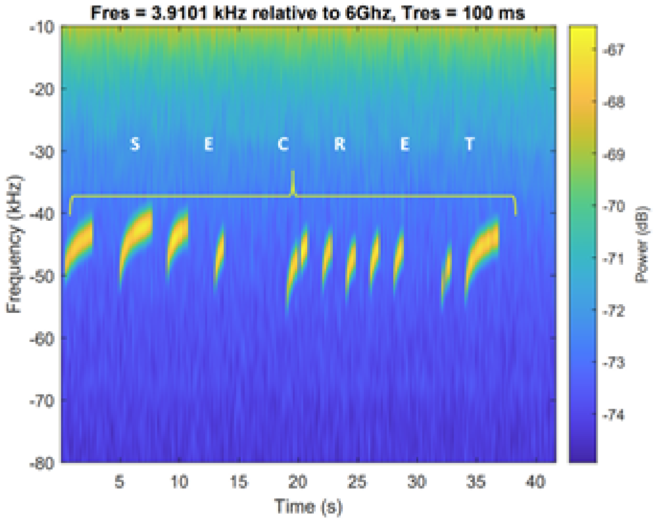
Technical background

SATA is a cable middleware for linking storage devices to a node. It offers various rewards evaluated with existing regulations such element PATA with higher bandwidths and movement rates. The wire is built with two sided 7 pins with the edge connected towards 90 degrees. The wire which is often paired links the SATA port on the motherboard and the storehouse devices. SATA authority connector has power supplies of range +3.3V DC, +5V DC, and +12V DC. SATA revision 1.0, revision 2.0, revision 3.0 has a data transfer speed of 150 MB/s, 300 MB/s and 600 MB/s respectively.

Transmission and reception

Signal Generation is deployed in implementing the covert channel with SATA conductor as an aerial and controlling the electromagnetic emergence is the key idea behind this approach and shows that the SATA 3.0 cables produce electromagnetic emissions of frequency bands of range 1 GHz,2.5 GHz, 3.9 GHz, and +6 GHz. TRANSMIT purpose is globalized and use read and write dealings of the transmittance with time factors for '0' (T0) modulation. The system call commands in Linux such as open(), fflush() and sleep() are used in signal generation shellcode. Frame preamble with 16-bit header payload allows actual recipients to sync with the communication with a parity bit used for error recognition. Anti-Virus evasion is applied in a part thread and inserted into the storage space of another convicted process system by using the techniques such as CreateRemoteThread', 'WriteProcessMemory' and 'LoadLibrary'.

Evaluation The experimental system combines SATA convergence with Linux Ubuntu 20.04.1 64-bit OS and a Transcend 256GB MLC SATA III 6Gb/s 2.5" SSD Drive 370. The recipient is ADALM PLUTO AD9364 RF 70 MHz to 6 GHz Software-defined Radio (SDR). The SDR was connected via USB to a laptop running Microsoft Windows 10 Enterprise, and the



. The payload 'SECRET' transmitted with the SATAn covert channel

Figure 5.16: SATAn covert channel transmission [8]

response and demodulation code from MATLAB were used to practice the results. The signs generated by PC-1 and PC-2 were much weaker, with 15 dB (PC-2) at 60 cm and 7 dB at 30 cm, respectively (PC-3). At distances of 0–90 cm, >120 cm, and 30 cm, respectively, the Bit Error Rate of 1%–5%, >15%, and 5% is maintained.

Counter measures The "red/black" strategy is defined by US and NATO regulations. Alternate method is to usage an external RF monitoring system scheme to identify malwares in the 6 GHz range close to the broadcasting node and the negative issue is it experience from fake devices and a low discovery rate since any interpret or compose process would generate electromagnetic release in this range, in spite of the channel. This explanation has a major disadvantage of harming the presentation of Input, Output and Storage behaviors in the OS. The exterior jamming action would engross the usage of radio indication jammers in the frequency range of 6 GHz. Moreover, such gadgets are costly and cannot be basically organized on a broad manner.

SATAn, a unique type of risk on air gapped computers, is presented in this study paper. The authors have utilized the SATA cable as a transmitter to convey electromagnetic signals in the frequency range of 6 GHz through non-prioritized read and write functions. Particularly, the

SATA middleware is highly accessible to attackers in all interlinked gadgets and networks. The results illustrate that attackers be able to use the SATA cable to convey a concise amount of privacy data from extremely protected wifi air-gap computers to a near recipient which is 1m away from the source. The authors also proved that malwares could work from user mode which is more convenient from inner a guest VM. They also discussed the security and preventive parameters for this channel attack through covert basis.

5.5 Spiral Spy mmWave covert channel

This covert channel attack method in air gapped systems using the millimeter wave sensing technology[9]. The proposed method named Spiralspy surreptitiously attack strongly isolated devices in reasonable distance. The authors leveraged the possibility of ordinal cooling fans for the vulnerable attacks. They demonstrate that the malicious code included in the fan control systems can encode the confidential data through the fan control systems. They too proved that Spiralspy can be scalable to multiple ordinal fan systems. Additionally, it is applicable to high-speed, multi-channel information transmission. They are examining this strategy in cooling fans of 71 computing devices. Results exemplify that this model can achieve 6 bps and 6-24X faster than the existing covert channel attacks. They evaluate the model in different real-world scenarios. Finally, they perform a comprehensive analysis in the countermeasures of the Spiralspy covert channel attacks.

Approach and Technical Background

The research contribution of this article is listed as follows: Research deployed 71 different computing devices which is equipped with cooling fans, and they used these devices for the experiments, and it includes 20 GPU, 20 Internet of Things gadgets, 20 coolers of CPU and 11 other devices.

They make use of 60-millimeter NVidia GTX XP GPU Titan cooling fans. Additionally, they used a cooler Master PRO 120 fan, which has a 120 mm diameter. Additionally, it contains a 120-diameter ENERMAX LIQMAX III 360 CPU. And they finally use the Raspberry Pi case IoT fan, and it has the 18 mm diameter.

They define control interface used in SpiralSpy which is competent of larceny data from diverse platforms, and it includes IoT, computing devices and cloud server. It can be deployed in different series of function scenarios. For data collection SpiralSpy response samples are collected from different fans using different sensing aspects. Evaluation Metrics used by the authors are confusion Matrix. The researchers focus on the following parameters:

• Signal preprocessing • Feature extraction • Fan speed identification **SpiralSpy Sniper reading scheme:**
The researchers propose a scheme which can read the fan speed remotely. They selected millimeter wave probe which has the high frequency and bandwidth. It has 24 gigahertz with 450-megahertz bandwidth, next to that they create a prototype of phenomenon using the SpiralSpy. They built up to 35 of physical features related to rotor speed. They deploy the machine learning model Random Forest for prediction of spiral RF.

SpiralSpy Architecture
The authors propose two unique phases, one's named as SpiralSpy planted agent and another one is named as SpiralSpy sniper.

1. SpiralSpy planted agent: It steels information in uni-directional method in the air gapped computers where agent is made pre-installed in the computing devices. Agent doesn't make any impact in the anti-virus issues, and it doesn't make any presence in computation performance or human perceptible noise. It seamlessly transfers the data using the fan cooling devices of the computing system generated by the cooling device. It is not notable by the human perception; agent controls the fan using the DC and voltage regulations which can accelerate or decelerate. They manipulate target fan status through customized fan status algorithm, control interface and fan speed modulator.
2. SpiralSpy remote sniper: It contains both hardware and software component.

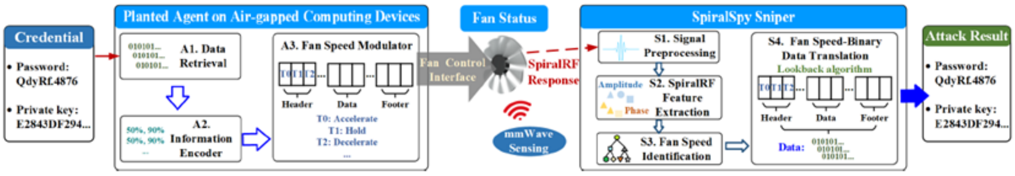


Figure 5.17: Spiral Spy & Agent-Sniper Flow diagram [9]

a. Sniper hardware: It uses the fan status from outside of the air-gapped computers. It employs FM mm wave radar and spiral sensor. It incessantly instigates the fans and captures the respective spiral RF response.
b. Sniper software: After receiving the spiral RF response a signal spatio-temporal features are retrieved. It efficiently retrieves information and forward to classification algorithm for machine learning. The translation of fan status to binary signals is fed into an algorithm to

renovate the information as per to the information transmission protocol.

Experiment results

The researchers evaluate the performance of GPU, IoT devices, CPU cooling fans[9], the performance of multi-channel attacks robustness and practical evaluation is carried out in identifying impact of attack orientation. Attack distances or proximity impact of computing devices are tested. Workloads and impact of through wall isolation's, ambient dynamics and the focus on sustained attack analysis are tested. The attack on the three types of data including text, audio and image is exemplified in following parameters in two types of channels (single and multichannel):

1. Text: they used 240 bits text with 272-bit token details □ Accuracy of 99.4%
2. Image: 3600 bit fingerprint image greater Accuracy of 99.1%
3. Audio: 4200 bit confirmation audio file greater Accuracy of 99.4%

They also have some binary errors, but it seems so be slight noise and not having impact in the accuracy.

Countermeasure

The authors propose countermeasures can be implemented in following aspects:

1. Creating a very large separation area (for example, hundreds of sq ft) is believed to be a successful protection against the majority of the air-gapped assaults, including SpiralSpy. This is one of the most intuitive countermeasures that can be implemented. In contrast, it is not applicable to situations that occur in the real world (for reasons such as cost and usability)
2. Electromagnetic Field (EMF) protection [9], such as aluminum foil, may be placed to the computer equipment that have fans in order to block the mmWave sensing signal, as seen in Fig. 5.17. This can be done in order to prevent the machines from overheating (a). In order to protect against a Spiral-Spy covert channel attempt, the shielding on the machine has the ability to block mmWave transmissions coming into or leaving the device. When it comes to applying this strategy on computer devices, nevertheless, only a handful of practical issues. Firstly, utilizing an EMF shielding material to protect the machine casing and fan set will surely produce temperature regulation difficulties owing to a lack of heat dissipation. These issues will make it challenging or impossible to operate the machine. Additionally, the deployment of

the protective material results in a rise in the additional cost. In addition, one more alternative for isolating the space involved is to make use of a room that has been electromagnetically protected by a trained expert. On the other hand, the implementation of this approach would result in a large increase in expenses, and it will be challenging to scale.

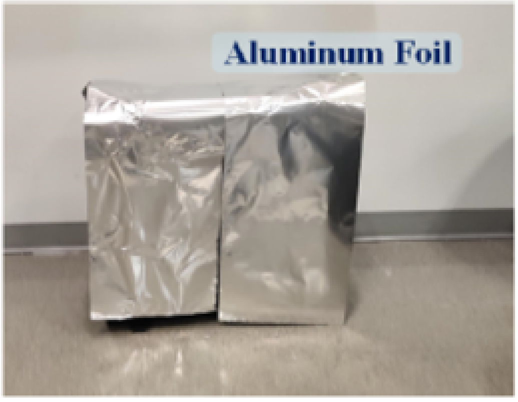


Figure 5.18: Countermeasures 1 Foil [9]

3. The use of a radio frequency interference device, such as a mmWave jammer, to block the mmWave receiving channel is still another method that might be used to get rid of this hidden channel. This method is shown in Figure 5.18 When this is done, all of the mmWave receiving terminals in the nearby area will be swamped with waves of full amplitude over the spectrum, and they will be unable to recognize the speed of the fans. However, putting it into reality without first determining the SpiralSpy carrier mmWave frequency may be difficult. In addition, prolonged exposure to this jammer device may be hazardous to the health of any employees who are in the direct proximity. 4. It is also feasible to stop this backdoor by installing a comparable additional computer equipment or fan nearby in order to spoof and deflect the mmWave sniper's signal. SpiralSpy, on the other hand, has the ability to circumvent this countermeasure thanks to a specifically defined header and footer area of the packet. In addition to the advantages provided by the EWT signal separation, SpiralSpy is able to eliminate the noise caused by the additional fan during the first stage of the reading technique. In addition, figuring out the SpiralSpy information transfer methodology simultaneously in real practice is a difficult task to accomplish. Also, it will drive up the price of the protection.[9]
These are some suggestions of the authors to overcome the SpiralSpy covert channel attacks. This study demonstrated a practical, covert ordinal fan-based exploit using mmWave sensing

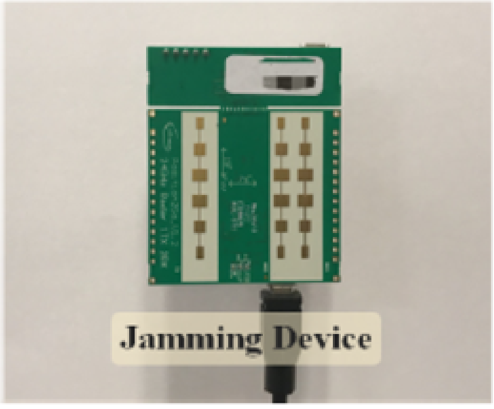


Figure 5.19: Countermeasures 2 jamming Device [9]

on air-gapped computer equipment. They controlled the SpiralRF response based on the fan's tangential velocity. They advise taking some of the actions indicated in the section. They offer a fresh viewpoint on fan-based assaults against air-gapped computers.

6 Proposed solution

Data Diode: A Hardware-based Security Solution [10] Cybersecurity risks are growing more widespread and complex in today's linked society. Government organization's and service providers of vital infrastructure are especially vulnerable to these attacks because they handle sensitive information that might have catastrophic effects if it falls into the wrong hands. Here is where the data diode comes into play: it is a hardware-based security solution that offers a one-way communication channel between two networks. The data diode is widely employed by the US DoD and Cp-commands, as well as US intelligence agencies, DISA, DOE, DHS, and several other US government agencies. It is approved for unclassified, secret, top secret, and coalition partner networks. This means it has been extensively tested and certified to meet the highest security requirements, ensuring sensitive data stays secure and protected.

For 15 years, the data diode has been implemented and supported critical infrastructure, including nuclear, hydropower production, oil, gas, petrochemical, and water/wastewater management. Certain industries are especially vulnerable to cyber-attacks because any disruption in their operations might have major ramifications for public safety and the economy. Critical infrastructure providers may safeguard the security of their operations and sensitive information by utilising a data diode.

One of the most significant benefits of the data diode is that it cannot be compromised by software threats. In contrast to software-based security solutions, which are subject to malware and other kinds of cyber-attacks, the data diode is a fully hardware-based solution that acts as a physical barrier between two networks. This implies that even if one of the networks is compromised, sensitive data on the other network is safe. Finally, the data diode is a crucial security solution for government organizations and critical infrastructure companies. Its hardware-based architecture protects sensitive information from cyber-attacks, and its accreditation for a wide range of security levels guarantees that it may be utilized in a number of scenarios. With 15 years of successful deployments in critical infrastructure, the data diode has demonstrated its efficacy in protecting sensitive information and ensuring the security of our most essential systems.

Data Diode Architecture The twin diode architecture is a hardware-based security approach that employs two communication cards connected in series to provide an ”air gap” and enforce network isolation. This air gap guarantees that data can only move in one way, avoiding data loss or intrusion.

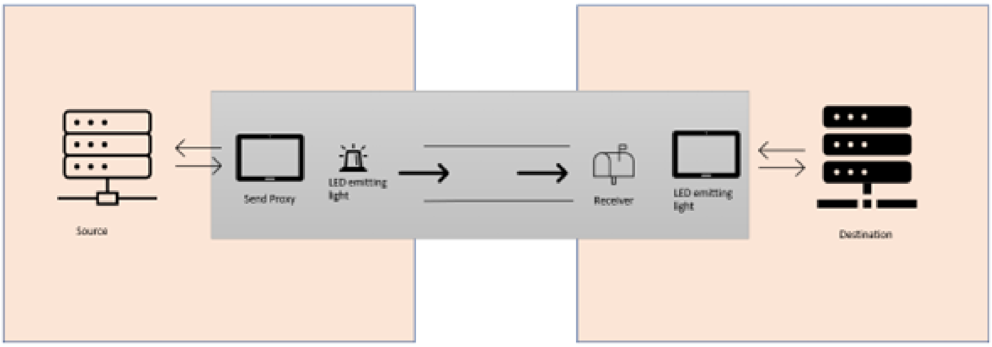


Figure 6.1: Data Diode Architecture [10]

Furthermore, the dual diode design includes IP proxies that both terminate and originate IP traffic. This implies that routable information, such as MAC and IP addresses, is never exposed outside of the OT (Operational Technology) network, and only the payload crosses the air gap. **Security Attributes:** The dual diode architecture has several security attributes that make it an ideal solution for critical infrastructure and government agencies. Firstly, the routable information is never exposed outside the OT network, which means that any potential attackers are unable to gain any information about the network itself. This ensures that the network remains secure and protected.

Second, the dual diode design employs a regulated and whitelisted transport of all data kinds. This implies that only authorized data types may get across the air gap, while unauthorized data types are prohibited. This guarantees that the network is safe and free of any dangers. The dual diode architecture is further constrained by a single fiber optics cable, which adds an additional

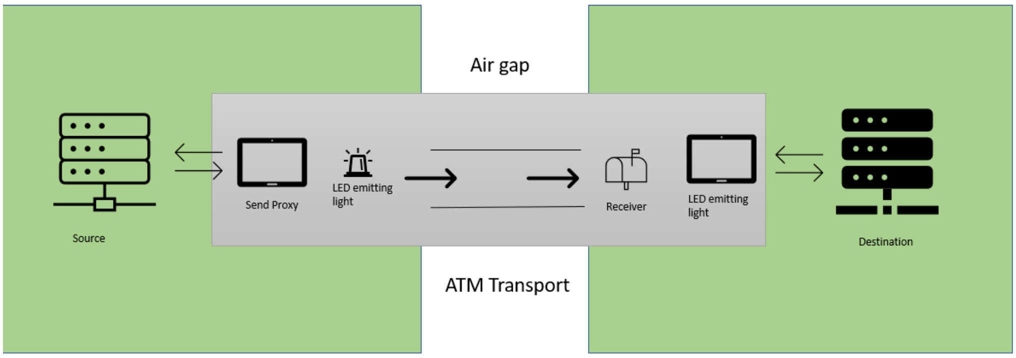


Figure 6.2: Data Diode Architecture & ATM Protocol [10]

layer of security to the system. This ensures that data can only flow in one direction, from the source network to the destination network. **ATM (Asynchronous Transfer Mode)**
ATM (Asynchronous Transfer Mode) protocol is a high-speed networking protocol that was originally designed for use in high-speed WAN (Wide Area Network) and LAN (Local Area Network) environments. The ATM protocol is a connection-oriented protocol that uses fixed-length cells to transport data across the network.

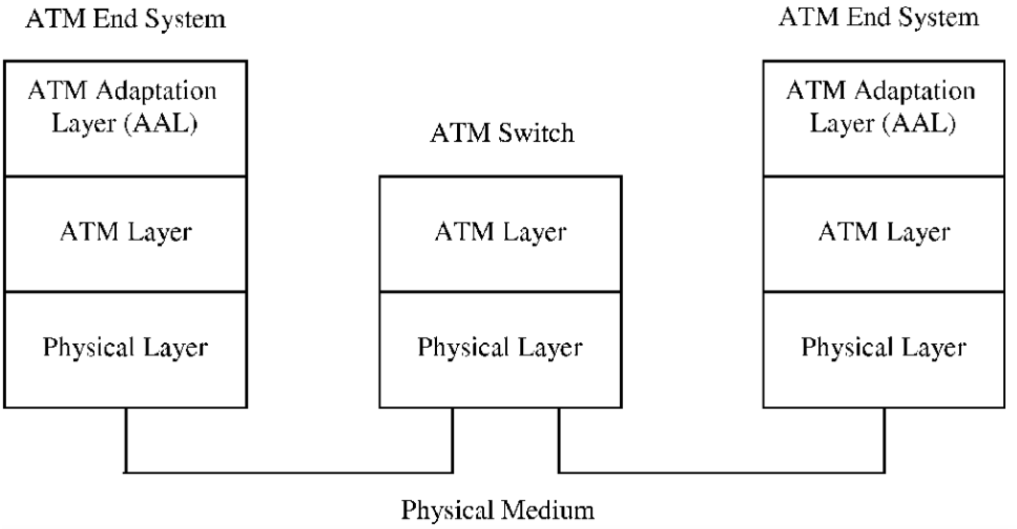


Figure 6.3: ATM Protocol structure [11]

The ATM protocol is employed in the context of an air-gap solution as a dependable high-speed transport method that enables a ”deep protocol break.” This implies that the data is extensively examined and authenticated before it is permitted to pass through the air gap.
One of the primary benefits of employing the ATM protocol with an air-gap solution is that it

is a very reliable protocol capable of delivering extremely high data rates. This makes it an excellent choice for usage in critical infrastructure and government organizations where fast and dependable data transfer is required. Furthermore, because it is a connection-oriented protocol, the ATM protocol assures that all data is sent in a safe and regulated way. Potential attackers will find it far more difficult to intercept or manipulate data when it passes the air gap as a result.

Overall, combining the ATM protocol with an air-gap solution is a highly effective technique to keep sensitive data secure and secure. The combination of high-speed data transmission and extensive protocol inspection guarantees that only legitimate data is transmitted over the air gap, and that any possible threats or abnormalities are recognized and prevented. In an air-gap solution, fiber optic cables can be utilized instead of WAN (Wide Area Network) connections to send data utilizing ATM (Asynchronous Transfer Mode) protocols. Because of its capacity to carry data over great distances with minimal signal quality degradation, fiber optic cables are widely sought for high-speed data transmission. Using fiber optic cables in an ATM-based air-gap system has various advantages, including:

High-speed data transmission: Fiber optic cables can provide very high data rates, which makes them an ideal choice for use in critical infrastructure and government agencies, where high-speed and reliable data transmission is essential.

Low signal loss: Because fibre optic connections have relatively minimal signal loss, data may be transported across vast distances with little loss in signal quality. This makes them excellent for use in air-gap solutions, where data must be sent over great distances.

Security: Fiber optic cables are highly secure, as they are very difficult to intercept or tap without detection. This makes them an ideal choice for use in sensitive applications such as critical infrastructure and government agencies.

7
Conclusion

Given the significant risk that air gap systems pose to various researchers on various hardware appliances, it's crucial to have a thorough understanding of information leakage and potential exploitation techniques. We examined potential current air gap attacks based on this open challenge and searched for commonalities among them in order to thoroughly categorize all current attacks and their methodologies. By outlining the classification system, we hope to fully explain information breaches caused by air gap systems, encourage more research and defenses against air gap attacks, and set the stage for secure air gap systems. However, the proposed system, which makes use of a data diode with a dual diode design, the ATM protocol, and fiber optic connections, offers a highly secure option for critical infrastructure and government organizations. The technology assures that sensitive data may only go in one way by deploying an air-gap solution, while the ATM protocol provides high-speed data transfer and thorough protocol inspection to avoid any potential risks or irregularities. Overall, considering the enormous danger that air-gap systems provide to various hardware appliances, our strategy emphasizes the significance of ongoing study and security against air-gap threats."

Acknowledgment

I would like to take this opportunity to express my heartfelt appreciation to the Italian country for providing a high-quality education system. Their commitment to education has enabled me to pursue my academic goals and attain success in my studies.

I would also like to extend my sincere thanks to Asst. Prof. Alessandro Brighente and Prof. Mauro Conti for their invaluable support and guidance throughout my academic journey. Their time, effort, and tolerance have been instrumental in my academic success, and I am deeply grateful for their great knowledge and breadth of experience.

Furthermore, I would like to express my gratitude to Wanders, Peter from KLM for the thesis opportunity. Their trust and support have been essential in helping me achieve my academic goals. During my time spent taking classes and living in Italy, I have been blessed to encounter kindness and encouragement from many individuals, which has made my experience extremely gratifying. I am truly grateful for their support, and I believe that their positive influence has contributed significantly to my personal growth. Lastly, I would like to express my gratitude to God and my parents for their steadfast support and unwavering belief in my abilities. Without their support, I could not have completed my studies over the previous two years. Thank you for everything!

References

[1] M. Guri, "Lantenna: Exfiltrating data from air-gapped networks via ethernet cables emission." Institute of Electrical and Electronics Engineers Inc., 7 2021, pp. 745–754.

[2] cables solutions, "Ethernet-cable." [Online]. Available: https://www.cables-solutions.com/how-to-choose-right-cat5e-cable-for-your-network.html

[3] OPTCORE, "Ethernet cable difference and comparison," pp. 1–end, 6 2021.

[4] E. T. fiber), "Advantages of fiber optic and immunity to electromagnetic interference," p. 1, 7 2017. [Online]. Available: https://www.emctech.com.au/advantages-fiber-optic/

[5] E. Knowles and L. Olson, "Cable shielding effectiveness testing," *Electromagnetic Compatibility, IEEE Transactions on*, vol. EMC-16, pp. 16 – 23, 03 1974.

[6] M. U. T. T. A.-G. C. usingSpeaker-to SpeakerCommunication, *IEEE DSC 2018 : the 2018 IEEE Conference on Dependable and Secure Computing : Kaohsiung, Taiwan, December 10-13, 2018*.

[7] M. Guri, M. Monitz, and Y. Elovici, "Usbee: Air-gap covert-channel via electromagnetic emission from usb." Institute of Electrical and Electronics Engineers Inc., 2016, pp. 264–268.

[8] M. Guri, "Satan: Air-gap exfiltration attack via radio signals from sata cables," 7 2022. [Online]. Available: http://arxiv.org/abs/2207.07413

[9] Z. Li, B. Chen, X. Chen, H. Li, C. Xu, F. Lin, C. X. Lu, K. Ren, and W. Xu, "Spiralspy: Exploring a stealthy and practical covert channel to attack air-gapped computing devices via mmwave sensing." Internet Society, 4 2022.

[10] O. cyber Defense, "Data diode products."

[11] K.-Y. Siu and R. Jain, "A brief overview of atm: Protocol layers, lan emulation, and traffic management."

[12] M. Guri and D. Bykhovsky, "air-jumper: Covert air-gap exfiltration/infiltration via security cameras infrared (ir)," *Computers and Security*, vol. 82, pp. 15–29, 5 2019.

[13] SecureStrux, "Siprnet: A brief introduction to the secret router network," 8 2021. [Online]. Available: https://blog.securestrux.com/siprnet-a-brief-introduction-to-the-secret-router-network

[14] P. NSCSAR Chair, "Niprnet/siprnet cyber security architecture review - disa," pp. 1–10, 4 2016.

[15] D. Y. Kim, "Cyber security issues imposed on nuclear power plants," *Annals of Nuclear Energy*, vol. 65, pp. 141–143, 2014.

[16] A. V. Dine, M. Assante, P. Stoutland, and A. Van, "Outpacing cyber threats priorities for cybersecurity at nuclear facilities about the authors."

[17] D. Das, "An indian nuclear power plant suffered a cyberattack," 11 2019. [Online]. Available: https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/

[18] M. . Baezner and P. Robin, "Eth library stuxnet report," 2017. [Online]. Available: https://doi.org/10.3929/ethz-b-000200661

[19] M. Willett, "Lessons of the solarwinds hack," *Survival*, vol. 63, pp. 7–26, 2021.

[20] M. A. T. K. C. V. P. Mission Engineering, "Azure government top secret now generally available for us national security missions," pp. 1–end, 6 2021.

[21] M. Guri, M. Monitz, and Y. Elovici, "Usbee: Air-gap covert-channel via electromagnetic emission from usb." Institute of Electrical and Electronics Engineers Inc., 2016, pp. 264–268.

[22] ——, "Usbee: Air-gap covert-channel via electromagnetic emission from usb." Institute of Electrical and Electronics Engineers Inc., 2016, pp. 264–268.

[23] E. T. fiber), "Advantages of fiber optic and immunity to electromagnetic interference," p. 1, 7 2017. [Online]. Available: https://www.emctech.com.au/advantages-fiber-optic/

[24] P. Vitello, "A ring tone meant to fall on deaf ears," p. 1, 6 2006.

[25] V. Mavroudis, S. Hao, Y. Fratantonio, F. Maggi, C. Kruegel, and G. Vigna, "On the privacy and security of the ultrasound ecosystem," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, pp. 95–112, 4 2017.

[26] M. Guri, "Power-supplay: Leaking data from air-gapped systems by turning the power-supplies into speakers." [Online]. Available: http://www.covertchannels.comDemovideo:http://www.covertchannels.com

[27] M. .-. D. o. D. National Security Agency, Fort George G. Meade, "Nstissam tempest/2-95." p. 1, 12 2000.

[28] S. Abraham and I. Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications," *Technology in Society*, vol. 32, no. 3, pp. 183–196, 2010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0160791X10000497

[29] M. Hanspach and M. Goetz, "On covert acoustical mesh networks in air," *Journal of Communications*, vol. 8, 06 2014.

[30] Mavroudisv, "Silverdog," p. 1, 7 2018.

[31] A. D. B.-G. Y. E. Mordechai Guri, Yosef Solewicz, "Diskfiltration: Data exfiltration from speakerless air-gapped computers via covert hard drive noise." [Online]. Available: https://www.youtube.com/watch?v=H7lQXmSLiP8

[32] Intel, "Emi design guidelines for usb components 1. disclaimer."

Acknowledgments