SATAn: Air-Gap Exfiltration Attack via Radio Signals From SATA Cables

Mordechai Guri
Ben-Gurion University of the Negev, Israel
Department of Software and Information Systems Engineering
Cyber-Security Research Center
Email: gurim@post.bgu.ac.il
Demo video: http://www.covertchannels.com

***Abstract*—This paper introduces a new type of attack on isolated, air-gapped workstations. Although air-gap computers have no wireless connectivity, we show that attackers can use the SATA cable as a wireless antenna to transfer radio signals at the 6 GHz frequency band. The Serial ATA (SATA) is a bus interface widely used in modern computers and connects the host bus to mass storage devices such as hard disk drives, optical drives, and solid-state drives. The prevalence of the SATA interface makes this attack highly available to attackers in a wide range of computer systems and IT environments. We discuss related work on this topic and provide technical background. We show the design of the transmitter and receiver and present the implementation of these components. We also demonstrate the attack on different computers and provide the evaluation. The results show that attackers can use the SATA cable to transfer a brief amount of sensitive information from highly secured, air-gap computers wirelessly to a nearby receiver. Furthermore, we show that the attack can operate from user mode, is effective even from inside a Virtual Machine (VM), and can successfully work with other running workloads in the background. Finally, we discuss defense and mitigation techniques for this new air-gap attack.**

***Index Terms*—air-gap, network, exfiltration, electromagnetic, leakage, covert channels, SATA**

I. Introduction

Information is one of the organization's valuable assets in the digital era and, accordingly, is coveted by adversaries. There are many types of threats to the organization's data, including data theft, malware, spyware, ransomware, advanced persistent threats, data leakage, data misuse, etc. Air-gap is a network security measure taken where highly sensitive data is involved, in order to protect the information from cyber attacks or accidental leakage. In this measure, the local area network (LAN), computerized systems, or specific device is maintained in an isolated environment, disconnected from the Internet or other non-secure networks. Air-gap policies are commonly backed up with supporting regulations, such as forbidding Wi-Fi and Bluetooth connections, restricting the use of external media, enforcing access control, and using Anti-Virus (AV) and Endpoint Detection and Response (EDR) products. The air-gapped measure is used in many IT environments, such as military and defense networks, industrial control systems, government agencies, and banking and finance sectors [14].

A. Air-Gap Penetration

But even offline networks, which are completely disconnected from the Internet, can be hacked. It has been proven that motivated and persistent threat actors can breach the air-gap isolation, installing advanced persistent threat (APT) in the network. The most notorious example is the Stuxnet attack from 2010 designed to target nuclear facilities by targeting programmable logic controller (PLC) units [34]. In this case, the attackers targeted Microsoft Windows machines and spread them through USB drives plugged into the air-gapped machines on the network. Since 2010, more than ten new APTs have been reported targeting air-gapped facilities, including ProjectSauron, EZCheese, and USBCulprit [9]. In 2019 security firms reported the Ramsay Advanced Persistent Threat (APT), a cyber-espionage malware that was targeting air-gapped networks. This malware moves data between isolated networks and Internet-connected computers using external USB thumb drives [2]. Such cases prove that the risk is increased because the air-gapped isolation brings a false sense of security that the systems are immune to breaches.

B. Covert Channels

Compromising the air-gapped network is only the first operative phase for an attacker. For espionage purposes, the APT moves to a collection phase, where it gathers different types of information; files, images, keylogging, etc. In the case of Internet-connected networks, APTs commonly use different covert communication channels to hide the data and leak it outward. Over the years, many types of covert channels have been revealed, researched, and analyzed. To evade DLP and monitoring solutions, an attacker may conceal data in ICMP, HTTP(S), DNS, SMTP, and other common protocols [39], [41]. However, because air-gapped networks lack connectivity to the Internet, the attacker must use non-standard ways to exfiltrate data. The air-gap covert channels explored over the years include acoustic, optical, electromagnetic, electric, and other types of physical covert communication techniques [8], [14].

This paper presents a new type of electromagnetic air-gap covert channel. The covert enables attackers to leak data from air-gapped systems using the SATA cable as a transmitting an-

tenna. We present the design and implementation and discuss the evaluation of the covert channel.

C. Paper Organization

This paper is organized as follows. The attack model on air-gapped networks is explained in Section II. Related work is discussed in Section III. Technical background on the SATA interface is given in Section IV. The design, implementation, and algorithms of the transmitter and receiver are described in Section V. Section VI presents the evaluation results. Countermeasures are proposed in Section VII. We conclude in Section VIII.

II. Attack Model

To steal valuable assets such as sensitive information, financial data, and intellectual property, attackers may employ an offensive strategy known as the advanced persistent threat (APT). The life cycle of a modern advanced persistent threat consists of various phases. The main steps are the initial penetration, establishing foothold, lateral movement, data collection, and exfiltration [6].

A. Initial Penetration

In this phase, the attacker breaches the layers of defense and installs malware in the target network. In the case of a standard connected network, this step is commonly performed using social engineering, spear-phishing, zero-day exploits, and malicious web pages. However, when the target network is disconnected from the Internet (air-gapped), an attacker may use complex methods such as supply chain attacks, removable media attacks, malicious insiders, and deceived employees to breach the network [7], [40]. Various advanced cyber attacks targeting air-gapped networks have been publicized since 2010, including Agent.BTZ, Stuxnet, ProjectSauron, Emotional Simian, and USBCulprit and Ramsay [9]. Most of these attacks use removable media, such as USB thumb drives to infect workstations within the air-gapped network. For example, the Agent.btz is a computer worm that breached U.S. military networks via an infected USB drive attached to a computer in the network . Similarly, the Stuxnet malware attacked supervisory control and data acquisition (SCADA) systems in 2010 [32]. In 2020, researchers published technical details on USBCulprit [13] and Ramsay [2], APTs which seems to be designed to reach air-gapped networks.

B. Data Collection

After establishing a foothold in the target network and expanding control to other workstations, servers, and infrastructure, the attack move to the data collection phase. In this phase, various data of interest are gathered and collected. The information may vary from victim to victim and includes files with sensitive information, keylogging, emails, images, keylogging, etc. The attacker may encrypt or hide the data at this stage, concealing it from data leakage prevention (DLP) solutions [38].

C. Data Exfiltration (SATAn)

At some point, the attacker might want to exfiltrate the data. In this stage, the malware locates workstations or servers in the network that contains active SATA interfaces; computers with Hard Disk Drives (HDD), Solid State Drives (SSD), or optical drives such as CD/DVD. The malware then uses a specialized shellcode to maintain file system activity to generate radio signals from the SATA cables. The collected data is modulated, encoded, and transmitted via this covert channel.

D. Data Reception

The exfiltrated information can be received in different ways. A hardware receiver might be hidden on implanted near the air-gapped computer. For example, in 2018, tiny microchips were found hidden inside servers used by Apple, Amazon, and government contractors. According to a report by Bloomberg Businessweek, the chip allows control of the compromised computer [1]. Another way is to have a malicious insider or visitor carry a radio receiver nearby the air-gapped computer, for instance, within a laptop. The receiver monitors the 6 GHz spectrum for a potential transmission, demodulates the data, decodes it, and sends it to the attacker.

Figure 1 shows the demonstration of the covert channel. Sensitive information in an air-gapped workstation (A) is transmitted via radio signals from the SATA cable to a nearby laptop receiver (B). In this case, the word ‘SECRET’ was transmitted.

III. Related Work

The covert channel term, coined in 1973 by Butler Lampson, is defined as communication channels that are not intended for information transfer [33]. Covert communication channels have been explored for many years. Attackers may use legitimate network traffic to conceal and hide data in traditional covert channels. For instance, information may be hidden within TCP headers, HTTPS requests, DNS extra fields, and SMTP messages [39]. The attacker may also use techniques such as stenography and image or video manipulations to hide textual binary data [38].

Air-gap covert channels are special types of covert communication channels that enable attackers to leak data from isolated, air-gapped systems where no standard networking exists. In this domain, the attacker uses physical mediums to modulate information into the air. These methods can be mainly classified into electromagnetic, magnetic, electric, optical, and acoustic [14].

Information can be leaked from network-less systems via electromagnetic waves. In this technique, malware triggers electromagnetic emissions from various computer components such as buses, cables, and processors. Data is modulated on these signals and broadcast to the environment where a potential radio receiver receives the data, process, and demodulate it. Electromagnetic-based channels have been proposed and explored in the covert channels research domain for many years. The AirHopper attack used the video cards in air-gapped computers to generate FM signals modulated with the leaked

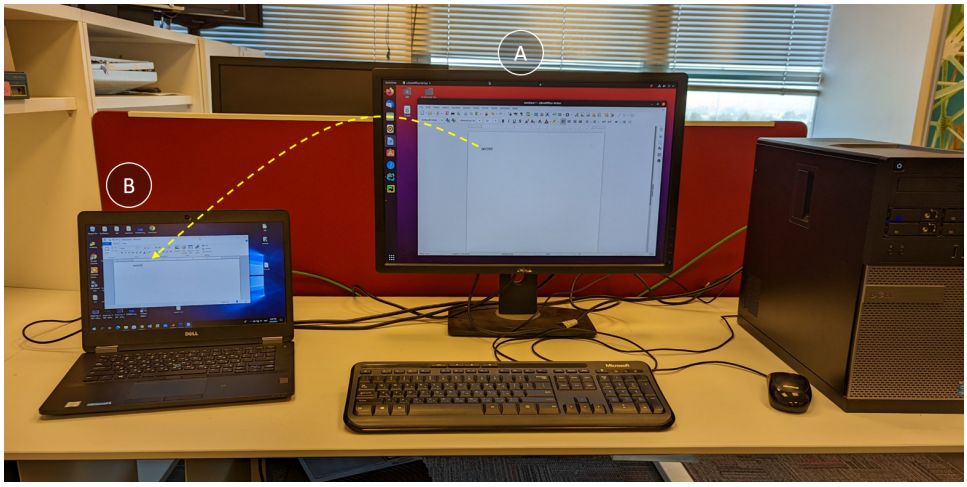

Fig. 1. Demonstration of the SATAn covert channel. A piece of sensitive information in an air-gapped workstation (A) is transmitted via radio signals from the SATA cable to a nearby laptop receiver (B). In this case, the word 'SECRET' was transmitted.

information [17]. The USBee attack used the A Universal Serial Bus (USB) data buses to control electromagnetic waves emanated from the USB and encode binary data over it [18]. Other work such as GSMem [16], BitJabber [47], EMR [45], AIR-FI [10], and CloakLoRa [29] used the memory modules and CPU to generate radio waves from an air-gapped systems for data exfiltration.

Although the electromagnetic-based covert channels can be mitigated with Faraday cages, researchers found a way to bypass them. Guri et al. proposed using magnetic fields to evade Faraday shields and maintaining covert communication to leak data from Faraday caged air-gapped computers to nearby magnetic sensors [5], [11], [26]. PowerHammer is a cyberattack that allows data exfiltration via emission from power supplies emanated to the power lines [24]. Shao et al. proposed using the noise in the power lines for communication [44].

Information can also be leaked from air-gapped systems in optical ways. In general, optical communication is defined as any type of communication in which light is used to carry signals. In the case of covert channels, optical sources in computers are used to carry signals, which are received by remote cameras or photo-detector, which convert light into electricity using the photoelectric effect. Loughry [35] and recently Guri [23] proposed to use the status LEDs of workstation keyboards to encode information. Nassi et al. used lasers and scanners to infiltrate air-gapped networks in the organization [42]. The LEDs in network devices, cameras, and screens [15] were also used for data leakage purposes [25]. Other works such as [19], [37] discuss a thermal covert communication between different computers and cores via the control of heat emission and sensing.

Sound waves, in the audible and non-audible bands, are also used to leak data from air-gapped systems [36]. Managing 'Audio modem' between laptops was proposed by Hanspach et al. Other works extended this method for malicious purposes

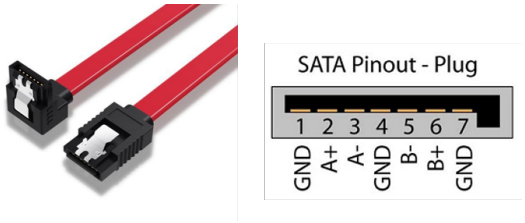

Fig. 2. SATA cable and pinout scheme.

where the attacker uses inaudible frequencies to establish covert mesh networking between laptops or workstations in a room [28] [21]. Researchers also showed that sound (sonic and ultrasonic) could be generated from a system with no audio hardware or speakers. They used various components to synthesize sound such as computer fans [22], HDD drives [20], and power supplies [12].

IV. Technical Background

SATA (Serial Advanced Technology Attachment) is a bus interface for connecting storage devices such as hard disk drives (HDD), Solid State Drives (SSD), and optical drives (CD/DVD) to a computer. SATA offers several advantages compared with the older standards such as PATA, such as larger bandwidths and higher transfer rates.

SATA cables are two side 7-pin cables, consisting of ground (pins 1,4,7), transmit (pins 2,3), and receive pins (pins 5,6) as specified in Table I and Figure 2. The ends are usually made at a 90-degree angle for better cable handling. The cable connects the SATA port on the motherboard and the storage device (e.g., HDD). There are smaller versions of SATA connectors, known as mSATA (mini-SATA), used with smaller computers, laptops, and tablets. The SATA power connector has supplies of +3.3V DC, +5V DC, and +12V DC. SATA power cables that connect the device to the power supply unit (PSU) cables are often paired.

TABLE I
SATA DATA PINOUT

Pin #	Signal Name	Signal Description
1	GND	Ground
2	A+	Transmit +
3	A-	Transmit -
4	GND	Ground
5	B-	Receive -
6	B+	Receive +
7	GND	Ground

TABLE II
SATA I,II,III TRANSFER SPEEDS

Standard	Bandwidth	Data Transfer Speed
SATA I	1.5 Gb/sec	150 MB/sec
SATA II	3 Gb/sec	300 MB/sec
SATA III	6 Gb/sec	600 MB/sec

A. *Transfer Rates*

The SATA standard has three main revisions that determine its bandwidth and data transfer speed, and other characteristics [31]. SATA revision 1.0, released in 2003, has a bandwidth of 1.5 Gbit/s and a data transfer speed of 150 MB/s. SATA revision 2.0, released in 2004, has a bandwidth of 3.0 Gbit/s and a data transfer speed of 300 MB/s. SATA revision 3.0, released in 2008, has a bandwidth of 6.0 Gbit/s and a data transfer speed of 600 MB/s. SATA 3 cables (third-generation SATA cables) are capable of transferring data at six gigabits per second. SATA 3 cables have locking latches on the ends of the cable. The three SATA major revisions, along with the bandwidth and transfer speeds, are presented in Table II.

V. TRANSMISSION AND RECEPTION

In this section, we describe the electromagnetic signal generation and the transmission protocol over the SATA interface.

A. *Signal Generation*

The domain of information security of electromagnetic devices that are the source of unintentional emission induced in the surrounding area is known as TEMPEST [30]. When signals of undesirable emission are correlated with classified or confidential information, they can be used for reconstructing that information by intelligence entities. The phenomenon of such undesirable emissions is also known as the compromising emission threat. In the case of the SATAn covert channel, the attacker intentionally uses the SATA interface to generate and manipulate its electromagnetic emission.

The SATA interface is a rich source of compromising radiated and conducted emission, mainly deriving from its data wires. Previous measurements of the radiated emission of the SATA 1.0 Shows that it spans a frequency range of 100 kHz to 1 GHz during the data transmission. In this work, we used the new SATA 3.0 interface to generate the emission [43]. Notably, previous work shows that the transmitted data can not be intercepted since there is no relation between the *content* of transmitted binary sequences and the compromising emission

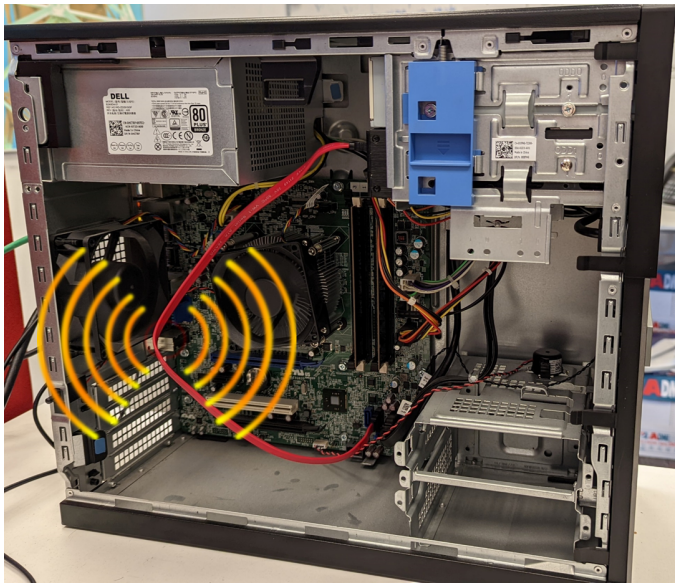

Fig. 3. The SATA cable is used as an antenna to emanate electromagnetic signals (the case is open for the snapshot).

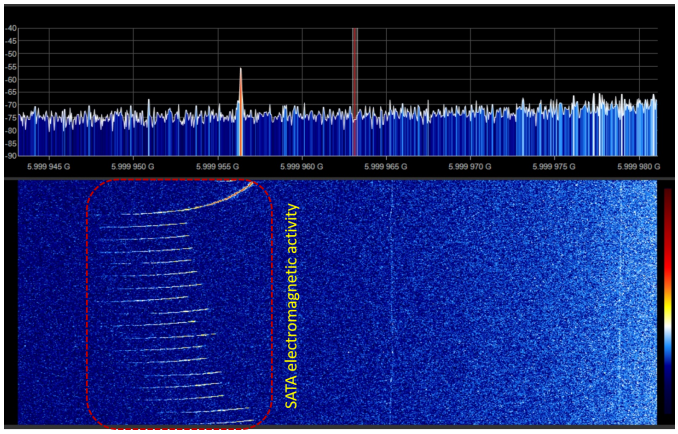

Fig. 4. Electromagnetic emissions around 6 GHz emanated from the SATA interface due to a sequence of reading and writing operations.

signals [43]. Our experiments show a correlation between the bandwidth and data transfer speed and the radiated emission activity on the spectrum. More specifically, in SATA 3.0, the burst throughput of SATA 6.0 Gbit/s can be observed on the electromagnetic spectrum.

Our experiments show that the SATA 3.0 cables emit electromagnetic emissions in various frequency bands; 1 GHz, 2.5 GHz, 3.9 GHz, and +6 GHz. However, the most significant correlation with the data transmission spans from 5.9995 GHz to 5.9996 GHz (Figure 4). The idea behind the covert channel is to use the SATA cable as an antenna and control the electromagnetic emission, as shown in Figure 3.

Algorithm 1 shows the signal generation process. The version of the SATA-TRANSMIT function is generalized and can use both read and write operations of the transmission. The function receives the vector of bits to transmit (data), the

bit-time for reading (T_{read}) and writing (T_{write}) operations, and the percentage of times the read operation will be used from the whole operations (S_{read}). It also receives the time parameters for '0' (T_0) modulation. In the beginning, we disable the cache and buffering delay to make the SATA activity as instant as possible. Note that this might be achieved differently in different operating systems. For example, in the `open()` system call in Linux might receive the O_DIRECT flag, which tries to minimize cache effects of the I/O to and from the file [4]. Other options are to use O_SYNC or `fflush()` commands [3]. The function iterates on bits to transmit and randomize the current operation to perform (read or write) due to the user parameter, for S_{read} and 1-S_{write}. The function reads or writes the data from a file or performs `sleep()` with the corresponding times, according to the current bit.

Algorithm 1 SATA-TRANSMIT (data, T_{read}, T_{write}, S_{read} ,T_0)

```
setNoCache(true)
setNoDelay(true)
for i ← 0 to data.size() do
    bit ← data[i]
    if bit == 1 then
        currentOp ← Random(T_read, T_write, S_read, 1 − S_read)
        if currentOp == read then
            read(datafile, T_read)
        end if
        if currentOp == write then
            open(tmpFile, "w")
            randomData ← randomBuff(1024)
            write(tmpFile, randomData, T_write)
        end if
    end if
    if bit == 0 then
        sleep(T_0)
    end if
end for
```

B. Protocol

Since the electromagnetic-based covert channel is unidirectional, we transmit the data in fixed-length data frames. Each frame begins with four alternating bits '1010' to broadcast the frame preamble. The frame preamble allows potential receivers to sync with the transmission. A 16-bit payload follows the preamble. The final information is a parity bit that is used for elementary error detection.

C. AV Evasion

In order to evade anti-virus (AVs), Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS), the function can be implemented in a separate thread and injected into the memory space of another trusted process in the system. In Windows OS, such techniques are commonly used via the 'CreateRemoteThread', 'WriteProcessMemory', 'LoadLibrary', and similar APIs [46]. The advantage of the approach is that trusted processes in the system are allowed to write or read files in different folders frequently (e.g., temporary folders) without creating anomalies or being reported as suspicious activities (Figure 5).

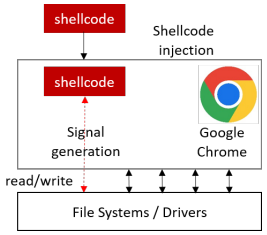

Fig. 5. A signal generation shellcode was injected into the Google Chrome browser for evasion.

D. Receiver

For the evaluation and testing purpose, we implemented the receiver in a MATLAB script. The reeving laptop is connected to a Software Defined Radio receiver and continently samples the output in the 5.9 GHz to 6 GHz frequency band. After performing the raw Fast Fourier Transform (FFT), the preamble is detected, and the payload is extracted. The pseudo-code for payload extraction is outlined in Algorithm 2.

Algorithm 2 SATA-DEMODULATE-FRAME (freq)

```
setFreq(freq)
delta ← 1M
while find(vec,'1010') ≠ true do
    vec+ = GetFFTVec(freq, delta)
end while
T ← preamble[1].time − preamble[0].time
while i < 16 do
    vec = GetWindowedFFTVec(freq, delta, T)
    if find(vec,'1') then
        payload+ = '1'
    else
        payload+ = '0'
    end if
end while
parity ← extractParity()
return(payload, parity)
```

Note that in a real attack scenario, the receiver might be implemented as a process in the nearby computer or embedded in a dedicated hardware receiver.

Figure 6 shows the payload of the text 'SECRET' as transmitted by the covert channel.

VI. Evaluation

In this section, we present an evaluation of the SATAn covert channel. For the experimental setup, we used three off-the-shelf computers listed in Table III. The computers under test have a metal chassis closed during the experiments.

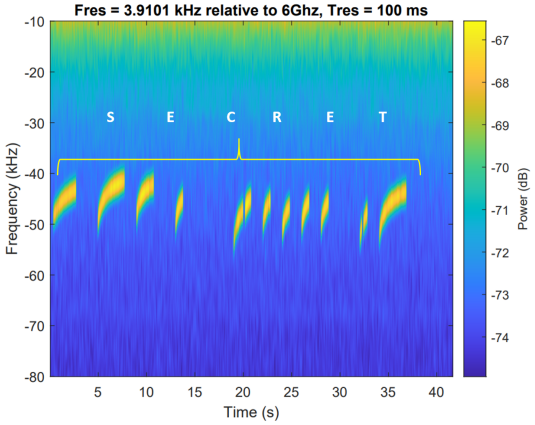

Fig. 6. The payload 'SECRET' transmitted with the SATAn covert channel

TABLE III
EXPERIMENTAL SETUP

#	System	Operating System (OS)
PC-1	i7-4790 DELL 0N4YC8 8GB	Linux Ubuntu 20.04.1 64-bit
PC-2	i7-6900k X99 ASRock 32GB	Linux Ubuntu 20.04.1 64-bit
PC-3	i3-4130 H81M-S2V 4GB	Linux Ubuntu 20.04.1 64-bit

All tested computers had a SATA interface with Transcend 256GB MLC SATA III 6Gb/s 2.5" Solid State Drive 370 and were running Linux Ubuntu 20.04.1 64-bit. As a receiver, we used the ADALM PLUTO Software-defined Radio (SDR) AD9364 RF coverage from 70 MHz to 6 GHz. The SDR was connected through USB to a laptop with Microsoft Windows 10 Enterprise OS, and the output was processed by MathWorks MATLAB reception and demodulation script.

A. Signal to Noise Ratio (SNR)

Table IV presents the signal-to-noise ratio (SNR) received with the three transmitting computers. The signal transmitted from PC-1 has a strength of 20 dB at 30 cm to 9 dB at 120 cm apart. The signal generated from PC-1 and PC-2 were significantly weaker, with 15 dB at 60 cm (PC-2) and 7 dB at 30 cm (PC-3).

B. Bit Times

The timing parameter of the read and write operations T_{read} and T_{write} has a direct effect on the SATA activity, the electromagnetic emission, and the generated signal time. Since we use On-off-keying for modulation, the '1' and '0' times T_1 and T_0 correlate with the read/write operation times.

TABLE IV
SIGNAL TO NOISE RATIO (SNR)

#	30 cm	60 cm	90 cm	120 cm
PC-1	10 dB / 20 dB	7 dB / 15 dB	6 dB / 13 dB	4 dB / 9 dB
PC-2	7 dB / 1 dB	3 dB/ 9 dB	-	-
PC-3	3 dB / 7 dB	-	-	-

TABLE V
BIT TIMES AND THE CORRESPONDING SIGNAL

T	0.2 sec	0.4 sec	0.6 sec	0.8 sec	1.0 sec	1.2 sec
Signal	-72 dBm	-72 dBm	-70 dBm	-70 dBm	-68 dBm	-68 dBm

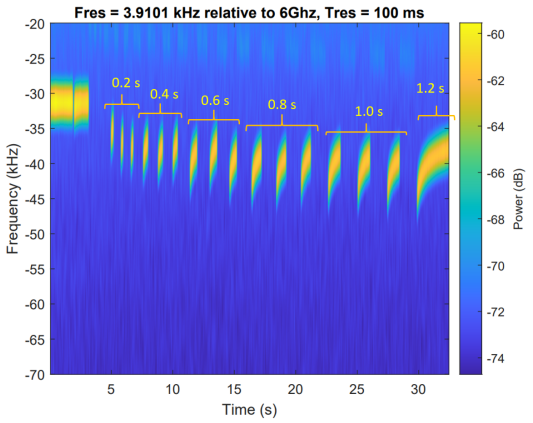

Fig. 7. Signal generated with timing of 0.2, 0.4, 0.6, 0.8, 1.0, and 1.2 seconds.

Figure 7 shows the spectrogram of a bit transmission with different timing parameters. In this case sequences of three bits with 0.2 sec, 0.4 sec, 0.6 sec, 0.8 sec, 1.0 sec, and 1.2 sec have been modulated and received. The SNR levels with the different times are given in Table V.

C. Bit Error Rate (BER)

We transmitted the data with a bit rate of 1 bit/sec, which is shown to be the minimal time to generate a signal which is strong enough for modulation. The BER for PC-1 is presented in Table VI. As can be seen, the BER of 1% - 5% is maintained between 0 - 90 cm. With a greater distance of 120 cm, the BER is significantly higher and reaches 15%. With PC-2 and PC-3, the bit error rates (BER) are less than 5% only in short proximity up to 30 cm, and hence the attack is relevant only for short ranges in these computers.

D. Read vs. Write Operations

The signal can be generated with reading or writing operations and translated into the corresponding ATA read or write commands at the hardware level. Figure 8 presents the signal generated with reading and writing operations, where a sequence of alternating bits was transmitted from PC-1. The results show that read operations yield a signal with an average of 3 dB stronger than write operations. It means that it is preferable to use read operation for the covert channel.

TABLE VI
PC-1 BER

#	30 cm	60 cm	90 cm	120 cm
PC-1	1%	3%	5%	15%

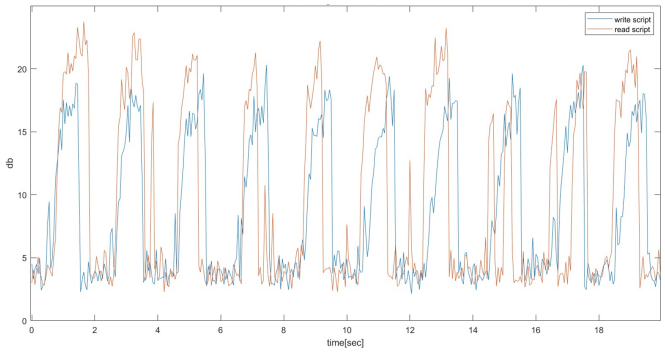

Fig. 8. SNR of read and write operations.

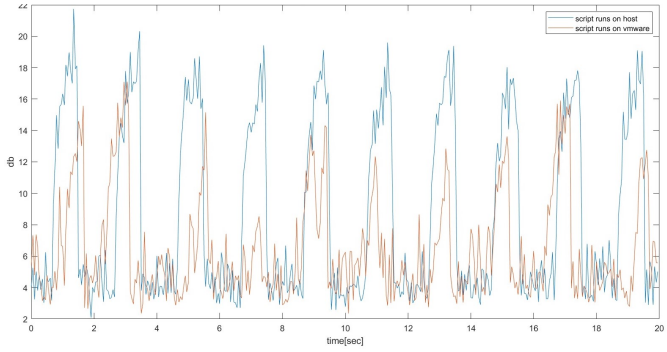

Fig. 9. VMM vs. host signal generation.

TABLE VII
SIGNAL QUALITY WITH DIFFERENT WORKLOAD

#	Activity	Type	SNR
1	Idle	-	15 dB - 20 dB
2	Intensive computation (100% CPU)	CPU-bound	15 dB - 20 dB
3	Intensive RAM activity	CPU-bound	15 dB - 20 dB
4	Word processing application	Interactive	15 dB - 20 dB
5	YouTube video playing	I/O (network)	15 dB - 20 dB
6	Copy files between directories	I/O (disk)	4.5 dB - 5.5 dB

Notably, read operations may require lower permissions than write operations. For example, an application may be permitted to read data or configuration files but might be restricted in writing to them.

E. Background Processes

Background processes in the system are generating electromagnetic emissions due to the internal activity in the controller, buses, and motherboard computers. We checked the effect of typical CPU-bound and I/O-bound workloads on the signal's quality. Table VII presents the different workloads and the SNR measured with these activities. In an idle state where no special processes run in the background, the signal generation yields an SNR of 15 dB - 20 dB. Our test shows that the signal generation in an idle state where no special processes run in the background yield an SNR of 15 dB - 20 dB. Intensive computation and virtual memory operations didn't affect the signal quality and yielded an SNR of 15 dB - 20 dB. The daily workload of an interactive process such as word processing and network bound such as YouTube video playing in Google Chrome web browser didn't affect the signal quality either and yielded an SNR of 15 dB - 20 dB. The intensive disk operations with file transfer cause significant signal degradation to 4.5 dB - 5.5 dB. The above results indicate that the attack can be a maintained event with active workloads on the system, which are CPU and I/O bound. However, the covert channel is rendered less effective when intensive disk activity is involved due to the reduced quality. From the attacker's point of view, where intensive disk activity is detected, the transmission should be halted or postponed to a later time.

F. Virtual Machine (VM)

Virtual Machines (VM) are widely used technology in modern working environments, including in servers, local networks, cloud environments, and personal workstations. The Virtual Machine Monitor (VMM) or hypervisor creates a layer of abstraction where a physical host is virtualized at the hardware of the operating system level, enabling multiple isolated and secure virtualized guests to run on a single physical machine. The VMM usually provides host-level storage virtualization, which logically abstracts the physical storage layer from virtual machines. The VM uses a virtual disk to store its operating system, program files, and other data associated with its activities. Many VMMs, such as Oracle's VirtualBox, Microsoft's Virtual PC, and VMware use a single-file virtual file system to manage the virtual storage device [27]. In the context of our covert channel, it means that the read/write commands are not necessarily sent directly through the SATA interface but may through layers of buffering and caching in the VMM and the host, which may cause a delay or interruption to the generated signal. We tested the signal generation from inside a VMWare VM with the six workloads from table VII. The results show an average reduction of 5 dB in the signal quality in VM compared to the signal generated from the host, as shown in Figure 9. These differences are due to the inconsistent read/write activity in the physical SATA interface when the read/write operations are executed from within a VM.

VII. COUNTERMEASURES

There are different classes of countermeasures for the electromagnetic covert channels. Preventing the initial penetration is the first step that should be taken as a preventive countermeasure. There is a wide range of network security technologies that protect the usability and integrity of a company's infrastructure. To prevent the first phase of the air-gap penetration, multiple layers of security should be used in the network, including firewalls, intrusion detection and prevention systems, network traffic analysis, and access control mechanisms. Policy-based countermeasures might forbid the use of radio receivers in secured facilities or rooms within a certain distance. This approach is also known as 'red/black'

separation and is mentioned by US and NATO standards [30]. Another approach is to use an external RF monitoring system to detect anomalies in the 6 GHz nearby the transmitting computer. However, this approach will likely suffer from false alarms and a low detection rate since any read/write operation would create electromagnetic emission in this range, regardless of the covert channel. In order to detect the signal, the system has to know the specific signal shape and modulation in use, which is less practical from the defender's perspective. It is possible to install a dedicated driver (e.g., filter driver in Windows OS) that detect abnormal read/write operations. In the case of this covert channel, anomalous read and write operations from or to temporary files would trigger alerts. Figure 11 shows our anomaly detection of the covert channel by monitoring the I/O operations per second and the disk utilization of a process. The anomalous pattern of the transmitting process can be clearly observed in the covert channel process (left) compared to a Google Chrome browsing (right). However, its important to note the detection of such dummy operations is highly contextual to the specific process and very challenging in a runtime environment, mainly due to the inability to distinguish between legitimate and malicious operations.

Other preventing types of countermeasure belong to the jamming category. The jamming can be done from the operating system by performing random read and write operations when a suspicious covert channel activity is detected. Algorithm 3 shows the outline of the jammer function SATA-JAM. The function received the parameters for a maximum bit time (T). A random read or write operation is initiated for a random time of (0..T).

Algorithm 3 SATA-JAM (T)

```
for i ← 0 to data.size() do
    tm ← Random(T)
    currentOp ← Random(0.5, 0, 5, read, write)
    if currentOp == read then
        read(datafile, tm)
    end if
    if currentOp == write then
        open(tmpFile, "w")
        randomData ← randomBuff(1024)
        write(tmpFile, randomData, tm)
    end if
end for
```

Figure 10 shows the power of a clean signal and a jammed signal. The signal was jammed for over 20 seconds using the random read and write operations. As observed, the SNR of the jammed signal is significantly reduced to 3.5 dB - 5.5 dB.

As observed in Section VI, the existence of intensive disk operations causes an interruption to the signal generation process and reduces the quality of the signal. However, this solution has a significant drawback of harming the performance of disk and I/O activities in the OS and, in the long term, may cause damage to the storage. The external jamming approach would involve the use of radio signal jammers in the 6 GHz frequency band. However, such devices are expensive and can not be practically deployed on a wide scale.

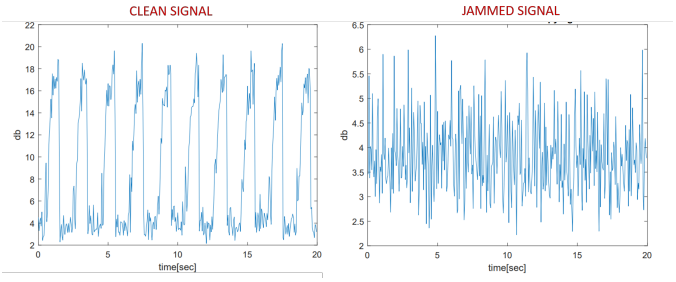

Fig. 10. A clean signal and jammed signal.

VIII. Conclusion

This paper presents SATAn - a new type of attack on air-gapped computers. We show that attackers can exploit the SATA cable as an antenna to transfer radio signals in the 6 GHz frequency band by using non-privileged read() and write() operations. Notably, the SATA interface is highly available to attackers in many computers, devices, and networking environments. We discuss related work and provide technical background. We show the design of the covert channel and present the implementation of the transmitter and receiver. The results show that attackers can use the SATA cable to transfer a brief amount of sensitive information from highly secured, air-gap computers wirelessly to a nearby receiver more than 1m away. We also show that the attack can operate from user mode and is effective even from inside a guest VM. We also discuss preventive and protective countermeasures to this covert channel attack.

References

[1] The big hack: How china used a tiny chip to infiltrate u.s. companies - bloomberg. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies. (Accessed on 09/05/2022).

[2] Eset research discovers cyber espionage framework ramsay — eset. https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-discovers-cyber-espionage-framework-ramsay/. (Accessed on 09/05/2022).

[3] fflush(3) - linux manual page. https://man7.org/linux/man-pages/man3/fflush.3.html. (Accessed on 05/01/2022).

[4] open(2) - linux manual page. https://man7.org/linux/man-pages/man2/open.2.html. (Accessed on 05/01/2022).

[5] Overview of the civilian and military emc norms electronic environment. https://www.electronic.nu/2015/10/05/general-overview-of-the-civilian-and-military-emc-norms/. (Accessed on 09/05/2022).

[6] Michael J Assante and Robert M Lee. The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room*, 1, 2015.

[7] Pooneh Nikkhah Bahrami, Ali Dehghantanha, Tooska Dargahi, Reza M Parizi, Kim-Kwang Raymond Choo, and Hamid HS Javadi. Cyber kill chain-based taxonomy of advanced persistent threat actors: analogy of tactics, techniques, and procedures. *Journal of Information Processing Systems*, 15(4):865–889, 2019.

[8] Brent Carrara. *Air-Gap Covert Channels*. PhD thesis, Université d'Ottawa/University of Ottawa, 2016.

[9] Alexis Dorais-Joncas and Facundo Munõz. Jumping the air gap. 2021.

[10] Mordechai Guri. Exfiltrating data from air-gapped computers via vibrations. *Future Generation Computer Systems*, 122:69–81, 2021.

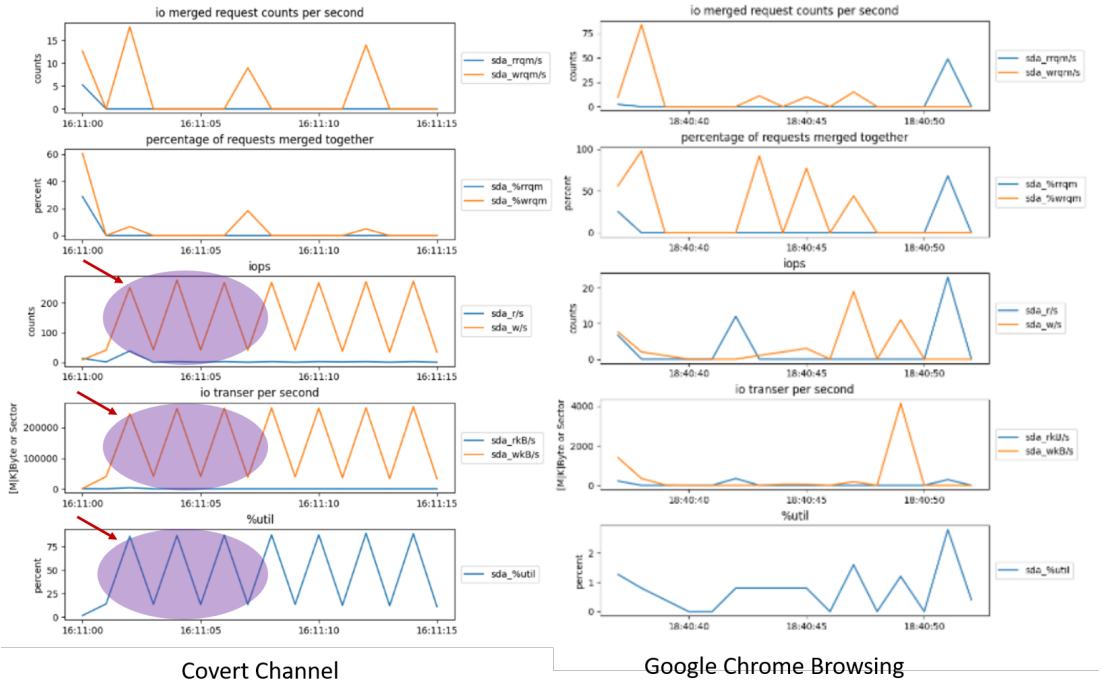

Fig. 11. Detection of the covert channel (left) using measurements of I/O transfer per second and disk utilization over time.

[11] Mordechai Guri. Magneto: Covert channel between air-gapped systems and nearby smartphones via cpu-generated magnetic fields. *Future Generation Computer Systems*, 115:115 – 125, 2021.

[12] Mordechai Guri. Power-supplay: Leaking sensitive data from air-gapped, audio-gapped systems by turning the power supplies into speakers. *IEEE Transactions on Dependable and Secure Computing*, pages 1–1, 2021.

[13] Mordechai Guri. Usbculprit: Usb-borne air-gap malware. In *European Interdisciplinary Cybersecurity Conference*, pages 7–13, 2021.

[14] Mordechai Guri and Yuval Elovici. Bridgeware: The air-gap malware. *Commun. ACM*, 61(4):74–82, March 2018.

[15] Mordechai Guri, Ofer Hasson, Gabi Kedma, and Yuval Elovici. An optical covert-channel to leak data through an air-gap. In *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*, pages 642–649. IEEE, 2016.

[16] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. Gsmem: Data exfiltration from air-gapped computers over gsm frequencies. In *USENIX Security Symposium*, pages 849–864, 2015.

[17] Mordechai Guri, Gabi Kedma, Assaf Kachlon, and Yuval 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*, pages 58–67. IEEE, 2014.

[18] Mordechai Guri, Matan Monitz, and Yuval Elovici. Usbee: Air-gap covert-channel via electromagnetic emission from usb. In *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*, pages 264–268. IEEE, 2016.

[19] Mordechai Guri, Matan Monitz, Yisroel Mirski, and Yuval Elovici. Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations. In *Computer Security Foundations Symposium (CSF), 2015 IEEE 28th*, pages 276–289. IEEE, 2015.

[20] Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, and Yuval Elovici. Acoustic data exfiltration from speakerless air-gapped computers via covert hard-drive noise (diskfiltration). In *European Symposium on Research in Computer Security*, pages 98–115. Springer, 2017.

[21] Mordechai Guri, Yosef Solewicz, and Yuval Elovici. Mosquito: Covert ultrasonic transmissions between two air-gapped computers using speaker-to-speaker communication. In *2018 IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–8. IEEE, 2018.

[22] Mordechai Guri, Yosef Solewicz, and Yuval Elovici. Fansmitter: Acoustic data exfiltration from air-gapped computers via fans noise. *Computers & Security*, page 101721, 2020.

[23] Mordechai Guri, Boris Zadov, Dima Bykhovsky, and Yuval Elovici. Ctrl-alt-led: Leaking data from air-gapped computers via keyboard leds. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, volume 1, pages 801–810. IEEE, 2019.

[24] Mordechai Guri, Boris Zadov, Dima Bykhovsky, and Yuval Elovici. Powerhammer: Exfiltrating data from air-gapped computers through power lines. *IEEE Transactions on Information Forensics and Security*, 2019.

[25] Mordechai Guri, Boris Zadov, and Yuval Elovici. *LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED*, pages 161–184. Springer International Publishing, Cham, 2017.

[26] Mordechai Guri, Boris Zadov, and Yuval Elovici. Odini: Escaping sensitive data from faraday-caged, air-gapped computers via magnetic fields. *IEEE Transactions on Information Forensics and Security*, 15:1190–1203, 2019.

[27] Jacob Gorm Hansen and Eric Jul. Lithium: virtual machine storage for the cloud. In *Proceedings of the 1st ACM symposium on Cloud computing*, pages 15–26, 2010.

[28] Michael Hanspach and Michael Goetz. On covert acoustical mesh networks in air. *arXiv preprint arXiv:1406.1213*, 2014.

[29] N. Hou and Y. Zheng. Cloaklora: A covert channel over lora phy. In *2020 IEEE 28th International Conference on Network Protocols (ICNP)*, pages 1–11, Los Alamitos, CA, USA, oct 2020. IEEE Computer Society.

[30] https://cryptome.org. Nstissam tempest/2-95. https://cryptome.org/tempest-2-95.htm, 2000. (Accessed on 09/05/2022).

[31] Masakazu Kawamoto. Hdd interface technologies. *Fujitsu scientific and technical journal*, 42(1):78–92, 2006.

[32] David Kushner. The real story of stuxnet. *ieee Spectrum*, 3(50):48–53, 2013.

[33] Butler W Lampson. Protection. *ACM SIGOPS Operating Systems Review*, 8(1):18–24, 1974.

[34] Ralph Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3):49–51, 2011.

[35] Joe Loughry and David A Umphress. Information leakage from optical emanations. *ACM Transactions on Information and System Security (TISSEC)*, 5(3):262–289, 2002.

[36] Anil Madhavapeddy, Richard Sharp, David Scott, and Alastair Tse. Audio networking: the forgotten wireless technology. *IEEE Pervasive Computing*, 4(3):55–60, 2005.

[37] Ramya Jayaram Masti, Devendra Rai, Aanjhan Ranganathan, Christian Müller, Lothar Thiele, and Srdjan Capkun. Thermal covert channels on multi-core platforms. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pages 865–880, 2015.

[38] Wojciech Mazurczyk and Luca Caviglione. Information hiding as a challenge for malware detection. *arXiv preprint arXiv:1504.04867*, 2015.

[39] Wojciech Mazurczyk, Steffen Wendzel, Sebastian Zander, Amir Houmansadr, and Krzysztof Szczypiorski. *Information hiding in communication networks: fundamentals, mechanisms, applications, and countermeasures*. John Wiley & Sons, 2016.

[40] Frank E McFadden and Richard D Arnold. Supply chain risk mitigation for it electronics. In *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*, pages 49–55. IEEE, 2010.

[41] Steven J Murdoch and Stephen Lewis. Embedding covert channels into tcp/ip. In *Information hiding*, volume 3727, pages 247–261. Springer, 2005.

[42] Ben Nassi, Adi Shamir, and Yuval Elovici. Xerox day vulnerability. *IEEE Transactions on Information Forensics and Security*, 14(2):415–430, 2018.

[43] Rafał Przesrnvcki, Marek Bugaj, and Marian Wnuk. Sata interface in the process of electromagnetic infiltration. In *2018 2nd URSI Atlantic Radio Science Meeting (AT-RASC)*, pages 1–4. IEEE, 2018.

[44] Zhihui Shao, Mohammad A Islam, and Shaolei Ren. Your noise, my signal: Exploiting switching noise for stealthy data exfiltration from desktop computers. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 4(1):1–39, 2020.

[45] C. Shen, T. Liu, J. Huang, and R. Tan. When lora meets emr: Electromagnetic covert channels can be super resilient. In *2021 2021 IEEE Symposium on Security and Privacy (SP)*, pages 1304–1317, Los Alamitos, CA, USA, may 2021. IEEE Computer Society.

[46] Michael Sikorski and Andrew Honig. *Practical malware analysis: the hands-on guide to dissecting malicious software*. no starch press, 2012.

[47] Z. Zhan, Z. Zhang, and X. Koutsoukos. Bitjabber: The worldâ€™s fastest electromagnetic covert channel. In *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 35–45, Los Alamitos, CA, USA, dec 2020. IEEE Computer Society.