International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT1952109

Air Gap Penetration

Pooja Mudgil *, Abhishek Raj, Anmol Biswas, Ravikant Kumar
Department of Information Technology, Bhagwan Parshuram Institute of Technology, Delhi, India

ABSTRACT

The issue of data security is very paramount for any organization now a day So through this project we will show how an attacker can steal data from the air –gapped channels and also provide some measures in order to protect data from such type of attacks. Now a day attackers can leak data from isolated, air-gapped computers to nearby smart phones via covert magnetic signals. Attacks have been demonstrated on eavesdropping computer displays by utilizing these emissions as a side-channel vector. The accuracy of producing a screen pic depends on the emission sampling rate and bandwidth of the attackers signal hardware. The cost of radio frequency hardware increased with supported frequency range and bandwidth. A number of affordable software defined radio equipment solutions are currently available satisfying a number of radio-focused attacks at a proper price point. This work investigates that the accuracy influencing factors, other than the sample rate and bandwidth, which are noise removal, image blending, and image quality adjustments, that affect the perfection of monitor image reconstruction through electromagnetic side-channel attacks.

Keywords : Air Gap Computers, Electromagnetic Fields, SDR

I. INTRODUCTION

Magnetic sensors (also known as magnetometers) in smart phones and tablets are mainly used for orientation and positioning. Like mobile, Wi-Fi and Bluetooth, magnetic sensors are not considered communication interfaces. Thus, they can be accessed with proper permissions and remain active even in airplane mode, where all wireless networks interfaces are closed.

In this project, we show how attackers can maliciously utilize a smart phone's magnetic sensors in order to ex-filtrate information from isolated, non-networked (air-gapped) computers. In this model, a malware on the air-gapped computer gathers critical data and transmits it via electromagnetic fields generated from the CPU cores. The covert magnetic signals are then received by a smart 9phone located in close proximity to the computer. The data received is decoded and sent to the intruder via the Internet.

An air-gapped network is a protected computer network in which security measures are taken to maintain a separation from public networks such as the internet. Such security measures taken includes distribution of network equipment, using physical access control to systems, banning unauthorized hardware. But above of these restrictions, several incidents in the last decade has shown that air-gapped networks are vulnerable to malwares. For example, In 2017, Wiki Leaks published a reference to a tool dubbed 'Brutal Kangaroo,' allegedly used to infiltrate air-gapped computers via external USB drives . Using such techniques, attackers can breach the network and bypass security measures such intrusion detection and intrusion prevention systems (IDS/IPS). In order to ex-filtrate data from the

compromised air-gapped, networkless, computer, attackers must leak the data through special types of covert channels known as air-gap covert channels. Over the years, several types of air-gap covert channels have been proposed based on electromagnetic, acoustic, optical, and thermal emanations from the computer. In this report, we propose a magnetic covert channel between air-gapped computers (e.g., workstation) and smart phone located nearby. Note that the covert channel requires that malicious code is run on both sides: on the air-gapped computer and the adjacent smart phone.

It has been shown that electromagnetic (EM) emissions from computing devices can be used as a side-channel by third parties for eavesdropping on these devices' activities. The information-leaking EM emissions can occur from components including the CPU, data bus lines, network controllers, and video displays [1]. Depending on the EM source, the information that can be revealed by third parties greatly varies. For example, the CPU executing a segment of instructions which handles data in registers and RAM can modulate information about the individual program instructions and variable values into the EM emission. Meanwhile, data bus lines and network drivers emit EM signals which can hint about the memory contents and the network data. Later works have shown that the threat still prevails in modern computer displays that employ various technologies to transmit video information from the system unit to the display such as VGA, DVI and HDMI [2]. While the principles of reconstructing display images are similar across eavesdropping techniques, the accuracy and the clarity of the image highly depends on the sampling rate and bandwidth of the EM signal acquisition hardware. Existing techniques for computer display eavesdropping in the literature succeeds in constructing the displayed image with a significant accuracy by relying on high sample rates and bandwidth provided by specialized radio frequency (RF) signal acquisition hardware. Such specialized equipment can be prohibitively expensive for many information security professionals. While the sample rate and bandwidth of the signal acquisition hardware have an obvious affect on the image reconstruction accuracy, it is important to investigate any other factors, which may help to improve the process. In order to enable low-cost RF signal acquisition hardware to be used, it is necessary to identify these extra factors and their influence. This work explores several potential avenues that can be utilized to improve the image reconstruction accuracy of electromagnetic side-channel attacks on video displays when the RF signal acquisition hardware does not provide ideal conditions. The contributions of this paper can be summarized as follows: • Evaluation of several approaches to increase the reconstructed image quality and the discussion of their respective pros and cons. The approaches evaluated include noise reduction of RF signals, changing properties of the reconstructed images such as brightness and contrast, and blending multiple reconstructed images together. • Discussion on the challenges associated with image quality enhancement with limited sampling rates, such as image frame misalignments and outlier detection. • Discussion on the possible directions for future improvements of EM side-channel attacks on computer monitors.

II. METHODS AND MATERIAL

In the past twenty years, several studies have proposed the use of electromagnetic emanation from computers for covert communication. In 1998, Kuhn and Anderson showed that attackers can control the electromagnetic emissions from computer displays [3]. Thiele presented a program dubbed 'Tempest for Eliza,' which used the VGA cable to transmit the song 'letter to Alice' played on the AM radio signals. In 2014, Guri et al introduced Air Hopper , malware that can leak data from air-gapped networks to a

nearby smart phone using electromagnetic signals in the FM radio band emanating from the video cable [4]. Guri et al also presented GSMem, malware that leaks data from air-gapped computers using frequencies in the GSM, UMTS, and LTE band emitted from the RAM buses. They used a multi-channel memory architecture to produce an amplified signal, which was received by a malware placed on the firmware of a compromised mobile phone. In 2016, Guri et al demonstrated a method dubbed USB that uses the USB connectors to generate covert electromagnetic signals from PCs.

Attack Model

Throughout the experiments, a monitor is used as the target device. The operating system of the target computer was configured to drive the monitor with a pixel width of 1784 and height of 798 while the frame rate was running approximately at 60 per second. Therefore, the pixel clock frequency of the target device is observed as an EM emission at approximately 85.25Hz. As this fundamental frequency of the EM emission lies in a busy range of the radio spectrum, where FM radio transmissions take place, a harmonic of the signal was used for the eavesdropping attacks which was observed at approximately 346.5MHz. In the experimental setup, a HackRF SDR hardware is used as the RF signal acquisition device [5]. It provides a sample rate up to 20MHz, which is the preferred upper limit of the data sampling rate in these experiments. The SDR device is connected to the attackers computer over a USB port and a small antenna connected to the SDR device is placed closer to the monitor of the target computer, as can be seen in Figure 1. In order to feed I/Q data streams into the experimental setup, a utility program was used, hackrf transfer, which is distributed with the default HackRF tools for the Linux platform [6,7]. The two built-in amplifiers were required to be set to fixed values throughout the experiments in order maintain the internal settings of the SDR device consistent. Setting amplifier values too high causes the noise floor to increase, while setting them too low results in the EM signal going undetected in both cases affecting the signal-to-noise ratio (SNR) required for a successful signal reception. Therefore, suitable values to resolve this issue were decided by trial and-error. The low-noise amplifier (LNA) was set to 24dB while the base-band variable gain amplifier (BB-VGA) was set to 20dB. Figure 4 illustrates the data processing stages of the experimental setup in detail. Handles the configuration settings of the SDR hardware and produces a steam of I/Q data samples that is passed onto the next stage. Even when the EM signal harmonic to be tuned to is carefully selected, it is not possible to completely avoid unnecessary RF signals from getting into the data samples. This is due to the 20MHz bandwidth of HackRF device in which the interested EM signal lies only in a smaller fraction of that spectrum. Therefore, in order to extract only a selected region of the acquired signal spectrum, a band-pass filter is applied which outputs a new I/Q data stream with attenuated signals except the region of interest.

Figure 1: Hardware components of an EM eavesdropping attack on a computer monitor.

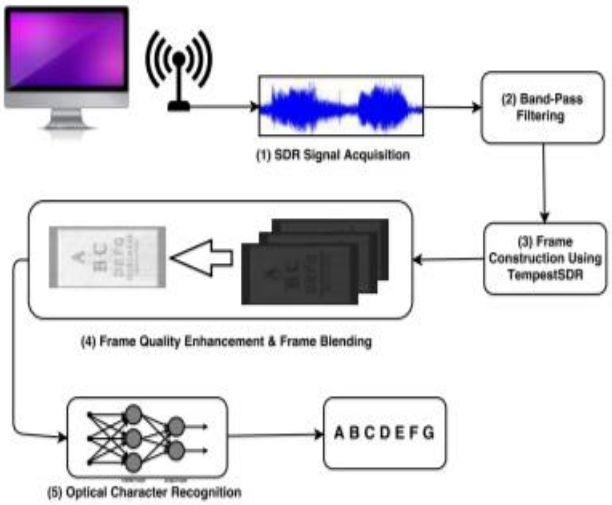


Figure 2: The steps to acquire EM signals, filter EM data, construct display image, feed to the machine learning model, and to classify the screen contents.

At the Black Hat security conference in Weizmann Institute of Science, Amsterdam, Adi Shamir professor of Applied Mathematics and one of the inventors of the RSA algorithm, presented a different technique that can be used to bypass air gap security. He showed that an attacker can transmit data to an isolated computer by flashing a laser at the scanner lid of a multifunctional printer that's connected to the targeted device. This attack can work on longer distances; it has been tested for up to 0.9 miles by researchers. Shamir, who worked on this project with the Ben Gurion University researchers who developed the AirHopper malware, also demonstrated that the light from the same printer's scanner can be utilised for transmission of data from the isolated computer to a receiver. In their experiments, the researchers situated a quadcopter at the window of the office in which the printer was located to take possession the data.

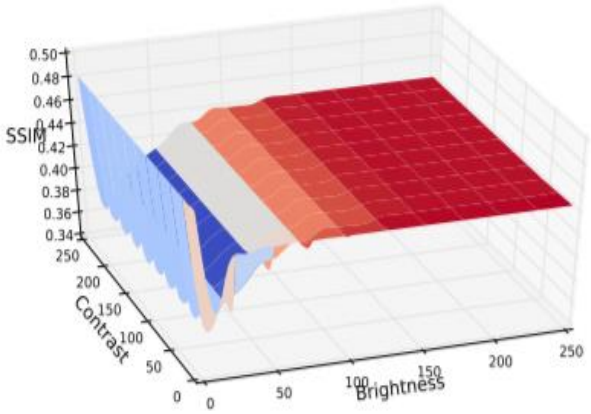
MOSQUITO, the new technique, discovered by a team of researchers at Israel's Ben Gurion University, works by reversing connected speakers (passive speakers, headphones, or earphones) into microphones by exploiting a specific audio chip feature. Before, the same team of researchers showed how attackers could secretly listen to private conversations in one's room just by reversing the headphones (connected to the compromised computer) into a microphone, as like a virus listening device [8].

III. RESULTS AND DISCUSSION

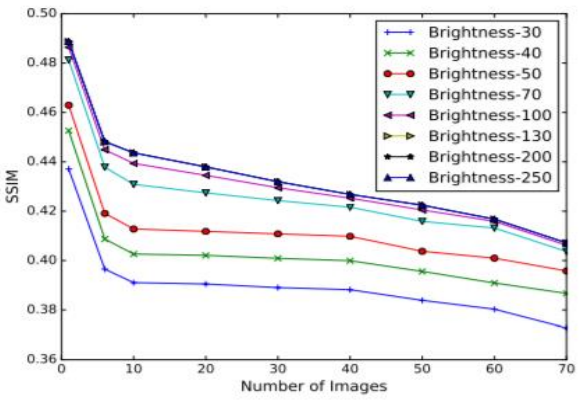
From the following data it can be observed that-

1. Variation of SSIM index with brightness and contrast of the captured images before blending to create a resulting image A brightness threeshold of 130 is evident in this graph.
2. Variation of SSIM with the number of images blended together.
3. A checkerboard pattern displayed on a computer screen is captured using the experimental setup with a sample rate of 10MHZ.

*Refer to Graph 1, Graph 2 and Figure 3.



Graph 1



Graph 2

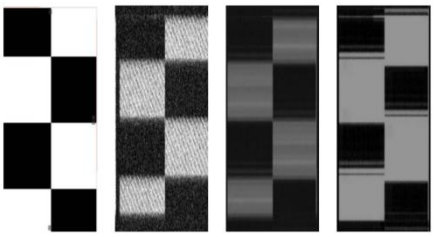


Figure 3

IV.CONCLUSION

This work focused on the issue of achieving successful EM side channel eavesdropping attacks on computer monitors using SDR hardware. Previous work has shown that the sample rate of EM signal acquisition is the largest contributing factor to the clarity of the reconstructed images. However, the unavailability of sophisticated hardware with extremely fast sample rates such as 500MHz limits the capability of successful image reconstruction. This work explored some of the available workarounds to make successful EM side-channel eavesdropping attacks to monitors with hardware capable of sampling at as lower rates as 20MHz.

Through empirical studies, it was revealed that when using SDR devices with wide bandwidths to acquire EM emissions from computer displays, it is necessary to extract the narrow band of frequencies emitted from the target carefully avoiding external noise sources including other computer monitors. A precisely designed band-pass filter can improve the image reconstruction significantly. Furthermore, proper adjustments to the reconstructed image quality have improved the recognizability of screen contents, such as text and shapes, as revealed through the SSIM index-based comparisons. It was revealed that even though blending similar images together is a well known method to increase the clarity of an image, the slight misalignments in the EM side-channel based eavesdropped images causes the technique to fail unless the maligned image frames are manually removed from the image data set. Algorithms to automatically detect and fix such issues are required in order to go further on that direction.

V. REFERENCES

[1]. Furkan Elibol, Uğur Sarac, and Işin Erer. 2012. Realistic Eavesdropping Attacks on Computer Displays with Low-cost and Mobile Receiver System.. IEEE, 1767–1771.

[2]. Robin Getz and Bob Moeckel. 1996. Understanding and eliminating EMI in Microcontroller Applications. National Semiconductor (1996).

[3]. Yu-ichi Hayashi. 2016. State-of-the-art Research on Electromagnetic Information Security. Radio Science 51, 7 (2016), 1213–1219. https://www.cl.cam.ac.uk/teaching/0910/R08/work/essay-ykrt2-videorf.pdf

[4]. Markus Guenther Kuhn. 2002. Compromising Emanations: Eavesdropping Risks of Computer Displays. Ph.D. Dissertation, University of Cambridge. https://www.markscanlon.co/papers/EMAttacksComputerMonitors.pdf

[5]. Martin Marinov 2018. TempestSDR Remote Video Eavesdropping using a Software-defined Radio Platform. (2018). https://github.com/martinmarinov/TempestSDR, Last accessed on 2018-02-01.

[6]. Samuel Joseph O'Malley and Kim-Kwang Raymond Choo. 2014. Association for Information Systems.

[7]. Michael Ossmann. 2016. Software Defined Radio with HackRF. Great Scott Gadgets, https://greatscottgadgets. com/sdr (2016).

[8]. https://www.scmagazineuk.com/does-mosquito-air-gapped-computer-exploit-lack-real-world-bite/article/1473054

Cite this article as :

Pooja Mudgil, Abhishek Raj, Anmol Biswas, Ravikant Kumar, "Air Gap Penetration", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 437-442, March-April 2019. Available at doi : https://doi.org/10.32628/CSEIT1952109
Journal URL : http://ijsrcseit.com/CSEIT1952109