Investigation of Radio Frequency Retroreflector Attacks

A Thesis Submitted to the Department of Computer Science and Communications Engineering,
the Graduate School of Fundamental Science and Engineering of Waseda University
in Partial Fulfillment of the Requirements for the Degree of Master of Engineering

Submission Date: February 1st, 2019

Satohiro Wakabayashi
(5117F100-2)
Advisor: Prof. Shigeki Goto
Resarch guidance: Resarched on Information Systems

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Radio Frequency Retroreflector Attack

Electromagnetic side-channel attacks are attacks performed by passively measuring the electromagnetic emanation originating from a target device. An attacker can reconstruct the original signal by analyzing the measured radio wave. Although there have been many studies on *passive* electromagnetic side-channel attacks [1, 2, 3, 4], few works have been performed on *active* electromagnetic side-channel attacks [5, 6]. In [5], Anderson mentioned that some of these methods were already known to the intelligence community; in particular, he mentioned the reports that the CIA uses software-based radio frequency (RF) exploits in economic espionage against certain European countries.

The NSA advanced network technology (ANT) catalog [7] is a classified document that lists several surveillance technologies used by the United States National Security Agency (NSA). The catalog was included in the series of documents leaked by Edward Snowden in December 2013. Among the technologies listed in the catalog, the technology called ANGRYNEIGHBOR and its variants are attack methods based on the principle of the *RF retroreflector attack* (*RFRA*), which is an active electromagnetic side-channel attack. An attacker actively irradiates the target device with a radio wave at a resonant frequency and passively monitors the reflected radio wave from the target device. As the attacker has embedded a malicious circuit (retroreflector) into the target device, the reflected wave is modulated by the target signal, and the attacker can read the target signal from the reflected wave. It is noteworthy that there was an ancestor of ANGRYNEIGHBOR, called “The Thing” [8], which is a technique to transmit an audio signal by making use of electromagnetic energy taken from an outside source. The technique had been used for intelligence activity in the mid-twentieth century.

After the NSA ANT catalog was leaked, several researchers have started to recreate the surveillance tools using opensource hardware and software [9, 10]. In DEF CON 22 [11], Michael Ossmann successfully demonstrated that RFRA could be implemented with an off-the-shelf SDR (HackRF One) and a simple RF retroreflector, and an attacker can read the keystroke remotely by applying the attack to a PS/2 keyboard. The efforts are fully described in one of the NSA Playset projects [9]. A researcher from the Green Bay Professional Packet Radio (GBPPR) [10] also demonstrated that RFRA could be implemented with their radio wave devices [12, 13].

1.2 The purpose of this study

Although the prior works have successfully demonstrated the threat of RFRA, success conditions have not been revealed. Given this background in mind, we aim to answer the following simple research question:

RQ "*Is the RFRA a feasible attack?*"

To answer this question, we adopt a systematical approach. We first create a simple RF retroreflector that is made from a coaxial cable. We embed a field-effect transistor (FET) chip in the cable and make its woven copper shield work as a dipole antenna. This setup can be seen as a generic form of an RF retroreflector. We then generate electric waveforms in the retroreflector using a function generator connected to it. Using SDR equipment, we irradiate the retroreflector with a radio wave at a resonant frequency of the reflector's antenna and analyze the reflected radio wave from the reflector. Finally, we embed a reflector into a USB keyboard cable and test whether typed key inputs can be reverted from the observed signals of a reflected radio wave.

The key findings we derived from the field experiments with an off-the-shelf SDR (USRP N210) and a laptop PC are summarized as follows:

- RFRA succeeded with the distance of 10 meters between an attacker and a target device.
- RFRA successfully read the internal signal of 10 Mbps, which was roughly half of the maximum rate of the SDR processing capability.
- RFRA successfully read what key was pressed on an RFRA-installed USB keyboard, which is connected with the low-speed mode (1.5 Mbps).

These findings suggest that the RFRA threat is real, and we need to develop effective countermeasures against it. Through our experiments, we conjecture that an attacker equipped with a hardware device instead of SDR will be able to target a higher frequency of internal signals, e.g., USB high-speed. We note that the total amount of our setup was USD 5,000, which would be affordable for non-professional attackers.

I delivered this research as some papers [14, 15, 16]. Particularly, [14] was awarded as Best Student Paper at WOOT '18. Also [16] was awarded as Student Paper Award.

Chapter 2

RFRA Mechanism

In this chapter, we briefly describe the mechanism of RFRA. The core of an RFRA lies in the retroreflector embedded into a *target* device. Figure 2.1 shows the structure of a retroreflector, which includes an FET chip and a dipole antenna. Figure 2.2 presents its actual implementation using a coaxial cable, where the gate of the FET is attached to the copper core, and the source and drain of the FET are connected to a woven copper shield, which works as a dipole antenna. The victim's *target* signal will go through the copper core, which is received by the gate of FET.

As shown in Figure 2.3, an attacker irradiates radio waves to the circuit and attempts to analyze the reflected radio wave, which is AM-modulated with the *target* signal. Let's see why the reflected radio wave is AM-modulated with the target signal. First, the current is induced when the dipole antenna receives the carrier wave, which is transmitted by an attacker. The FET controls the induced current proportionally to the voltage of the target signal applied to the gate. Therefore, the generated current on the antenna becomes an AM signal modulated by the target signal. The dipole antenna radiates radio waves according to the AM signal.

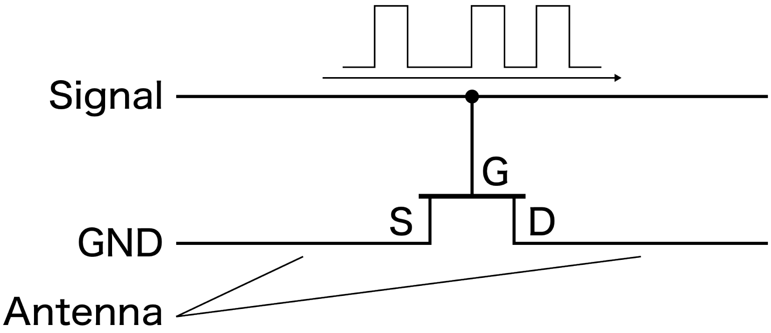

Figure 2.1: A RF retroreflector that includes a FET chip and a dipole antenna.

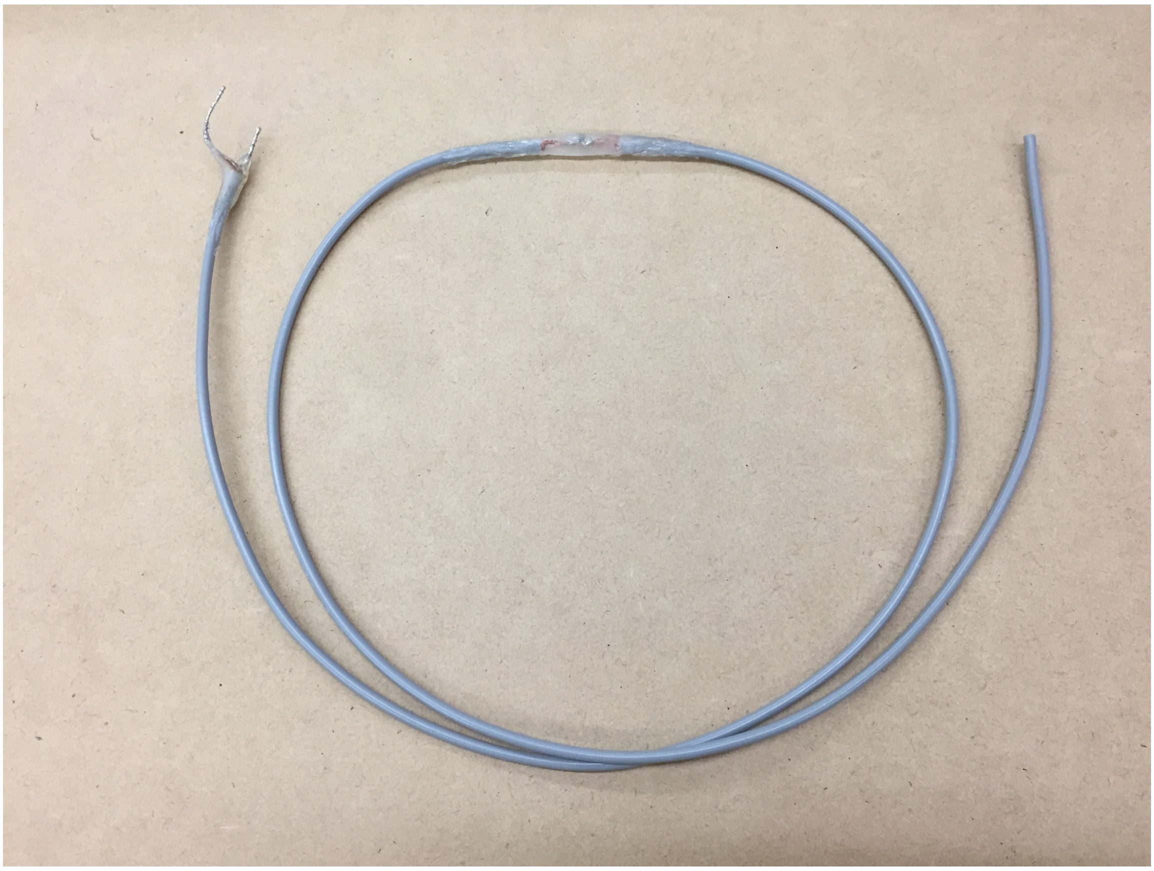

Figure 2.2: An implementation of the RF retroreflector using a coaxial cable.

Finally, the attacker will demodulate the AM signal to revert the original target signal.

We note that the resonant frequency is determined by the length of dipole antenna; i.e., when any odd multiple of half wavelength equals to the length of antenna. In our experiments, the length of the dipole antenna was set to 1 m, which corresponds to the resonant frequency of 599.6 MHz. However, this assumes that the shape of the target is linear. Actually, the resonance frequency varies depending on the shape of the target and also varies depending on the circuit of the device connected to the target. Therefore, it is difficult to calculate and predict the resonance frequency, and it is necessary to find the resonance frequency by changing the frequency of the radio wave to be irradiated.

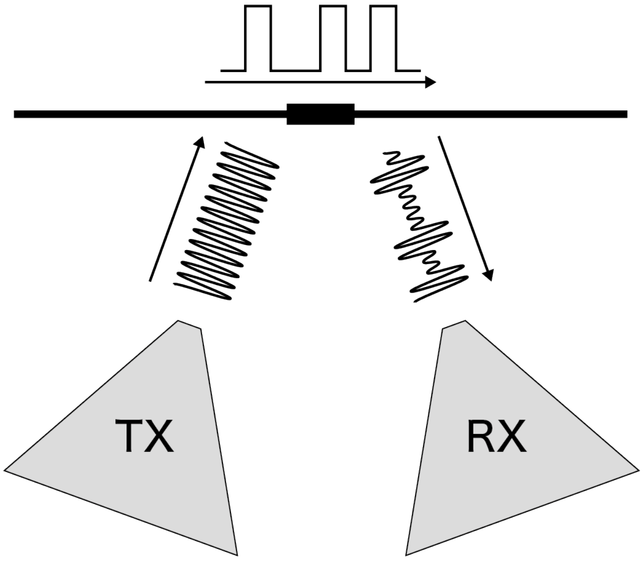

Figure 2.3: Overview of an RFRA attack.

Chapter 3

Feasibility of the RFRA

In this chapter, we study the feasibility of the RFRA using a generic implementation, which consists of a MOSFET chip and a 1 m coaxial cable. We evaluate the feasibility from the viewpoints of the distance to the target and the frequency of the target signal.

3.1 Design of the experiment

Figure 3.1 represents the experimental setup. The RF reflector is connected to a function generator that generates the target's signal. Two directional antennas are connected to an SDR (USRP). The antennas and the target reflector are placed on cardboard boxes at controlled distances. The reflector's antenna cable is set up straightened. Table 3.1 summarizes the instruments used in our experiments, and Table 3.2 lists the software and specs of the PC used for the SDR.

Table 3.1: Instruments used in the experiments.

Instrument	Model
Antenna	Ettus Research LP0410
Software Radio Peripheral (USRP)	USRP N210
Function generator	AFG3102
Oscilloscope	MSO4054
Attacker PC	ASUS ROG G752VS
FET (attached to the target)	ATF-54143

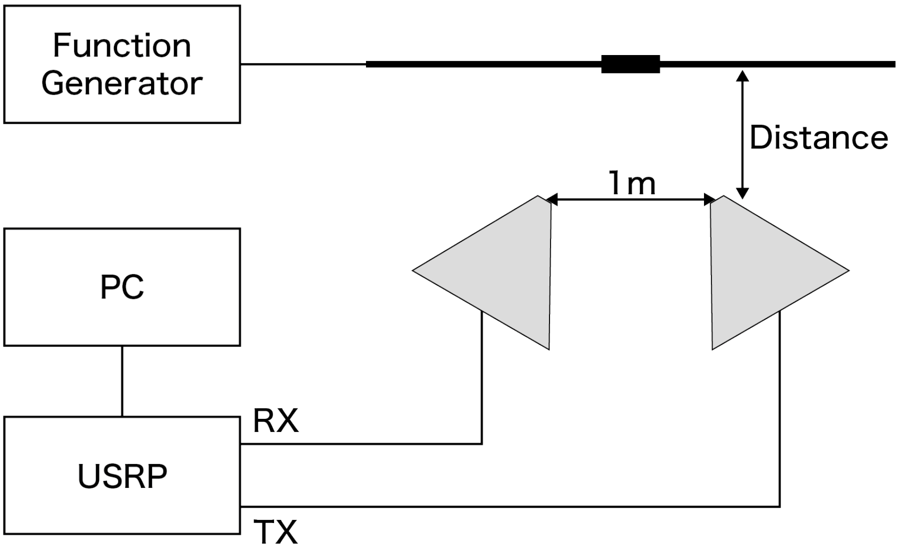

Figure 3.1: Experimental setup (overview).

Table 3.2: List of software and PC used for SDR.

OS	Windows 10
SDR software toolkit	GNU Radio 3.7.11
CPU	Core i7 7700HQ 2.8GHz/4 Core
RAM	32GB

3.2 Distance between the attacker and the target

We first investigate the effective range of an RFRA. To this end, we change the distance between the TX/RX antennas (on the attacker's side) and the reflector. The power of the irradiated radio waves is set to the maximum intensity of the USRP. The frequency of the irradiated waves ranges from 590 MHz to 680 MHz, which roughly corresponds to the resonant frequency of the target's antenna[1]. We let the target signal be a digital signal that repeats the 10-bits pattern "1101010010." The voltage of the signal is set to 3 Vpp. The transmission rate of the target signal is set to 2 Mbps, and the sampling rate of the USRP is set to 10 MS/s.

Figure 3.2 shows the measured waveforms for distances of 1 m, 3 m, 5 m, 7 m, 10 m, and 11 m. '0's and '1's present the decoded bits. The numbers shown above/below the middle line indicate the correctly/incorrectly estimated bits. The attack succeeds when the distance is less than or equal to 10 m. Note that for the case of 10 m, we show the result where 2 of 31

[1] As the actual resonant frequency was sensitive to the placement of the target, we manually adjusted the frequency for each trial.

bits are detected as errors. However, the attack succeeds to read most of the original signals in the 10 m case. At the distance of 11 m, however, we observe no signals (we did not have the way to decode). From these results, we conclude that RFRA is effective within the distance of 10 m, which is long enough to make the attack practical in many scenarios.

3.3 Transmission rate of the target signal

Next, we examine the highest transmission rate of the target signal, at which the RFRA attack is effective. The distance between the antennas and the target reflector is fixed to 1 m. The USRP sampling rate is set to 25 MS/s. The transmission rate of the target signal is set to 1 Mbps, 5 Mbps, 10 Mbps, and 20 Mbps. Figure 3.3 shows the results (the case for 20 Mbps is omitted). The frequency of the irradiated wave is set to 771.2 MHz.

After several trials, we find that RFRA can read signals up to 10 Mbps. USRP N210 has the maximum sampling rate of 25 MS/s[2]. Theoretically, with this sampling rate, it is possible to read a signal below 12.5 MHz, which corresponds to a transmission rate of 25 Mbps. However, the experiment fails to read the 20 Mbps signal. Although not conclusive, we conjecture that this limit is due to hardware performance; i.e., using high-performance hardware can extend the limitation of RFRA. We leave this issue for our future work. We note that the FET chip we used is capable of switching to the 6 GHz frequency.

3.4 Summary

We found that using off-the-shelf equipment, approximately 10 m and 10 Mbps are the limits of the attack. If an attacker can succeed the attack at a distance of 10 m, he/she may have the flexibility in setting up the attack equipment. Also, as we shall present in the next section, the speed of 10 Mbps is practical to attack real applications such as a USB keyboard. These observations support the feasibility of the attack.

We observed that there were several frequency ranges (from 590 MHz to 680 MHz) where attacks succeed. We also observed that the estimated waveforms had reversed from the original waveforms. Currently, we do not have a theory that can explain these observations, which could be affected by multiple factors, such as the EM reflection. Addressing the details of these observations is left for further study.

[2] The sampling rate can be configured up to 50 MS/s with the low dynamic range. However, we could not observe any signals in the low dynamic range.

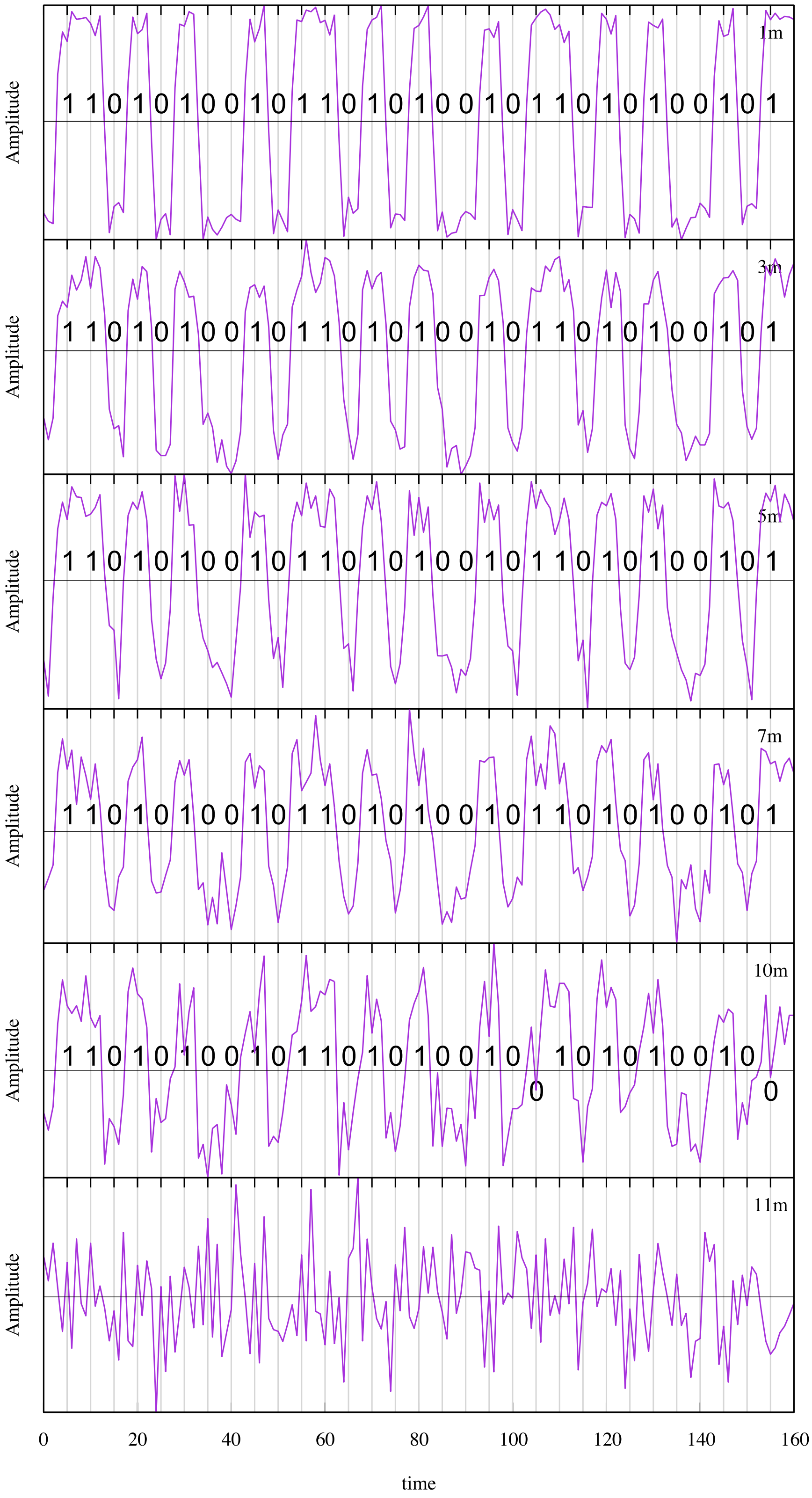

Figure 3.2: Measured signals under different distances between the attacker and the target.

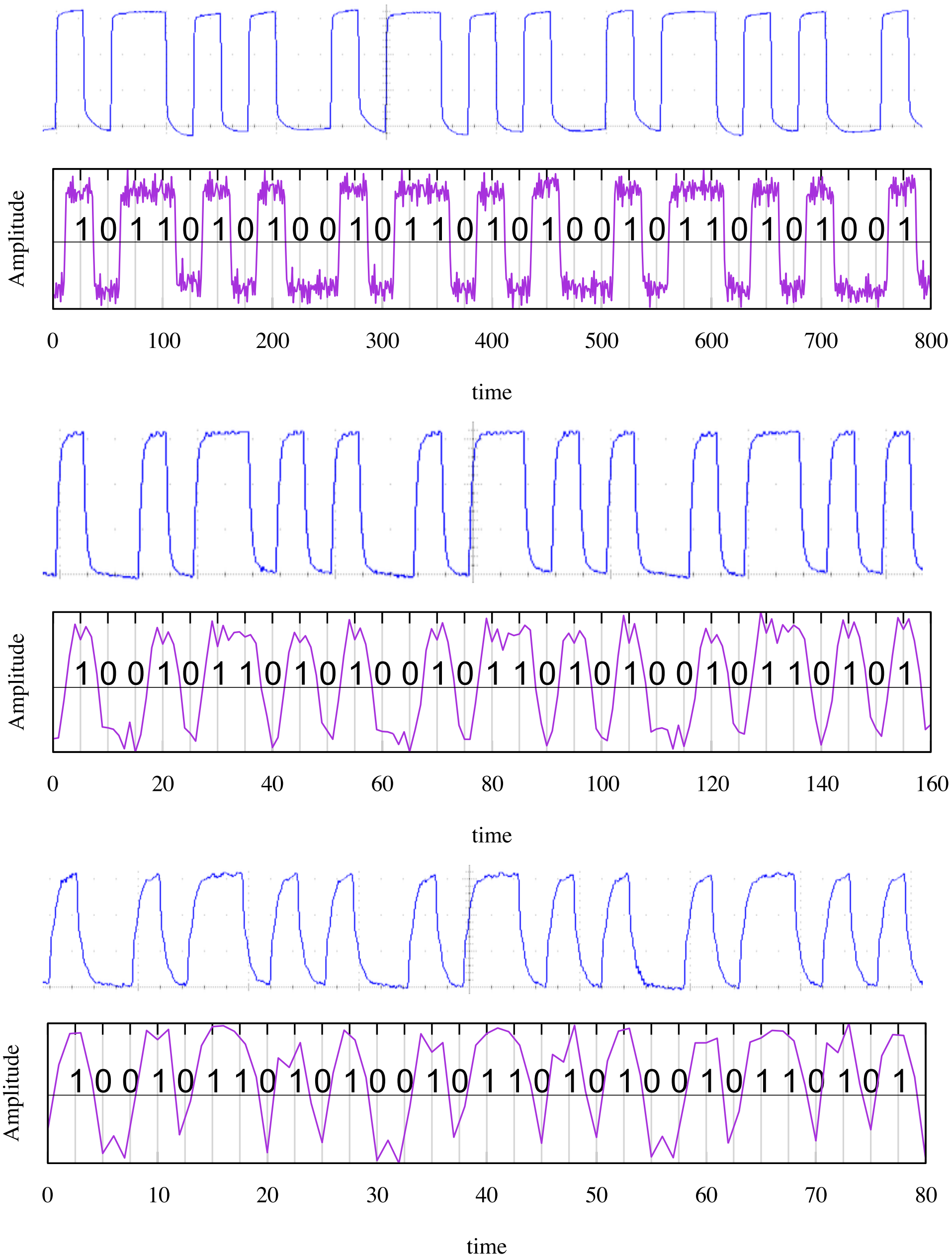

Figure 3.3: Measured waveforms for the target signals with the frequencies of 1 Mbps (top), 5 Mbps (middle), and 10 Mbps (bottom). The upper part of each figure is a waveform measured by oscilloscope.

Chapter 4

Application of RFRA to eavesdrop on USB keyboard

As an actual example of RFRA to a real device, we attacked a USB keyboard and evaluated the attack success rate. As we have shown in Section 3, we have proven that with our setup, RFRA can be applied to devices that operate under 10 Mbps of the data transmission rate. USB is a widely used communication protocol. According to the USB standards, the low-speed mode is used for peripheral equipment such as the keyboard or mouse, and works under the speed of 10 Mbps. As eavesdropping on an input device could lead to the exposure of private, sensitive information, we adopted a USB keyboard as the target of our study. We note that while the experiments shown in the previous section used a simple rectangular waveform, the attack shown in this section makes use of actual USB protocol, which is much more complex than the rectangular waveform. Therefore, it becomes difficult for an attacker to tune the parameters including radio frequency and the direction of antenna; which will lead to the lower attack success rate, compared to the ideal case shown in the previous section.

4.1 Overview of the attack

In this experiment, we typed keys of a USB keyboard and examined how much keystrokes could be eavesdropped upon. We defined the attack success rate as the fraction of the number of characters that were successfully eavesdropped upon over the number of characters typed on the keyboard. We study how the distance between keyboard and SDR affects the attack success rate. For simplicity, we decode the observed signal into key types in an offline manner, not in real-time. USB communication is decoded using Non Return to Zero Inversion (NRZI).

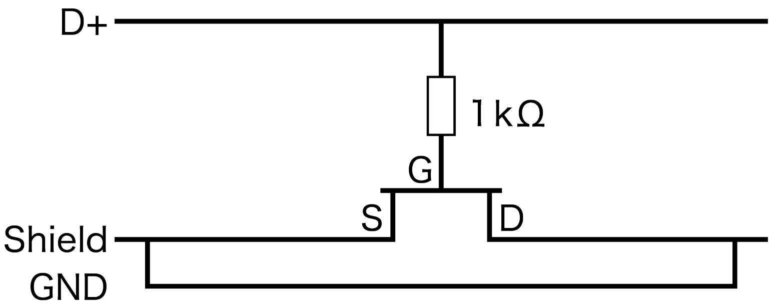

Figure 4.1: A circuit of RFRA embedded into a USB cable.

We developed a program that converts the observed waveform to binary data, and detects keys from the binary data.

4.2 Implementing RFRA on a USB cable

We start by briefly reviewing the specifications of a USB cable. A USB cable consists of four wires and they are shielded [17]. The four wires are denoted as $\mathrm{V_{BUS}}$, D+, D−, and GND, where D+ and D− transmit signals. $\mathrm{V_{BUS}}$ and GND represent power to the bus and ground (earth), respectively. As the two signal lines transmit the differential signals, they transmit mutually inverted waveforms. The differential signal transmission can achieve noise-tolerant data transmission. However, from the viewpoint of eavesdropping, an attacker does not need to obtain signals from both lines because an attacker can achieve her/his objective even when the transmission is noisy and the data is not completely decoded. Thus, we pick one of the two signal lines, D+ or D−, for the target signal and attach an FET chip to that line.

Figure 4.1 presents the circuit of RFRA embedded into an USB cable, where we set D+ as the target signal. We note that if we do not put a resistance between D+ and gate, the negotiation failed and the keyboard did not operate. After placing a resistance of roughly 1kΩ, we observed that the USB communication succeeded. Figure 4.2 presents a photo of the implemented RFRA-enabled USB cable. We use a small circuit board because of ease of implementation. In the real attack, an attacker can implement RFRA using smaller elements in the manufacturing phase of the cable. The RFRA will be completely embedded into a cable and no one will notice the existence of RFRA from outside.

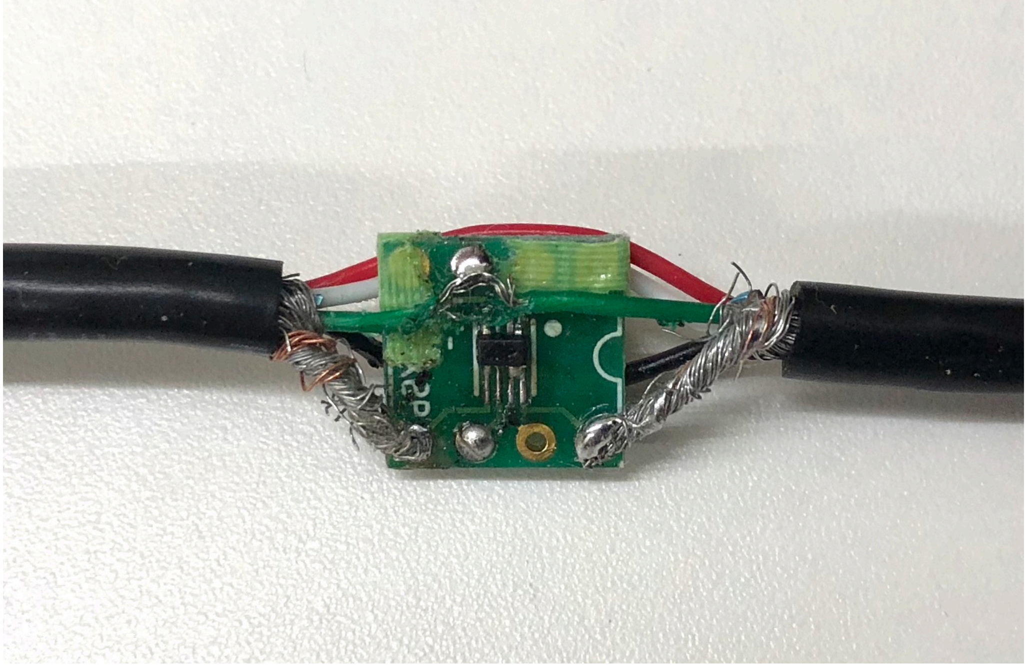

Figure 4.2: A photo of RFRA embedded into a USB cable.

Table 4.1: Additional instruments used in the USB keyboard experiments.

Instrument	Model
USB extension cable	KU-RAA1
USB Keyboard	FKD46AK297
Smartphone	Galaxy S6 edge

4.3 Design of the experiment

We attached an FET to an 1 m of USB extension cable and attacked it. An USB Keyboard and a smartphone is connected via the FET-embedded cable. We manually typed several keys using the keyboard. The typed letters were saved using a note app running on the smartphone. The saved letters will be used as the correct key inputs. The success rate is calculated by comparing the saved letters and decoded letters.

Figure 4.3 presents the overview of the experimental setup. We used the same equipment shown in Table 3.1 and Table 3.2. Table 4.1 summarises the instruments used additionally in the USB keyboard experiments. The distance between the target and antennas for the attack was increased by 0.5 m, starting with the distance of 0.5 m. The distance between the antenna was adjusted to the best location between 0.5 m and 1.5 m. Antennas and the target were

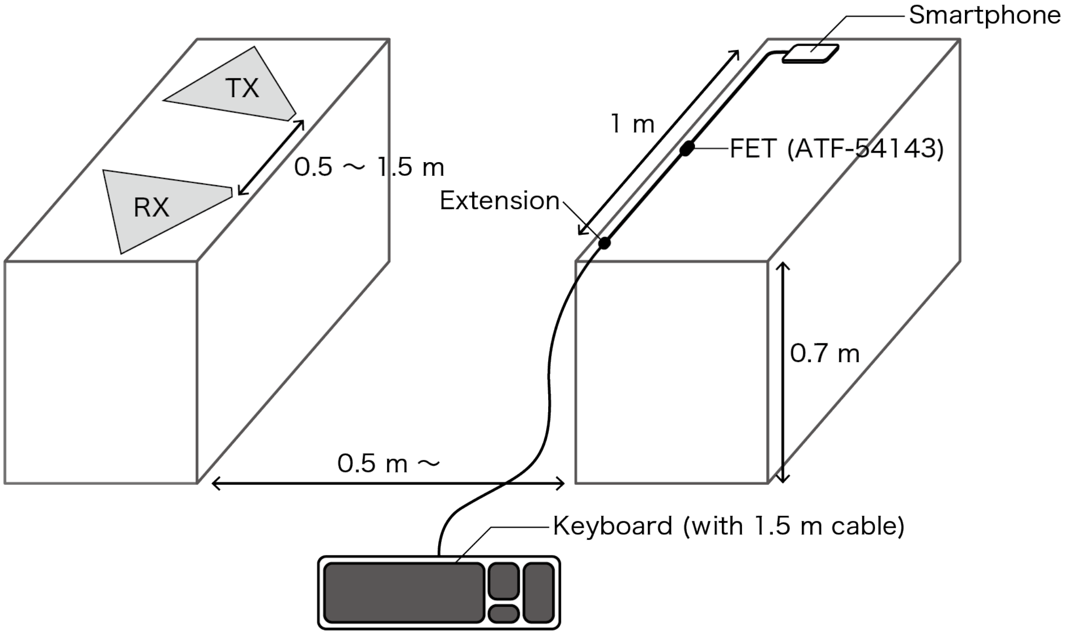

Figure 4.3: Experiment setup.

placed at the position of 0.7 m height from the floor. The sampling rate of a USRP was set to 10 Mbps, which corresponds to approximately 6.7 sampling points per 1 bit for the USB low-speed mode. Thus, high enough to be able to decode the observed waveforms into the binary data. The frequency of the irradiating radio wave was swept from 600 MHz to 900 MHz to find the best one.

To decode the observed radio wave signals, we built a GNU Radio project showed in Figure 4.4. It implements a simple AM demodulator. Of the blocks shown in the figure, three blocks, ‘differential’, ‘decide_threshold’, and ‘detect_preamble’ are the blocks we developed to detect preamble of USB signals. We also developed a code that converts the differential data into binary data and decode the binary data as USB keyboard inputs. For reference, the GNU Radio project and USB keyboard decoding code are publicly available at `https://github.com/RFRA-keyboard/`.

4.4 Evaluation

In our setup, the longest distance the attack succeeded was 1.5 m. The observed waveforms at each distance are presented in Figure 4.5, Figure 4.6, and Figure 4.7. We notice that the waveform observed at 1.5 m has lower amplitudes and noise effects, compared to the ones observed at 0.5 m and 1.0 m. However, it was clear enough to be decoded with our code.

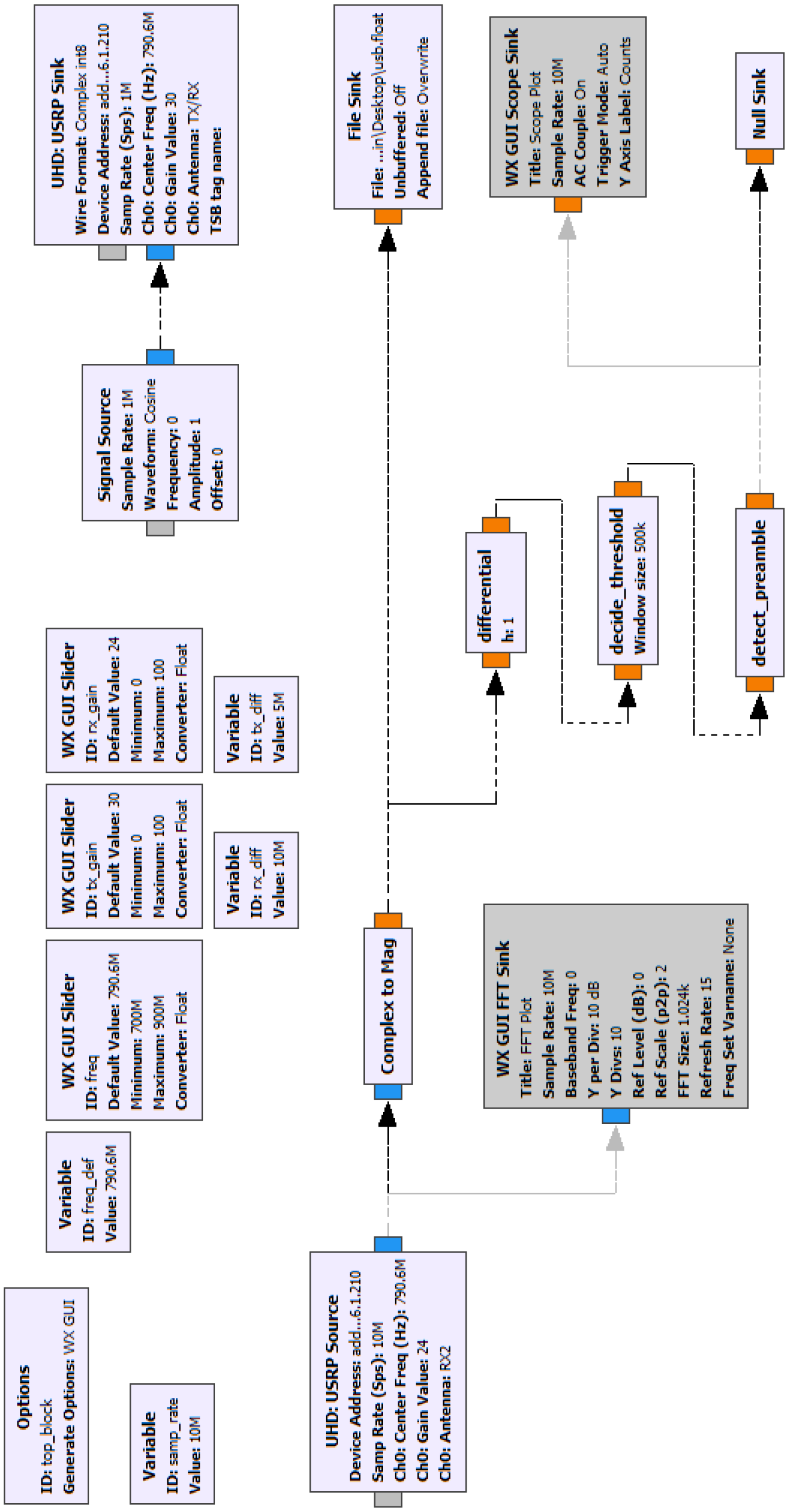

Figure 4.4: Composition of GNU Radio blocks used for decoding the observed radio wave signals.

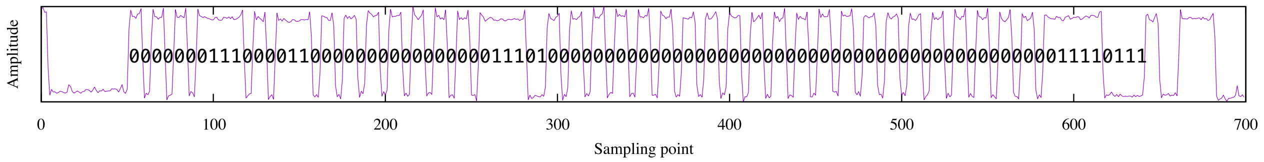

Figure 4.5: Waveform eavesdropped from 0.5 m from the target.

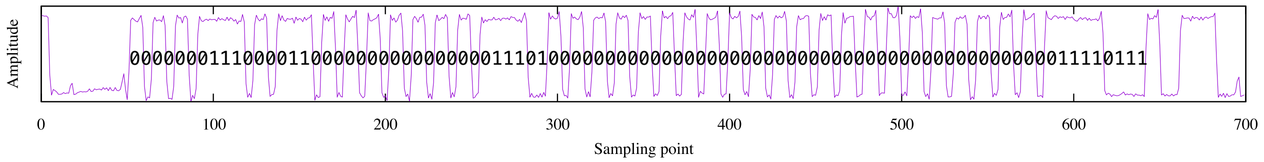

Figure 4.6: Waveform eavesdropped from 1.0 m from the target.

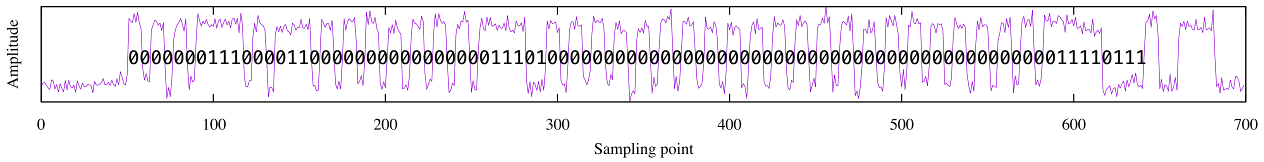

Figure 4.7: Waveform eavesdropped from 1.5 m from the target.

Table 4.2 presents the results, i.e., key inference error rate v.s. distance to the target. There were no errors up to 1.0 m. In 1.5 m, one letter failed to be decoded correctly, resulting the error rate of 1%. We failed to decode the letters when the distance was 2 m. To be accurate, we could not detect preamble with our code, so that no information was obtained through eavesdropping. However, as we have shown in Figure 3.2, it is possible to obtain the original waveforms up to the distance of 10 m. As the Friis transmission equation shows, the reception intensity of radio waves in the free space is inversely proportional to the square of the distance. For this reason, even if there is only a 0.5 m difference, the influence of noise becomes non-negligible, and our code fails to decode the signal. We expect that by improving our naive implementation of the decoding algorithm and program, the range of a successful attack will be increased. Another problem is that finding success conditions, like frequency and position of antennas, is very difficult. More research on success condition is required.

Finally, we present the examples of input letters and decoded letters in Figure 4.8. The input letters are an pangram, which is a sentence of letters that contains every alphabet letter at least once. We note that as we manually inputted the letters, there were typos in the input letters.

We conclude that an USB keyboard is attackable with the RFRA. Although the range is not great, the eavesdropping success rate at 1.5 m of distance was quite high, which suggests that eavesdropping sensitive information such as passwords is feasible with this attack.

- 0.5 m (no error.)
  - my faxed a joke won a paper in the cable tv quiz show. The quick brown fox jumps oever the lazy dog.
  - my faxed a joke won a paper in the cable tv quiz show. The quick brown fox jumps oever the lazy dog.
- 1.0 m (no error.)
  - my faxed joke won a paper in the cable tv show. The quick brown fox jumps over the lazy dog.
  - my faxed joke won a paper in the cable tv show. The quick brown fox jumps over the lazy dog.
- 1.5 m (one error.)
  - my faxed joke won a paper in the cable tv quiz show. The quick brown fox jumps over the lazy dog.
  - my faxed joke won a paper in th cable tv quiz show. the quick brown fox jumps over the lazy dog.

Figure 4.8: Comparisons of typed text and eavesdropped text. The upper letters are what we typed and lower letters are what were eavesdropped.

Table 4.2: Error rate.

Distance [m]	0.5	1.0	1.5
# of characters typed	100	92	97
# of characters succeeded to decode	100	92	96
Error rate [%]	0	0	1.03

Chapter 5

Discussion

We demonstrated that RFRA enables an attacker to steal the signal transmitted through a cable by merely attaching an FET to the cable. Although RFRA is an attack that does not work unless an attacker irradiates radio waves, it has several advantages:

- As FET is a tiny element, it can be embedded into the wide varieties of devices.
- Because FET is tiny, no one will notice that a FET chip is embedded, if it is embedded in the manufacturing stage.
- Because an RFRA circuit does not act as a standalone malicious system, it is difficult to find its existence in the absence of attack activity.

As the target-side gimmick is just to install a FET chip in a cable, an audio cable, for example, could be a target of the attack. Since it is not necessary to attach a device to eavesdrop the signal and transmit it, it will simply look like a normal cable.

As we mentioned above, defending against the attack is not easy because it is infeasible to detect the embedded small hardware trojans. One possible solution is to detect a malicious circuit in the physical layer. Gerdes [18] proposes a countermeasure for detecting hardware key loggers. The key idea of their approach was to leverage the observation that the installation of a hardware key logger affects the electrical characteristics of the system it is attached to. We note, however, that this approach may not be directly applicable to the detection of RFRA hardware trojan because it will be installed at the time of manufacturing, making it difficult to compare the electrical characteristics before and after the installation. Another possible solution is to monitor malicious/reflected RF signals. However, as installing additional sensors may increase the cost of manufacturing, the solution will not be adopted by manufacturers, given the fact that RFRA is a proof-of-concept attack. Of course, as this paper has proven the feasibility of the attack, there could be a possibility that the threat of RFRA becomes manifest in the future. Further study is necessary to develop the effective countermeasures against the attack.

Chapter 6

Related works

There have been many studies on *passive* electromagnetic side-channel attacks [1, 2, 3, 4]. In [1], Hayashi et al. leveraged EM emanation from a targeted table PC to recover the screen image. In [2], Schulz et al. monitored radiated electromagnetic fields around an Ethernet cable to eavesdrop Ethernet communications.

As we mentioned in Section 1, however, there have been very few studies on the *active* electromagnetic side-channel attacks. Although prior studies [5, 6] refer to the attack, its mechanism and feasibility has not been tested in a systematic manner there. There is a room for further research on *active* electromagnetic side-channel attacks. We hope this work becomes a stepping stone to attract more researchers in this field.

Chapter 7

Conclusion

Through the extensive experiments, we have evaluated the approximate limit of Radio-frequency (RF) retroreflector attack (RFRA). We also tested the application of RFRA by prototyping an RFRA-enabled USB cable. Given the experimental results, we conclude that the RFRA is feasible.

As we have shown, the mechanism of the signal leakage part of RFRA is very simple, and it consists of a small FET chip and an antenna, which is one of the cables used in a target, e.g., a shielded wire. A FET chip is so tiny that it is difficult for a targeted user to notice that it is embedded. It is also noteworthy that the cost needed for the attack was within USD 5,000. With our configuration of USD 5,000, the attack succeeded up to 10 m, and the attackable communication speed was up to about 10 Mbps. Since the distance depends on the radio field strength and the communication speed depends on the sampling rate of USRP, it is expected that this limit can be extended by upgrading the equipment.

Finally, we note that RFRA can target not only digital signals but also analog signals such as acoustic signals. Studying other applications of RFRA and their countermeasures is left for further study. We hope that the threat of RFRA encourages developers of transmission protocols and corresponding devices to be aware of the fact that even though a signal is transmitted through a wired cable, it could be leaked if an attacker embeds Trojan hardware like RFRA in advance.

Acknowledgements

I would like to thank my supervisor Professor Shigeki Goto for suggesting and supporting. I also would like to thank Professor Tatsuya Mori. He gave me many advices and helped my study.

MR. Maruyama worked together to resolve many questions and experiment. I would like to thank him, too.

Bibliography

[1] Yuichi Hayashi et al. "A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation". In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. CCS '14. Scottsdale, Arizona, USA: ACM, 2014, pp. 954–965. ISBN: 978-1-4503-2957-6. DOI: `10.1145/2660267.2660292`. URL: `http://doi.acm.org/10.1145/2660267.2660292`.

[2] Matthias Schulz et al. "Trust The Wire, They Always Told Me!: On Practical Non-Destructive Wire-Tap Attacks Against Ethernet". In: *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. WiSec '16. Darmstadt, Germany: ACM, 2016, pp. 43–48. ISBN: 978-1-4503-4270-4. DOI: `10.1145/2939918.2940650`. URL: `http://doi.acm.org/10.1145/2939918.2940650`.

[3] Josyula R. Rao and Pankaj Rohatgi. "EMpowering Side-Channel Attacks". In: *IACR Cryptology ePrint Archive* 2001 (2001), p. 37. URL: `http://eprint.iacr.org/2001/037`.

[4] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. "Electromagnetic Analysis: Concrete Results". In: *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*. Generators. 2001, pp. 251–261. DOI: `10.1007/3-540-44709-1_21`. URL: `https://doi.org/10.1007/3-540-44709-1_21`.

[5] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd ed. Wiley Publishing, 2008. ISBN: 9780470068526.

[6] Markus G. Kuhn and Ross J. Anderson. "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations". In: *Information Hiding*. Vol. 1525. LNCS. Springer, 1998, pp. 124–142.

[7] *NSA ANT Catalog*. `https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf`

[8] *Eavesdropping using microwaves - addendum.* http://eetimes.com/design/audio-design/4015284/Eavesdropping-using-microwaves--addendum

[9] M. Ossman and D. Pierce. “The NSA Playset”. In: *ToorCamp.* https://archive.org/details/nsaplayset-toorcamp2014. 2014.

[10] *GBPPR Project.* http://www.qsl.net/n9zia/

[11] Michael Ossmann. *The NSA Playset: RF Retroreflectors.* DEF CON 22. 2014

[12] *GBPPR TAWDRYYARD Experiments.* http://mail.blockyourid.com/~gbpprorg/mil/photoanglo/tawdryyard/index.html

[13] *GBPPR Vision #26: Overview of the NSA's TAWDRYYARD Radar Retro-Reflector.* https://youtu.be/KDQxDxiflyo

[14] Satohiro Wakabayashi et al. “A Feasibility Study of Radio-frequency Retroreflector Attack”. In: *12th USENIX Workshop on Offensive Technologies (WOOT 18).* Best Student Paper Award. Baltimore, MD: USENIX Association, 2018. URL: https://www.usenix.org/conference/woot18/presentation/wakabayashi.

[15] 若林 哲宇 et al. “電波再帰反射攻撃の実用性評価”. In: **コンピュータセキュリティシンポジウム** *2017***論文集**. Vol. 2017. 2. 学生論文賞受賞. Oct. 2017.

[16] Satohiro Wakabayashi et al. “POSTER: Is Active Electromagnetic Side-channel Attack Practical?” In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.* CCS '17. Dallas, Texas, USA: ACM, 2017, pp. 2587–2589. ISBN: 978-1-4503-4946-8. DOI: 10.1145/3133956.3138830. URL: http://doi.acm.org/10.1145/3133956.3138830.

[17] *Universal Serial Bus Specification, Revision 2.0.* http://www.usb.org/developers/docs/usb20_docs/. 2000

[18] Ryan M. Gerdes and Saptarshi Mallick. “Physical-Layer Detection of Hardware Keyloggers”. In: *Proceedings of the 18th International Symposium on Research in Attacks, Intrusions, and Defenses - Volume 9404.* RAID 2015. Kyoto, Japan: Springer-Verlag New York, Inc., 2015, pp. 26–47. ISBN: 978-3-319-26361-8. DOI: 10.1007/978-3-319-26362-5_2. URL: http://dx.doi.org/10.1007/978-3-319-26362-5_2.