LANTENNA: Exfiltrating Data from Air-Gapped Networks via Ethernet Cables

Mordechai Guri
Ben-Gurion University of the Negev, Israel
Cyber-Security Research Center
gurim@post.bgu.ac.il
air-gap research page: http://www.covertchannels.com

***Abstract*—Air-gapped networks are wired with Ethernet cables since wireless connections are strictly prohibited.**

In this paper we present LANTENNA - a new type of electromagnetic attack allowing adversaries to leak sensitive data from isolated, air-gapped networks. Malicious code in air-gapped computers gathers sensitive data and then encodes it over radio waves emanating from the Ethernet cables, using them as antennas. A nearby receiving device can intercept the signals wirelessly, decode the data, and send it to the attacker. We discuss the exfiltration techniques, examine the covert channel characteristics, and provide implementation details. Notably, the malicious code can run in an ordinary user-mode process and successfully operate from within a virtual machine. We evaluate the covert channel in different scenarios and present a set of countermeasures. Our experiments show that with the LANTENNA attack, data can be exfiltrated from air-gapped computers to a distance of several meters away.

***keywords*—air-gap, exfiltration, covert channels, data leakage, Ethernet, LAN, electromagnetic.**

I. Introduction

Information is the most valuable asset of modern organizations. Accordingly, adversaries spend a lot of resources and efforts to put their hands on the target information, usually documents and databases. After reaching the data, the attackers exfiltrate the information outside the boundaries of the organization. This is usually done in the form of covert communication channels within Internet protocols such as HTTPS, FTP, SMTP, and so on. Many massive data leakage incidents have been reported in the last decade. For example, In 2020, Microsoft disclosed a data breach event that occurred due to misconfigured security rules. According to the reports, 250 million records with personal information such as emails, IP addresses, and other details, were exposed [1]. In August 2021, Microsoft warned thousands of Azure users that their data might have been exposed through a database vulnerability named ChaosDB [3]. According to reports from the Identity Theft Resource Center (ITRC) and the U.S. Department of Health and Human Services, more than 98 million people were impacted by data breaches in the first half of 2021 [6].

A. Air-Gap Networks

Due to the increased risk of information leakage, when sensitive data is involved, an organization may move to so-called *air-gap* isolation. Air-gapped computers are wholly separated from external wide area networks (WAN) such as the Internet [4]. Many modern industries maintain their data within air-gapped networks, including financial, defense, and critical infrastructure sectors. Classified networks of military contractors and intelligence agencies may have air-gapped networks in place. E.g., the SIPRNet (Secret Internet Protocol Router Network) is a system of isolated and interconnected networks used by the U.S. Department of Defense to exchange classified information [8].

B. Air-Gap Penetration

While theoretically air-gapped networks provide ultimate protection from cyber threats, in practice, it has been proven that even air-gapped networks are not immune to attacks. In 2008, the Agent.BTZ worm compromised classified and unclassified networks in the United States Central Command [2]. Another example is Stuxnet, the virus that infected the enriching uranium in Natanz nuclear facility. In this case, the malware was reportedly delivered via a thumb drive. Motivated adversaries can use sophisticated attacks to breach highly secure networks, such as compromising elements in the supply chain and infecting third-party software. Another attack tactic is to use malicious insiders in a so-called 'evil maid attack,' or exploit deceived insiders within the organization [17][5].

In 2019, the Kudankulam Nuclear Power Plant in India was the target of a successful cyberattack earlier that year [19]. In December 2020 SolarWinds breach, the hackers gained access to thousands of companies and government offices that used its products. The incident that was referred to as "the largest and most sophisticated attack the world has ever seen" involved a highly evasive backdoor implanted within the company products. These types of techniques allow attackers to insert targeted malware into highly secured networks and environments.

C. Air-Gap Covert Channels

After the attackers implanted their advanced persistent threat (APT) in the target network, they move on to the next phases of the attack kill chain. Initially, sensitive information is gathered: documents, images, keylogging, encryption keys, or databases. If the network is connected to the Internet (directly or via a virtual private network (VPN)), the data is exfiltrated through covert channels within known Internet protocols (e.g., HTTPS,

FTP, SSH, and SMTP [51]). However, if the network is air-gapped, the attackers must exploit nonstandard communication techniques to exfiltrate the data outward, methods which are also referred to as air-gap covert channels [26]. Adversaries can exploit radio waves emanated from internal electronic components to transmit data [28], [43], [44], [49], [27]. They may also use the status LEDs on desktop computers to covertly transmit information [46], [38], [39]. Acoustic [16], [34], thermal [31], magnetic [24], electric [36], and seismic air-gap covert channels have also been introduced over the years [15].

D. Our Contribution

This paper introduces LANTENNA - a new type of electromagnetic attack that exploits the Ethernet networking cables to leak data wirelessly from air-gapped networks. Malware executed in a compromised workstation or server can regulate the electromagnetic waves emanated from an Ethernet cable, effectively use it as a transmitting antenna. We show that any type of binary data can be modulated on top of the generated radio signals. We also show that a standard software-defined radio (SDR) receiver in the area can decode the information and then deliver it to the attacker via the Internet.

The following sections are organized as follows: Related work is discussed in Section II. The adversarial attack model is introduced in Section III. Technical background is provided in Section IV. Sections V and VI, respectively, describe the signal generation, and data transmission and reception. In Section VII we present the evaluation results. We discuss the possible countermeasures in Section VIII, and we conclude in Section IX.

II. Related Work

Certain malware such as the Conficker worm could move between computers via USB thumb drives [48]. Kuhn showed that it is possible to exploit the electromagnetic emissions from the computer display unit to conceal data [43]. AirHopper, presented in 2014, is a malware capable of leaking data from air-gapped computers to a nearby smartphone via FM radio waves emitted from the screen cable [28], [30]. In 2015, Guri et al. presented GSMem [27], malware that transmits data from air-gapped computers to nearby mobile phones using cellular frequencies. USBee is malware that uses the USB data buses to generate electromagnetic signals [29]. To prevent electromagnetic leakage, Faraday cages can be used to shield sensitive systems. Guri et al. presented ODINI [40] and MAGNETO [24], two types of malware that can exfiltrate data from Faraday-caged air-gapped computers via magnetic fields generated by the computer's CPU. With MAGNETO, the authors used the magnetic sensor integrated into smartphones to receive covert signals. In 2019, researchers showed how to leak data from air-gapped computers by modulating binary information on the power lines [36].

Several studies have proposed the use of optical emanations from computers for covert communication. Loughry and Guri demonstrated the use of keyboard LEDs [46][35]. Guri used the hard drive indicator LED [38], router and switch LEDs [37], and security cameras and their IR LEDs [25], in order to exfiltrate data from air-gapped networks.

BitWhisper [32] is a thermal-based covert channel enabling bidirectional communication between air-gapped computers by hiding data in temperature changes.

Hanspach [41] used inaudible sound to establish a covert channel between air-gapped laptops equipped with speakers and microphones. Guri et al. introduced Fansmitter [34], Diskfiltration [33], and CD-LEAK [23] malware which facilitates the exfiltration of data from an air-gapped computer via noise intentionally generated from the PC fans, hard disk drives, and CD/DVD drives.

Another type of attack on the air-gapped system is the side channels. In this form of attack, adversaries could extract various information from systems remotely, via electromagnetic [50], acoustic [21], and optical [47] information leakage.

III. Attack Model

The adversarial attack model consists of two main steps: infecting the air-gapped environment and data exfiltration. In the first step of the attack, the air-gapped environment is infected with malware, usually in the form of APT.

A. Reconnaissance and Infection

The APT Kill chain model was developed by Lockheed Martin that categorizes seven stages of targeted cyber attacks. The seven common phases of APT intrusions are reconnaissance, weaponization, delivery, exploitation, installation, Command & Control, and data exfiltration. In the context of our work, the relevant phases to discuss are reconnaissance, delivery, and exfiltration.

In a reconnaissance phase, the attackers collect as much information as possible on their target, using various tools and techniques [11]. After defining the initial target, attackers might install malware on the network via different infection vectors: supply chain attacks, contaminated USB drives, social engineering techniques, stolen credentials, or by using malicious insiders or deceived employees.

Note that an infection of highly secure networks is proven to be feasible, as demonstrated by many incidents in the last decade [45], [22], [9], [7], [10]. At that point, the APT goal is to escalate privileges and spread in the network to strengthen its foothold in the organization.

B. Data Exfiltration

As a part of the APT exfiltration phase, the attacker might gather data from the compromised computers. The stolen information can be documents, databases, access credentials, encryption keys, and so on.

1) Data transmission: Once the data is collected, the malware exfiltrates it using the covert channel. In the case of LANTENNA attack, it modulates the data and transmits wirelessly via the radio waves emanated from the Ethernet cables.

Fig. 1. Illustration of the LANTENNA attack. Malware in the air-gapped network exploits the Ethernet cable, using it as an antenna to transmit radio signals. Binary information is modulated on top of the signals and intercepted by a nearby radio receiver.

2) Data reception: A nearby radio receiver can receive the covert transmission where it is decoded and send to an attacker. The receiving hardware can be carried by a malicious insider or hidden in the area.

The attack is illustrated in Figure 1. Malware in the air-gapped workstation generates electromagnetic emissions from the Ethernet cable. Binary information is modulated on top of the signals and intercepted by a nearby radio receiver.

IV. Technical Background

Ethernet cables connect networked devices such as workstations and servers, printers, cameras, routers, and switches within a local area network (LAN). The network cable consists of eight wires which are twisted into four pairs. Several categories (cat) of Ethernet cables define parameters such as working frequencies, shielding, and bandwidth. The commonly used network cables are Cat 5, Cat 5e, Cat 6, Cat 6a, Cat 7, and Cat 7a. The main parameters of each category are specified in Table I.

- **Cat 5, Cat 5e**. Cat 5 and Cat 5e (Category 5 enhanced), are similar at the physical level, and they are both working at a maximal frequency of 100 MHz. However, while Cat 5 cable supports network bandwidth of 10-100 Mbps, a Cat 5e cable supports networks bandwidth up to 1 Gbps. In addition, the wires in Cat 5e cables are twisted more tightly than those in the Cat5 cable, which makes them more protected to unwanted signal inference between communication channels (crosstalk). Cat 5e is currently the most commonly used cable for home and small office facilities.
- **Cat 6**. Cat 6 cables support networks bandwidth up to 1 Gbps. They are better shielded, which helps in the prevention of crosstalk and electromagnetic interference. Cat 6 cables support bandwidth up to 1 Gbps for a distance of 55 meters. Cat 6 is mostly used in Enterprise IT networking environments.
- **Cat 6a**. Cat 6a (category 6 augmented) cables support network bandwidth up to 10 Gbps. Cat 6a cables are shielded and could eliminate crosstalk and interference. Cat 6a is mostly used in Enterprise IT networking environments.
- **Cat 7, Cat 7a**. Cat 7 and Cat 7a (Category 7 enhanced) cables support higher bandwidths up to 10-40 Gbps to a range of 15 meters. Cat 7 cables are shielded and contain four individually shielded pairs inside an overall shield. They are manufactured with a GG45 connector which is also compatible with the RJ45 Ethernet ports. Cat 7 and Cat 7a are mostly used in data centers and high-bandwidth networking facilities.

Besides these Ethernet cables, there are less common types. Cat 3 is 10 Mbps unshielded cable with a maximum bandwidth of 16 MHz and is obsolete today. The new fast Cat 8 cable is an emerging technology. Cat 8 currently offers one of the highest performance Ethernet capabilities. It supports a bandwidth of 40 Gbps, and it is highly shielded. Cat 8 is mostly used in big data centers and high-bandwidth networking facilities.

V. Transmission

In this section we present the signal generation techniques, data modulation, and data transmission protocol.

A. Signal Generation

Ethernet cables are electromagnetic in various frequency bands and amplitudes. Note that this phenomenon was studied in previous work in the general context [20], [18]. Other work exploited the unintentional emission from the Ethernet cables to extract side-channel information [13], [14]. In our work, we *intentionally* exploit and trigger the electromagnetic emanation for data modulation and covert communication.

We used two techniques to regulate the electromagnetic signals emanated from the Ethernet cables: (1) Ethernet speed toggling and (2) raw packets transmission.

B. Ethernet Speed Toggling

Ethernet cables emit electromagnetic waves in the frequency bands of 125 MHz and its harmonics (e.g., 250 MHz and 375 MHz). Note that the radiated frequency bands are determined by the operational frequency of the cable (e.g., 0-250 MHz for Cat 6, 0-500 MHz for Cat 6a, and 0-700 MHz for Cat 7 cables). We observed that changing the adapter speed or turning it on and off makes it possible to regulate the electromagnetic radiation and its amplitude. Figure 2 shows the waveform and spectrogram generated by a transmission of the alternating sequence '10101010...' using the Ethernet speed toggling method with Cat 6 cable. In this case, the data was transmitted from an air-gapped computer through its Ethernet cable and received at a distance of 200 cm apart. As can be seen, the signal is wrapped around 125.010 MHz.

C. Raw Packets Transmission

The data and link layers activities determine the current flow on the copper wires in the Ethernet cables. By sending raw UDP packets, we could trigger and regulate the emission from the Ethernet cable at its operational frequency. Figure 3 shows the waveform and spectrogram generated by transmission of

TABLE I
ETHERNET CABLE CATEGORIES

#	Cable	Frequency	Ethernet Signal	Shielding	Connector	Pairs	Usage
1	Cat 5	100 MHz	10/100 Base T	Optional	8p8c, RJ45	4	Home, small office
2	Cat 5e	100 MHz	10/100 Base T, 1 Gigabit Ethernet	Optional	8p8c, RJ45	4	Home, small office
3	Cat 6	250 MHz	10/100 Base T, 1 Gigabit Ethernet	Optional	8p8c, RJ45	4	Enterprise IT
4	Cat 6a	500 MHz	10/100 Base T, 1/10 Gigabit Ethernet	Optional	8p8c, RJ45	4	Enterprise IT
5	Cat 7	600 MHz	10/100 Base T, 1/10 Gigabit Ethernet	Pairs + overall	GG45, TERA	4	Datacenters
6	Cat 7a	1000 MHz	10/100 Base T, 1/10 Gigabit Ethernet	Pairs + overall	GG45, TERA	4	Datacenters

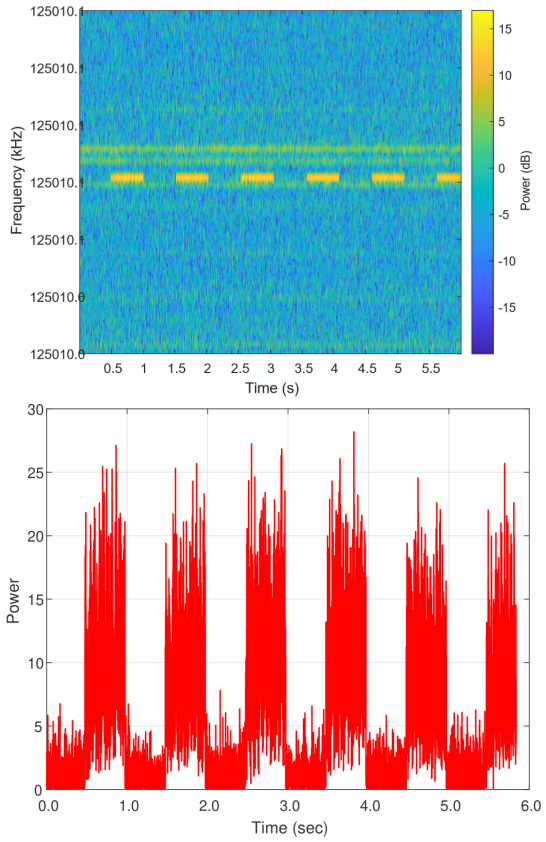

Fig. 2. The waveform and spectrogram generated by a transmission of the alternating sequence '0101010...' from the Ethernet cable, using the Ethernet speed toggling.

the alternating sequence '10101010...' using the raw packet transmission method. In this case, the data was transmitted from an air-gapped computer through its Ethernet cable and received at a distance of 200 cm apart. As can be seen, the signal is wrapped around 250.010 MHz and is narrower than the signal generated by the speed toggling method.

The pseudo code of the modulator is shown in Algorithm 1. The `modulate` function receive the array of bits to transmit (`bits`) and the time of each bit (`bitTimeMillis`). If the bit to transmit is '1', the function sends UDP packets to the network; otherwise, it sleeps for the same duration. Each UDP packet contains a payload of 1480 bytes. The payload consists of a sequence of the 'U' character, which is the alternate bits (`01010101`) in its binary representation. The full UDP frame, as shown in the Wireshark network protocol analyzer, is presented in Figure 4.

Algorithm 1 modulate(bits, bitTimeMillis)

```
bitEndTime ← getCurrentTimeMillis()
for bit in bits do
    bitEndTime ← bitEndTime + bitTimeMillis
    halfBitEndTime ← bitEndTime − bitTimeMillis/2
    if bit == 1 then
        sleep(bitTimeMillis/2)
        while getCurrentTimeMillis() < bitEndTime do
            sendPackets()
        end while
    else
        while getCurrentTimeMillis() < halfBitEndTime do
            sendPackets()
        end while
        sleep(bitTimeMillis/2)
    end if
end for
```

D. Encoding and Packets Frames

Note that the amplitude of the signal may change over time, and hence, a simple OOK modulation fails during the reception. We used Manchester encoding since a bit is demodulated by analyzing the change in amplitude during both halves of the bit with no overall threshold is needed. Figure 5 depicts the Manchester encoding for the packet: enable = 0xAA, DATA = 'DATA', CRC8 = 0xB6.

- Enable. The packet begins with a `0xAA` hex value. This sequence of `10101010` in binary allows the receiver to synchronize with the beginning of each packet and determine the carrier amplitude and one/zero thresholds.
- Data. The payload is the raw binary data transmitted within the packet. It consists of 32 bits.
- CRC-8. For error detection, we use the CRC-8 (a cyclic redundancy check) error detection algorithm. The CRC is calculated on the payload data and added at the end of each packet. If the received CRC and the calculated CRC differ, the packet is omitted on the receiver side.

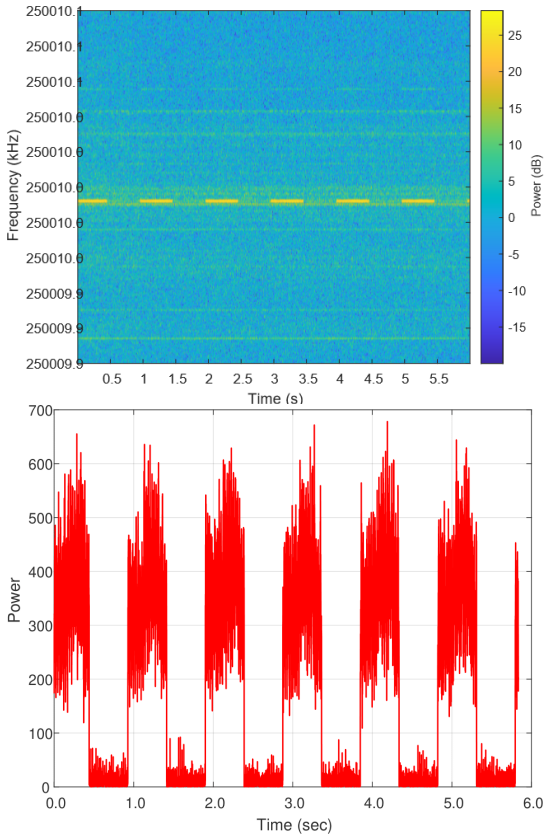

Fig. 3. The waveform and spectrogram generated by a transmission of the alternating sequence '10101010...' from the Ethernet cable, using the raw packets transmission method.

VI. Reception

A. Demodulation

The pseudo-code of the demodulator is presented in Algorithm 2. We provide the implementation for software-defined radio (SDR) receivers.

The `demodulate` function is based on sampling and processing the FFT information for the target frequency bands (125 MHz, 250 MHz, 375 MHz, and so on.). In lines 2-3, the SDR device is initialized, and the receiving buffer is configured with the frequency (in MHz) of the channel to monitor (`freq`), the sampling rate (`sampleRate`), and the buffer size (`windowsPerBit`). The demodulator samples the data in the target frequency and splits it into windows of `windowSize` size. The algorithm estimates the power spectral density for each window using Welch's method (lines 9-13). It then detects the *enable sequence* (`10101010`) using the `detectEnable` routine. It then decodes the bit using Manchester scheme (`SampleToBitManchester`) and determines the thresholds (amplitudes) for '1' and '0' bits (lines 14-18). Finally, the bits are demodulated and added to the output vector (lines 18-21).

VII. Evaluation

In this section, we present the evaluation of the covert channel. We describe the experimental setup and test the different reception modes used to maintain the covert channel.

Algorithm 2 demodulate(fileName, freq, sampleRate, bitTime, windowSize)

1: $enabled \leftarrow False$
2: $windowsPerBit \leftarrow bitTime * sampleRate/windowSize$
3: $fileID = writeRtlSdrOutputToFile(fileName, \leftarrow freq, sampleRate)$
4:
5: **while** $True$ **do**
6: $window = fileID.blockingRead(windowSize)$
7: $spectrum = fft(window)$
8: $sampleValue \leftarrow getSignalAmplitude(spectrum)$
9: $samples.append(sampleValue)$
10: **if** *not enabled* **then**
11: $enabled \leftarrow detectEnable(samples)$
12: **end if**
13: **while** $enabled$ and $enoughSamplesForBit(\leftarrow samples, windowsPerBit)$ **do**
14: $bit \leftarrow samplesToBitManchester(\leftarrow samples, windowsPerBit)$
15: $output(bit)$
16: **end while**
17: **end while**

TABLE II
Ethernet cables used for the evaluation

#	Color	Type
cable-1	White	CAT 5e UTP
cable-2	Blue	CAT 6A S/FTP
cable-3	Green	CAT 6A U/FTP

A. Experimental Setup

1) Receivers: For the reception we used two types of software-defined radio (SDR) receivers, as specified in Table III. The R820T2 RTL-SDR is capable of sampling up to 16bit at narrow band and has RF coverage from 30 MHz to 1.8 GHz or more. The HackRF device has 1 MHz to 6 GHz operating frequency and 8-bit quadrature samples (8-bit I and 8-bit Q). Both receivers are compatible with GNU Radio, SDR#, and others. We connected the receiver through the USB port to a laptop, with an Intel Core i7-4785T and Ubuntu 16.04.1 4.4.0 OS.

2) Transmitters: For the transmission, we used the three types of off-the-shelf workstations listed in Table IV. The computers are equipped with 10/100/1000 Mbps Gigabit Ethernet card. We tested three types of widely used Cat 5e and Cat 6A Ethernet cables listed in Table V. We also tested a laptop computer and an embedded device (Raspberry Pi) to evaluate the attack on these types of devices.

The following subsections present the results obtained for the two transmission methods.

```
> Frame 167: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: AsrockIn_21:58:06 (70:85:c2:21:58:06), Dst: Giga-Byt_2b:71:40 (fc:aa:14:2b:71:40)
v Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xe284 (57988)
  > Flags: 0x2456, More fragments
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x5a34 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.0.1
    Destination: 10.0.0.2
    Reassembled IPv4 in frame: 171
v Data (1480 bytes)
    Data: 5555555555555555555555555555555555555555555555555...
    [Length: 1480]
```

Fig. 4. The UDP frame generates the electromagnetic emission, as shown in the Wireshark network analyzer.

TABLE III
RECEIVERS USED IN THE EVALUATION

Receiver #	Device	Specs
SDR-1	R820T2 RTL-SDR	Frequency range from 30 MHz to 1.8 GHz
SDR-2	HackRF	Frequency range from 1 MHz to 6 GHz, with software-controlled antenna port power (50 mA at 3.3 V)

TABLE IV
THE WORKSTATIONS USED FOR THE EVALUATION

PC	Hardware	OS
PC1	Lenovo ThinkCentre M93p, Intel Core i7-4785T, 8GiB SODIMM DDR3 Synchronous 1600 MHz NIC: driver e1000e, device I217-LM (rev 04)	Ubuntu 16.04.1 4.4.0-modified
PC2	ASRock X99 Extreme4, Intel Core i7-6900K, 4 * 8GB PC4-1900 DDR4 SDRAM SK Hynix HMA81GU6AFR8N-UH NIC: driver e1000e, device I218-V (rev 05)	Ubuntu 18.04.2 5.0.0-25-generic
PC3	H97M-D3H, Intel Core i7-4790, 4 * 4GB DIMM DDR3 1600MHz Hynix NIC: driver r8169, device RTL8111/8168/8411 (rev 06)	Ubuntu 18.04.1 4.15.0-72-generic
Laptop	Dell 0T6HHJ, Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz 8GB PC4-1900 DDR4 NIC: driver e1000e, device I218-V	Ubuntu 18.04.3 LTS
Embedded	Raspberry Pi 3 Model, Model B	Raspberry Pi OS

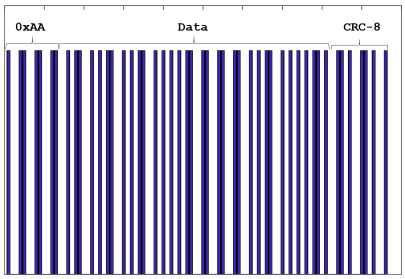

Fig. 5. Transmission of a packet with enable (0xAA), data payload, and CRC-8 code.

B. Ethernet Cables

Table V shows the signal-to-noise ratio (SNR) levels of a transmission generated by toggling the Ethernet interface for different PC with different cables. As can be seen, the signal strength depends on the transmitting computer and the cable used. In this case, PC1 and PC3 with cable-1 and cable-2 yield the most vital signals.

TABLE VI
MAIN FREQUENCY BANDS

	PC	Laptop	Embedded
Frequency	250.000 MHz	249.99488 MHz	250.00285 MHz

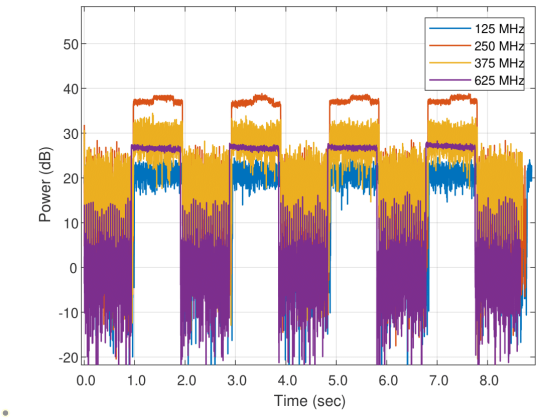

Fig. 6. Harmonics of the signal generated from the PC1.

TABLE V
THE SNR OF DIFFERENT CABLES

	cable-1	cable-2	cable-3
PC1	16.74 dB	6.35 dB	7.55 dB
PC2	1.5 dB	4.75 dB	8.02 dB
PC3	14.125 dB	14 dB	5.49 dB

C. Frequency bands

Our experiments show that the exact frequency band is derived from the type of the transmitting device. Table VI shows the frequency responses for the Ethernet speed toggling method for the PC, laptop, and embedded devices. The base frequency is wrapped around 250 MHz with differences of less than 0.1 MHz between them.

1) Harmonics: There are various harmonics for the main signal. Figure 6 shows the harmonics of the signal generated from PC1. The 250 MHz is the strongest harmonics with 37 dB signal, while the 375 MHz, 125 MHz, and 625 MHz bands yield a weaker signal. In the context of the attack, it implies that it is optimal to calibrate the receiver device to the 250 MHz frequency band.

D. Ethernet Speed Toggling

1) SNR: Table VII shows the SNR values generated by the Ethernet speed toggling for the PC, laptop, and embedded transmitters. As can be seen, the PC and embedded signals were successfully received from a distance of 4m and 4.5m, respectively. The SNR values are decreased from 27 dB to 7 dB in PC and 12 dB to 3 dB in the embedded device. The laptop could generate a weak signal for a maximal distance of 50 cm with an SNR of 8 dB at most.

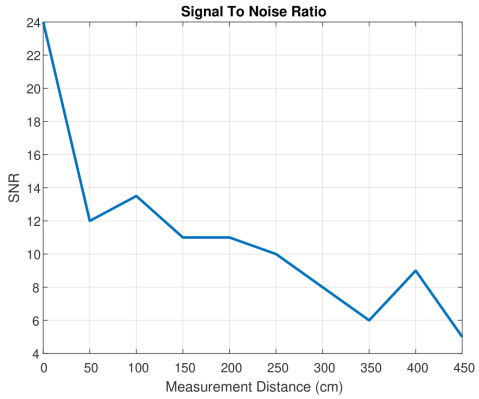

Fig. 7. The SNR levels for the PC with the raw packet transmission method.

2) Speed: Table VIII shows the transition response between link speeds of 10, 100, and 1000 for PC, laptop, and embedded devices. Note that for the Ethernet toggling method, the bit rate is derived directly from the transition time. As can be seen for the PC and laptop transmitters, an average of 4 seconds is required for a transition between different speeds and turning the interface on. However, shutting the interface down takes much less time, with 0.013-0.024 seconds on average. The embedded devices transition is much faster, with an average speed of 0.095-0.017 seconds for the 0-100 Mbps.

E. Raw Packet Transmission

1) SNR: Table VII shows the SNR values generated by the raw packet transmission for the PC, laptop, and embedded transmitters. As can be seen, the signal for the PC was successfully received from a distance of 4.5m. As can be seen in Figure 7 the SNR values are decreased from 24 dB to 5 dB. The laptop and embedded devices could generate a weak signal for maximal distances of 1m and 1.5m, respectively, with SNR values of 4.77 dB and 8 dB at most.

2) Speed: Tables X, XI and XII show the bit error rates (BER) for PC, laptop, and embedded devices, respectively, with the raw packets transmission method. for the PC, transmission rates of 1 bit/sec and 5 bit/sec maintained 0% errors up to a distance of 3m. With a transmission rate of 10 bit/sec we maintained 12.5% errors up to a distance of 3m. For the embedded device, transmission rates of 1 bit/sec and 5 bit/sec maintained 0% errors up to a distance of 3.5m. However, we maintained 0% errors to a distance of 1m only for a transmission rate of 1 bit/sec with a laptop. With transmission rates of 5 bit/sec and 10 bit/sec, we could reach short 1m and 0.5m distances, respectively.

F. Virtual Machines (VMs)

We examined whether the covert channel could be launched from within virtual machines. Since virtualization has become a standard in many IT environments today, the malicious code would likely run in guest OS. One of the properties of visualization technologies is the isolation of hardware resources. Hypervisors/virtual machine monitors (VMMs) provide a layer

TABLE VII
SNR OF THE ETHERNET SPEED TOGGLING

	0 cm	50 cm	100 cm	150 cm	200 cm	250 cm	300 cm	350 cm	400 cm	450 cm
PC	27 dB	15 dB	18 dB	14 dB	13 dB	7 dB	7 dB	6 dB	7 dB	-
Laptop	8 dB	2.6 dB	-	-	-	-	-	-	-	-
Embedded	12 dB	6.5 dB	6 dB	7 dB	5.5 dB	5 dB	5 dB	4.5 dB	3 dB	3 dB

TABLE VIII
TIMING MEASUREMENTS OF THE ETHERNET SPEED TOGGLING

	0-10 Mbps (up/down)	0-100 Mbps (up/down)	0-1000 Mbps (up/down)	10-100 Mbps (up/down)	100-1000 Mbps (up/down)
PC	4 sec / 0.013 sec	4 sec / 0.013 sec sec	4-6 sec / 0.013 sec	4 sec / 4 sec	4 sec / 4 sec
Laptop	4 sec / 0.02 sec	4 sec / 0.024 sec sec	4 sec / 0.024 sec	4 sec / 4 sec	4 sec / 4 sec sec
Embedded	0.095 sec / 0.17 sec	0.095 sec / 0.17 sec	-	0.081 sec / 0.072 sec	-

TABLE IX
SNR OF THE RAW PACKET TRANSMISSION

	0 cm	50 cm	100 cm	150 cm	200 cm	250 cm	300 cm	350 cm	400 cm	450 cm
PC	24 dB	12 dB	13.5 dB	11 dB	11 dB	10 dB	8 dB	6 dB	9 dB	5 dB
Laptop	5.5 dB	5 dB	4.77 dB	-	-	-	-	-	-	-
Embedded	20 dB	11 dB	10 dB	8 dB	-	-	-	-	-	-

TABLE X
BER FOR THE PC, WITH THE RAW PACKETS TRANSMISSION

	0 cm	50 cm	100 cm	200 cm	300 cm
1 bit/sec	0% (no errors)	0% (no errors)	0% (no errors)	0% (no errors)	0% (no errors)
5 bit/sec	0% (no errors)	0% (no errors)	0% (no errors)	0% (no errors)	0% (no errors)
10 bit/sec	0% (no errors)	0% (no errors)	12.5%	12.5%	12.5%

TABLE XI
BER FOR THE LAPTOP, WITH THE RAW PACKETS TRANSMISSION

	0 cm	50 cm	100 cm
1 bit/sec	0% (no errors)	0% (no errors)	0% (no errors)
5 bit/sec	0% (no errors)	0% (no errors)	12.5%
10 bit/sec	0% (no errors)	12.5%	37.5%

of abstraction between the virtual machine and the physical hardware, including the network interface card. The architecture of virtual machine networking uses the concept of virtual network adapters. A virtual network adapter is maintained by the hypervisor and exposed to the guest via kernel drivers. In the context of our covert channel, there is two common networking configurations for virtual machines:

- NAT mode. In this mode, the guest OS on a VM communicates with other hosts in the local area network through a virtual NAT (Network Address Translation). Other workstations and networked devices can be accessed from a guest OS. However, the IP address of the VM is assigned via DHCP, and the external network is exposed only to the IP of the host machine.
- Bridge mode. In this mode, the virtual network adapter is connected to the physical network adapter of the host machine. The network traffic is sent and received directly from/to the real network adapter without encapsulation, modification, or routing.

A process executed in a VM can access the virtual networks cards assigned to the VM. In regard to the covert channel, it implies the malicious code can not disable or change the speed of the *physical* network interface and hence, can not control the electromagnetic emission using the network toggling technique. However, since UDP packets can be delivered to the network, the raw packet transmission technique can still be used in both NAT and bridge modes. We compared the covert channel using a bare-metal machine and VMware VMM in the NAT and bridge modes in PC3. Our experiments show that the covert signals can be maintained from within virtual machines. Figure 8 shows the electromagnetic signals generated using the raw packet transmission with bridged network configurations on bare metal and VMWare workstations. As can be seen, the execution on a bare metal yields a slightly stronger signal than a VM, mainly due to the delay in packet transmission caused by the hypervisor.

G. Evasion

The Ethernet speed toggling method generates strong signals, but it is less evasive than the raw packet transmission. First, it required root privileges to perform the changes to the network interfaces speeds. Technically, it requires the

TABLE XII
BER FOR THE EMBEDDED DEVICE, WITH THE RAW PACKETS TRANSMISSION

	0 cm	50 cm	100 cm	200 cm	300 cm	350 cm
5 bit/sec	0% (no errors)	0% (no errors)	0% (no errors)	0% (no errors)	0% (no errors)	0% (no errors)
10 bit/sec	0% (no errors)	0% (no errors)	0% (no errors)	0% (no errors)	0% (no errors)	0% (no errors)

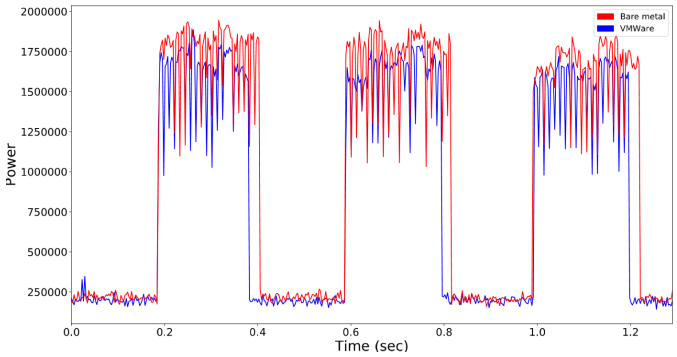

Fig. 8. Signal generated from a bare metal and a WMware virtual machine.

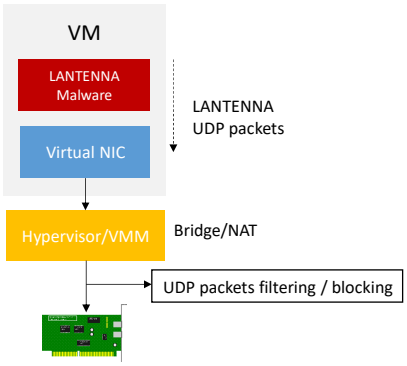

Fig. 9. Hypervisor-level detection and prevention.

process to run in root privileges or exploit a privilege escalation vulnerability. Both techniques can be monitored and detected by modern intrusion detection systems. The raw packet transmission method can be executed as an ordinary user-level process. Transmitting UDP packets doesn't require higher privileges or interfering with the OS routing table. In addition, it is possible to evade detection at the network level by sending the raw UDP traffic within other legitimate UDP traffic.

VIII. COUNTERMEASURES

There are several defensive measures that can be taken against the LANTENNA covert channel.

A. Separation

The NATO telecommunication security standards (e.g., NSTISSAM TEMPEST/2-95 [42]) propose zone separation to protect against TEMPEST (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions) threats and other types of radiated energy attacks. In our case any radio receiver should be banned from the area of air-gapped networks.

B. Detection

For the Ethernet speed toggling method, it is possible to monitor the network interface card link activity at the user and kernel levels. In our case, any change of the link state should trigger an alert. E.g., usage of `ethtool` to modify the interface configuration should be examined. If the interface speed is toggling during a short period of time, the activity will be blocked. However, both user and kernel defensive components can be evaded by sophisticated malware such as rootkits. In addition, the malware may inject a shellcode with a signal generation code into a legitimate, trusted process to bypass the security products. To overcome the evasion techniques, it is possible to deploy solutions at the hypervisor level (Figure 9). In this approach, a hypervisor-level firewall inspects the changes to the network interface and examines the UDP packets from the active virtual machine. Irregular activities are logged, and the outgoing packets are blocked. Using visualization for firewalls and security studied in previous work [12].

C. Signal Monitoring

Another approach is to use RF monitoring hardware equipment to identify anomalies in the LANETNNA frequency bands. However, due to the legitimate activities of local network devices (e.g., UDP traffic) such a detection approach will lead to many false positives.

D. Signal Jamming

It is possible to block the covert channel by jamming the LANTENNA frequency bands. Modern jammers are signal blocking devices with radio frequency (RF) hardware that transmits radio waves in the entire range of the required frequency bands (e.g., the 250 MHz). A jammer generates high power, constant radio transmissions which span the channels and interrupt any covert channel transmissions. Another approach is to generate random traffic which interrupts the possible covert transmission from other devices in the network. In this case, a networked device such as a PC or Raspberry Pi generates UDP traffic at random times and in different volumes.

E. Cable Shielding

Metal shielding is a typical measure used to block or limit electromagnetic fields from interfering with or emanating from the shielded wires. Ethernet cable shielding copes with the threat presented in this paper by limiting the leakage of signals generated by the LANTENNA techniques. Different

TABLE XIII
ETHERNET CABLES SHIELDING CODES. TP = TWISTED PAIR, U = UNSHIELDED, F = FOIL SHIELDED, S = BRAIDED SHIELDING

#	Code	Type of shielding
1	U/UTP	Unshielded cable, unshielded twisted pairs
2	F/UTP	Foil shielded cable, unshielded twisted pairs
3	U/FTP	Unshielded cable, foil shielded twisted pairs
4	S/FTP	Braided shielded cable, foil shielded twisted pairs

techniques can be used for shielding Ethernet cables. The most common is to place a shield around each twisted pair to reduce the general electromagnetic emission and the internal crosstalk between wires. It is possible to increase the protection by placing metal shielding around all the wires in the cable. Table XIII contains the codes used to mark the different types of Ethernet cable shielding.

IX. CONCLUSION

This paper shows that attackers can exploit the Ethernet cables to exfiltrate data from air-gapped networks. Malware installed in a secured workstation, laptop, or embedded device can invoke various network activities that generate electromagnetic emissions from Ethernet cables. We present two methods of signal generation: network speed toggling and UDP packet transmissions. We implemented malware (LANTENNA) and discussed the implementation details of the modulator and demodulator. We evaluated this covert channel in terms of bandwidth and distance and presented a set of countermeasures. Our results show that adversaries can transmit data several meters away from compromised air-gapped networks by using the electromagnetic covert channel. Furthermore, we show that this attack can be launched from an ordinary user-level process without root privileges and works successfully from within virtual machines.

REFERENCES

[1] "Access misconfiguration for customer support database – microsoft security response center," https://msrc-blog.microsoft.com/2020/01/22/access-misconfiguration-for-customer-support-database/, (Accessed on 02/20/2021).

[2] "Agent.btz - wikipedia," https://en.wikipedia.org/wiki/Agent.BTZ, (Accessed on 29/08/2021).

[3] "Chaosdb: Unauthorized privileged access to microsoft azure cosmos db," https://chaosdb.wiz.io/, (Accessed on 09/30/2021).

[4] "May-2018_government-security-classifications-2.pdf," https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf, (Accessed on 10/11/2020).

[5] "Post — dreamlab technologies," https://dreamlab.net/en/blog/post/bypassing-air-gaps-in-ics-systems/, (Accessed on 11/28/2020).

[6] "Protecting data: Cybersecurity theory confirmed by researchers — texas a&m university engineering," https://engineering.tamu.edu/news/2021/08/protecting-data-cybersecurity-theory-confirmed-by-researchers.html, (Accessed on 09/30/2021).

[7] ""red october" diplomatic cyber attacks investigation — securelist," https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/, (Accessed on 06/15/2020).

[8] "Storefront - top secret/sensitive compartmented information data," https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/top-secretsensitive-compartmented-information-data, (Accessed on 29/08/2021).

[9] "The epic turla (snake/uroburos) attacks — virus definition — kaspersky lab," https://www.kaspersky.com/resource-center/threats/epic-turla-snake-malware-attacks, 2018, (Accessed on 29/08/2021).

[10] "A fanny equation: "i am your father, stuxnet" - securelist," https://securelist.com/a-fanny-equation-i-am-your-father-stuxnet/68787/, 2018, (Accessed on 29/08/2021).

[11] P. N. Bahrami, A. Dehghantanha, T. Dargahi, R. M. Parizi, K.-K. R. Choo, and H. H. Javadi, "Cyber kill chain-based taxonomy of advanced persistent threat actors: analogy of tactics, techniques, and procedures," *Journal of Information Processing Systems*, vol. 15, no. 4, pp. 865–889, 2019.

[12] S. N. Brohi, M. A. Bamiah, M. N. Brohi, and R. Kamran, "Identifying and analyzing security threats to virtualized cloud computing infrastructures," in *2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*. IEEE, 2012, pp. 151–155.

[13] T. Carbino and R. Baldwin, "Side channel analysis of ethernet network cable emissions," in *ICCWS2014-9th International Conference on Cyber Warfare & Security: ICCWS 2014*. Academic Conferences Limited, 2014, p. 16.

[14] T. J. Carbino, "Exploitation of unintentional ethernet cable emissions using constellation based-distinct native attribute (cb-dna) fingerprints to enhance network security," 2015.

[15] B. Carrara, "Air-gap covert channels," Ph.D. dissertation, Université d'Ottawa/University of Ottawa, 2016.

[16] B. Carrara and C. Adams, "On acoustic covert channels between air-gapped systems," in *International Symposium on Foundations and Practice of Security*. Springer, 2014, pp. 3–16.

[17] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.

[18] H.-Y. Chen and S.-W. Shiu, "Analysis of radiated fields for the design of a rj45 connector using fdtd method," *IEEE transactions on antennas and propagation*, vol. 56, no. 4, pp. 1041–1047, 2008.

[19] D. Das, "An indian nuclear power plant suffered a cyberattack. here's what you need to know. - the washington post (04/11/2019)," https://www.washingtonpost.com.

[20] K. Eroglu, "A practical comparison of cabling effects on radiated emissions," in *1999 IEEE International Symposium on Electromagnetic Compatability. Symposium Record (Cat. No. 99CH36261)*, vol. 2. IEEE, 1999, pp. 734–738.

[21] D. Genkin, A. Shamir, and E. Tromer, "Rsa key extraction via low-bandwidth acoustic cryptanalysis," in *Annual Cryptology Conference*. Springer, 2014, pp. 444–461.

[22] R. Grant, "The cyber menace," *Air Force Magazine*, vol. 92, no. 3, 2009.

[23] M. Guri, "Cd-leak: Leaking secrets from audioless air-gapped computers using covert acoustic signals from cd/dvd drives," in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2020, pp. 808–816.

[24] ——, "Magneto: Covert channel between air-gapped systems and nearby smartphones via cpu-generated magnetic fields," *Future Generation Computer Systems*, vol. 115, pp. 115 – 125, 2021. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X2030916X

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

[26] M. Guri and Y. Elovici, "Bridgeware: The air-gap malware," *Commun. ACM*, vol. 61, no. 4, pp. 74–82, Mar. 2018. [Online]. Available: http://doi.acm.org/10.1145/3177230

[27] M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, and Y. Elovici, "Gsmem: Data exfiltration from air-gapped computers over gsm frequencies." in *USENIX Security Symposium*, 2015, pp. 849–864.

[28] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici, "Airhopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," in *Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on*. IEEE, 2014, pp. 58–67.

[29] M. Guri, M. Monitz, and Y. Elovici, "Usbee: Air-gap covert-channel via electromagnetic emission from usb," in *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*. IEEE, 2016, pp. 264–268.

[30] ——, "Bridging the air gap between isolated networks and mobile phones in a practical cyber-attack," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 8, no. 4, p. 50, 2017.

[31] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici, "Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations," in *Computer Security Foundations Symposium (CSF), 2015 IEEE 28th*. IEEE, 2015, pp. 276–289.
[32] ——, "Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations," in *Computer Security Foundations Symposium (CSF), 2015 IEEE 28th*. IEEE, 2015, pp. 276–289.
[33] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Acoustic data exfiltration from speakerless air-gapped computers via covert hard-drive noise (diskfiltration)," in *European Symposium on Research in Computer Security*. Springer, 2017, pp. 98–115.
[34] M. Guri, Y. Solewicz, and Y. Elovici, "Fansmitter: Acoustic data exfiltration from air-gapped computers via fans noise," *Computers & Security*, p. 101721, 2020.
[35] M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, "Ctrl-alt-led: Leaking data from air-gapped computers via keyboard leds," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 1. IEEE, 2019, pp. 801–810.
[36] ——, "Powerhammer: Exfiltrating data from air-gapped computers through power lines," *IEEE Transactions on Information Forensics and Security*, 2019.
[37] M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, "xled: Covert data exfiltration from air-gapped networks via switch and router leds," in *2018 16th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2018, pp. 1–12.
[38] M. Guri, B. Zadov, and Y. Elovici, *LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED*. Cham: Springer International Publishing, 2017, pp. 161–184.
[39] ——, *LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED*. Cham: Springer International Publishing, 2017, pp. 161–184.
[40] ——, "Odini: Escaping sensitive data from faraday-caged, air-gapped computers via magnetic fields," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1190–1203, 2019.
[41] M. Hanspach and M. Goetz, "On covert acoustical mesh networks in air," *arXiv preprint arXiv:1406.1213*, 2014.
[42] https://cryptome.org, "Nstissam tempest/2-95," https://cryptome.org/tempest-2-95.htm, 2000, (Accessed on 15/06/2020).
[43] M. G. Kuhn and R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations." in *Information hiding*, vol. 1525. Springer, 1998, pp. 124–142.
[44] M. G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays," Ph.D. dissertation, University of Cambridge, 2002.
[45] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.
[46] J. Loughry and D. A. Umphress, "Information leakage from optical emanations," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 3, pp. 262–289, 2002.
[47] B. Nassi, Y. Pirutin, T. Galor, Y. Elovici, and B. Zadov, "Glowworm attack: Optical tempest sound recovery via a device's power indicator led."
[48] S. Shin and G. Gu, "Conficker and beyond: a large-scale empirical study," in *Proceedings of the 26th Annual Computer Security Applications Conference*, 2010, pp. 151–160.
[49] M. Vuagnoux and S. Pasini, "Compromising electromagnetic emanations of wired and wireless keyboards." in *USENIX security symposium*, 2009, pp. 1–16.
[50] B. B. Yilmaz, M. Prvulovic, and A. Zajić, "Electromagnetic side channel information leakage created by execution of series of instructions in a computer processor," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 776–789, 2019.
[51] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," *IEEE Communications Surveys & Tutorials*, vol. 9, no. 3, pp. 44–57, 2007.