POSTER: Is Active Electromagnetic Side-channel Attack Practical?

Satohiro Wakabayashi
Waseda University
Shinjuku, Tokyo, Japan
wakabayashi@goto.info.waseda.ac.jp

Seita Maruyama
Waseda University
Shinjuku, Tokyo, Japan
maruyama@nsl.cs.waseda.ac.jp

Tatsuya Mori
Waseda University
Shinjuku, Tokyo, Japan
mori@nsl.cs.waseda.ac.jp

Shigeki Goto
Waseda University
Shinjuku, Tokyo, Japan
goto@goto.info.waseda.ac.jp

Masahiro Kinugawa
National Institute of Technology, Sendai College
Sendai, Miyagi, Japan
kinugawa@sendai-nct.ac.jp

Yu-ichi Hayashi
Nara Institute of Science and Technology
Ikoma, Nara, Japan
yu-ichi@is.naist.jp

ABSTRACT

Radio-frequency (RF) retroreflector attack (RFRA) is an *active* electromagnetic side-channel attack that aims to leak the target's internal signals by irradiating the targeted device with a radio wave, where an attacker has embedded a malicious circuit (RF retroreflector) in the device in advance. As the retroreflector consists of small and cheap electrical elements such as a field-effect transistor (FET) chip and a wire that can work as a dipole antenna, the reflector can be embedded into various kinds of electric devices that carry unencrypted, sensitive information; e.g., keyboard, display monitor, microphone, speaker, USB, and so on. Only a few studies have addressed the basic mechanism of RFRA and demonstrated the success of the attack. The conditions for a successful attack have not been adequately explored before, and therefore, assessing the feasibility of the attack remains an open issue. In the present study, we aim to investigate empirically the conditions for a successful RFRA through field experiments. Understanding attack limitations should help to develop effective countermeasures against it. In particular, with regard to the conditions for a successful attack, we studied the distance between the attacker and the target, and the target signal frequencies. Through the extensive experiments using off-the-shelf hardware including software-defined radio (SDR) equipment, we revealed that the required conditions for a successful attack are (1) up to a 10-Mbps of target signal and (2) up to a distance of 10 meters. These results demonstrate the importance of the RFRA threat in the real world.

CCS CONCEPTS

• **Security and privacy → Hardware attacks and countermeasures**;

KEYWORDS

Active electromagnetic side-channel attack, Hardware security, RF retroreflector attack

1 INTRODUCTION

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, few works have been performed on *active* electromagnetic side-channel attacks [1, 2]. In Ref. [1], Anderson mentioned that some of these methods were already known to the intelligence community; in particular, he mentioned reports of the CIA using software-based radio-frequency (RF) exploits in economic espionage against certain European countries.

The NSA advanced network technology (ANT) catalog 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.

After the NSA ANT catalog was leaked, several hackers started recreating the surveillance tools using open-source hardware and software [3]. In DEF CON 22 [4], Michael Ossmann successfully demonstrated that RFRA can 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. Although these prior works have successfully demonstrated the threat of RFRA, an empirical research approach has not been applied to understanding the attack mechanism. Given this

CCS '17, October 30-November 3, 2017, Dallas, TX, USA
© 2017 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-4946-8/17/10.
https://doi.org/10.1145/3133956.3138830

background, we aim to answer the following simple research question: **RQ** "*Is RFRA a practical attack?*" To answer this question, we first create a simple RF retroreflector that is made from 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 a RF retroreflector. We then generate electric waveforms in the retroreflector using a function generator connected to it. Finally, using SDR, 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.

The key findings we derived through 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 m between an attacker and a target device.
- RFRA succeeded to read the internal signal of 10 Mbps, which was roughly half of the maximum rate of the SDR processing capability.

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 hardware device instead of SDR will be able to target higher frequency of internal signals, e.g., USB high-speed.

2 RFRA MECHANISM

The core of an RFRA lies in the retroreflector embedded into the target device. Figure 1 shows the structure of a retroreflector, which includes a FET chip and a dipole antenna. Figure 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 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, current is induced when the dipole antenna receives the carrier wave, which is transmitted by an attacker. The FET controls the induced current in proportional 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. 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.

3 EXPERIMENTS

3.1 Setup

Figure 4 shows the experimental setup. The RF reflector is connected to a function generator, which 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 with controlled distances. The reflector's antenna cable is set up straightened. Table 1 summarizes the instruments used in our experiments, and Table 2 lists the software and specs PC used for SDR.

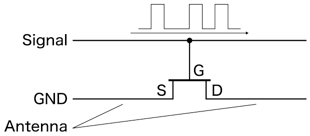

Figure 1: A RF retroreflector that includes a FET chip and a dipole antenna. An internal signal is applied to the gate of FET.

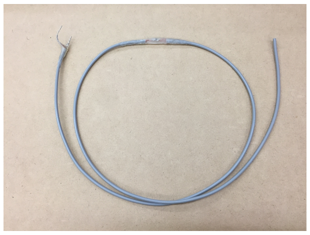

Figure 2: An implementation of the RF retroreflector using a coaxial cable.

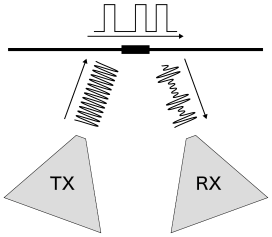

Figure 3: Overview of an RFRA attack.

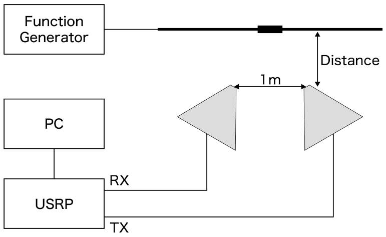

Figure 4: Experimental setup (overview).

3.2 Distance between the attacker and the target

We first investigate the effective distance for 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 USRP. The frequency of the irradiated wave ranges from 590 MHz to 680 MHz, roughly

Table 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

Table 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

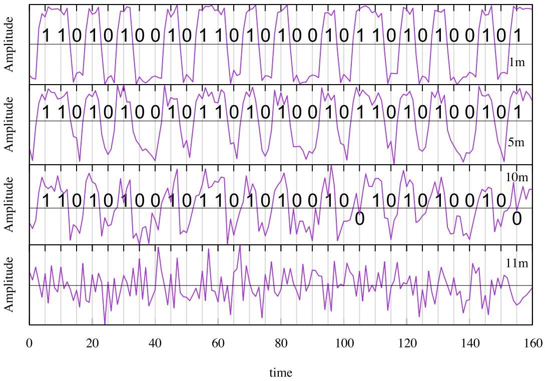

Figure 5: Measured signals under different distances between the attacker and the target.

corresponding 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 USRP is set to 10 MS/s.

Figure 5 shows the measured waveforms for the distances of 1 m, 5 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 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. 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 6 shows the results (the case for 20 Mbps is omitted due to space limitation). The frequency of the irradiated wave is set to 771.2 MHz.

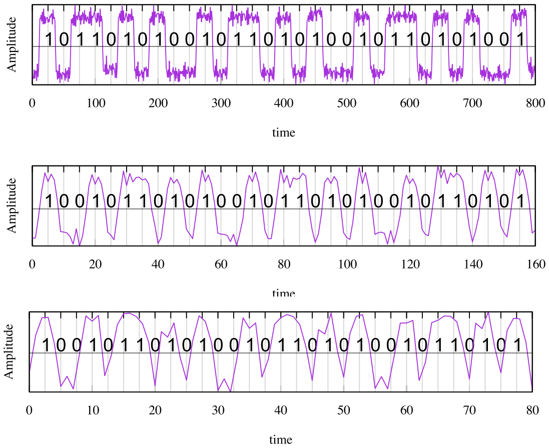

Figure 6: Measured waveforms for the target signals with the frequencies of 1 Mbps (top), 5 Mbps (middle), and 10 Mbps (bottom).

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, our setup 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.

4 SUMMARY

Through the field experiments, we demonstrated that the threat of RFRA is practical; the implementation with an off-the-shelf SDR and a laptop PC successfully reads the target's internal signal at 10 m distance. To the best of our knowledge, this work is the first to characterize the limitation of RFRA in a systematic way. The following issues are left for future study. What kind of devices/signals could be targeted with RFRA? Can hardware-implemented RFRA read high-speed signals such as 1 G+ bps? How can we detect RF retroreflectors? How can we mitigate RFRA?

REFERENCES

[1] Ross J. Anderson. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems* (2 ed.). Wiley Publishing.

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

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

[4] Michael Ossmann. 2014. The NSA Playset: RF Retroreflectors. (2014). DEF CON 22.

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

[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.