Detection of Rogue Devices using Unintended Near and Far-field Emanations with Spectral and Temporal Signatures

Md Faizul Bari, Meghna Roy Chowdhury, Baibhab Chatterjee, Shreyas Sen
Department of Electrical and Computer Engineering, Purdue University, USA
{mbari, mroycho, bchatte, shreyas}@purdue.edu

***Abstract*— In this work, using data collected from a desktop computer in an anechoic chamber, we have characterized both near and far-field emissions over a wide frequency band and demonstrated that it matches closely with the monopole antenna in Fresnel and Fraunhofer regions and can be used to detect the start-up of a rogue device in a security-critical room. Detailed spectral analysis shows that emission is strong at lower frequencies. Additionally, high-frequency leakage can also be detected from a 200 cm distance. Frequency shifting of the peaks is observed over time and linked to the program execution. Finally, detection of the onset of a rogue device in a static facility has been demonstrated for different SNRs.**

***Keywords*— electromagnetic emission, Fresnel and Fraunhofer regions, anechoic chamber, rogue detection**

I. Introduction

A. Background and Motivation

The unintentional electromagnetic emission from electronic devices is known as emanation and poses a significant security threat as it can spill over important data. These intelligence-bearing signals can be easily intercepted to reveal data and/or secret encryption keys, leading to different attacks e.g., *side-channel attack (SCA)*. The problem was first discovered in the 50s and forced many countries to adopt various protective shielding mechanisms under the code name *TEMPEST* [1]. However, as low power devices emerged over the next decades, the radiation power became weak and researchers mainly focused on near-field emissions only.

Recent studies have been performed targeting a specific device at a certain clock frequency. Complex equipment can have chips operating at different frequencies over a wide band which demands an extensive study of the emission pattern and the interaction of the clock frequencies. Additionally, metal case and other protective parts limit in-proximity probing to a certain distance (e.g., heat sink and cooling fan make $\sim 3\,\mathrm{cm}$ distance over a microprocessor inaccessible). However, such complex equipment is quite common in secured and sensitive facilities due to their diverse application, leading to their emission security of paramount importance. Recently, significant research efforts are being provided, including the *Securing Compartmented Information with Smart Radio Systems (SCISRS)* program by the *Intelligence Advanced Research Projects Activity (IARPA)* [2], to find an anomaly in the RF emission spectrum to detect the onset of rogue equipment in a secured facility as shown in Fig. 1(a).

In this work, we have used an off-the-shelf desktop computer which is widely used nearly in every facility.

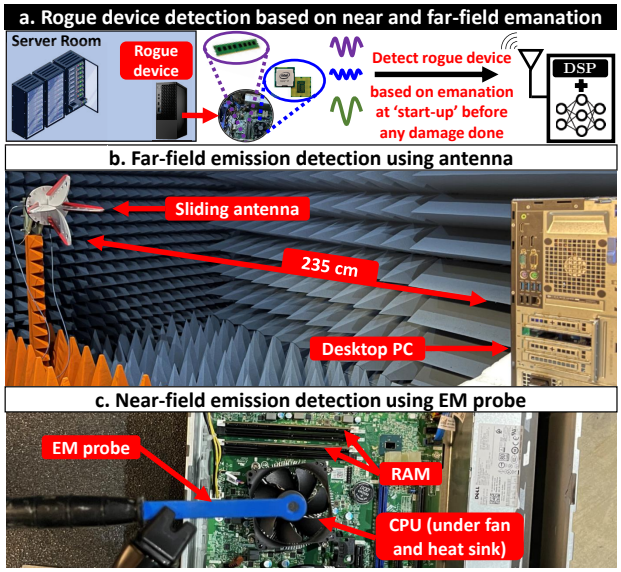

Fig. 1. (a) Onset of a rogue device adds emanations at different frequencies and SNR to the environment. The near and far-field emanation can be used to detect the onset and prevent attacks. (b) Experimental setup in the anechoic chamber. A sliding antenna can move from 35 cm to 235 cm from the target. (b) EM probe on a sliding stand to detect near-field emission.

Collecting data using both EM probe and RF antenna, we have shown that emanations can be detected at different frequency ranges, showing strong peaks at lower bands (e.g., 2.64 MHz). However, emission at high frequency (e.g., 3.5 GHz) can still be detected even from 200 cm. Temporal analyses have been performed to show the time evolution of EM peaks and their link to the booting process. The emission pattern matches closely with the theory and shows both Fresnel and Fraunhofer regions of antenna radiation. This analysis leads to the loss modeling that helps in finding integration time and bandwidth to determine enough SNR for peak detection. In the end, using results from these analyses, the start-up of a rogue device is detected at different SNR levels.

B. Literature Review

The first publicly available work on using emanation to successfully eavesdrop was done by Wim Van Eck [3] and emanations are often called 'Van Eck radiation' after him. Since then, emanations have found diverse applications in emission security (EMSEC). EM emission has been used to find an anomaly in program execution or malware [4]. In 2018, researchers developed a new side-channel attack that affected

2022 IEEE/MTT-S International Microwave Symposium - IMS 2022 | 978-1-6654-9613-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/IMS37962.2022.9865347

mixed-signal chips [5]. They demonstrated key-recovery on an nRF52832 chip with AES-128 implementation. Recent works involve both deep learning-based cross-device SCA [6], [7] and countermeasures [8], [9], [10], [11]. They used NAE 308T XMEGA to achieve $> 99.9\%$ accuracy on cross-device SCA.

C. Our Contribution

1) Using a commercial desktop PC, **both near and far-field emissions are detected and analyzed both from a theoretical and experimental perspective**. This analysis shows the relevance of far-field detection even for devices with low-power, high-frequency chips.

2) Detailed spectral analysis reveals that **the emanation is very strong at MHz frequencies, yet still detectable at GHz frequencies even from a 200 cm distance**. Extensive temporal analysis has also been performed.

3) An application of the far-field emanation, **detection of the onset of a rogue device in a data center or server**, is explored in detail.

II. Experimental Setup and Data Processing

Fig. 1(b) and (c) show our experimental setup for near and far-field respectively. We used a desktop with an intel® core™ i7-6700 microprocessor ($3.4\,\mathrm{GHz}$ base frequency, up to $4\,\mathrm{GHz}$ turbo boost) as our target device. It was equipped with $8\,\mathrm{GB}$ RAM ($2.4\,\mathrm{GHz}$). The target was placed in an anechoic chamber. EM emanations are collected using both a moving antenna and an EM probe and observed in a spectrum analyzer. Based on initial observation of emission from kHz to GHz spectrum, we selected 3 target frequencies, $3.5\,\mathrm{GHz}$ (processor frequency zone), $2.4\,\mathrm{GHz}$ (RAM frequency), and $264\,\mathrm{MHz}$ (low-frequency emission from motherboard routing), and reduced span so that noise integrated over the band is low.

III. RF Emanation Patterns

A. Spatial Variation - Fresnel and Fraunhofer Region

We know that if TX-RX separation is R, antenna length is D, and the emission wavelength is λ, then the emission from an antenna can be divided into 3 regions: (i) reactive near-field ($R < 0.62\sqrt{\frac{D^3}{\lambda}}$) (ii) radiative near-field/ Fresnel region ($0.62\sqrt{\frac{D^3}{\lambda}} < R < \frac{2D^2}{\lambda}$) (iii) far-field/ Fraunhofer region ($R > max(\frac{2D^2}{\lambda}, \sim 5\lambda, \sim 5D)$). In these three regions, fields die off as $\frac{1}{R^3}$, $\frac{1}{R^2}$, and $\frac{1}{R}$ respectively.

1) Near-field region

At high frequency, short λ makes the near-field region too close to the target. Hence we observe near-field at $264\,\mathrm{MHz}$ where $\lambda = 1.14\,\mathrm{m}$ and $D \sim \frac{\lambda}{4} = 0.284\,\mathrm{m}$. Hence, reactive and radiative near-fields will be at $R < 8.8\,\mathrm{cm}$ and $8.8\,\mathrm{cm} < R < 14.15\,\mathrm{cm}$ respectively. Fig. 2(a) shows that the emission pattern exhibits $\frac{1}{R^3}$ behavior very closely up to $9\,\mathrm{cm}$ and follows $\frac{1}{R^2}$ curve from $10\,\mathrm{cm}$ onwards as shown in Fig. 2(b). So, $10\,\mathrm{cm}$ is the deflection point at which emission switches from reactive near-field to radiative near-field. It matches the theoretical prediction ($8.8\,\mathrm{cm}$) with reasonable accuracy.

2) Far-field Region

At $3.5\,\mathrm{GHz}$, $\lambda = 8.6\,\mathrm{cm}$ and $D \sim \frac{\lambda}{4} = 2.14\,\mathrm{cm}$. Hence, far-field is defined at $R > max(\frac{2D^2}{\lambda}, \sim 5\lambda, \sim 5D) = \sim 43\,\mathrm{cm}$. Hence, far-field data are taken for $R > 40\,\mathrm{cm}$ as shown in Fig. 2(c). Indeed, the $\frac{1}{R}$ fitting curve matches with the emission pattern within experimental error and confirms the theoretical prediction.

B. Spectral Signatures

Fig. 3(a) shows the max emission power versus frequency for $35\,\mathrm{cm}$ – $235\,\mathrm{cm}$ distances. We make a few interesting observations from this plot. To begin with, EM emission shows much higher power at lower frequencies. Next, emanation power decreases with distance, which is also observed in spatial variation plots and theoretically expected. Finally, we observe that emission at $3.5\,\mathrm{GHz}$ frequency can be observed up to $200\,\mathrm{cm}$ and submerge into noise at $235\,\mathrm{cm}$. On contrary, lower frequency emissions have a strong peak even at $235\,\mathrm{cm}$ and can have a much longer detection range.

C. Temporal Signatures

Fig. 3(b) shows the temporal variation of the emanation at $\sim 3.5\,\mathrm{GHz}$. At $t = 0$, PC is turned on. Distinct peak shows up at $t = 0.5\,\mathrm{ms}$ and gradually shifts towards left with time as shown in the subplots for $t = 1$ to $2.5\,\mathrm{s}$. Eventually they start moving towards the right and then hop around in both directions. The same phenomenon is observed at other frequencies, though less pronounced at low frequencies. It can be linked to the *booting sequence*. This observation opens up the door for multiple applications to detect device types, initial behavior, etc. based on temporal signatures.

IV. Application

A. Detection of the Onset of a Rogue Device

In a test environment, there is always an RF baseline consisting of RF background, known signals, and emanations. When a new device turns on, it adds new emanation peaks to the existing baseline. Peak detection and comparison with prior baseline can detect the presence of a new device in a secured server where no new device is supposed to be introduced during normal operation. Since server rooms are large, even low SNR emanations must be detected. Fig. 4(a) and (b) show device onset detection using the peak search method at $82\,\mathrm{dB}$ and $18\,\mathrm{dB}$ SNRs. The EM emission is filtered using a Savitzky-Golay filter and compared with the prior emanation profile to determine the presence of the rogue device.

B. Comparison with Relevant Work

Table 1. Comparison of EDDIE [4] and our work.

Parameter	**EDDIE**	**Our Work**
Application	Malware detection	Onset of rogue device detection
Frequency	1 GHz	Wide band, 264 MHz to 3.5 GHz
Detection distance	Right on the device	200 cm at 3.5 GHz and much longer distance at 264 MHz

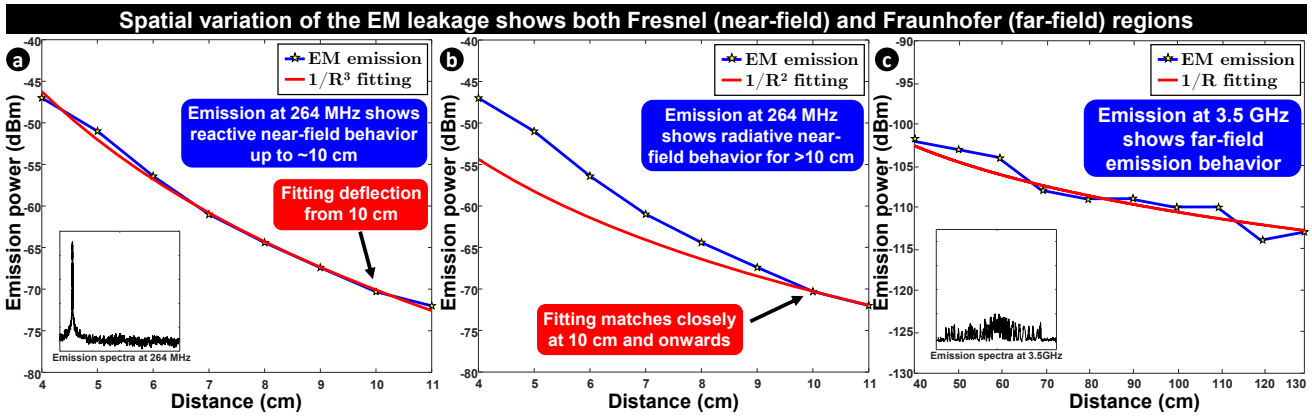

Fig. 2. (a) Reactive and (b) radiative near-field regions with $\frac{1}{R^3}$ and $\frac{1}{R^2}$ pattern for emission at 264 MHz. Deflection point at $\sim$ 10 cm (c) Far-field region ($\frac{1}{R}$ fitting) shown at 3.5 GHz.

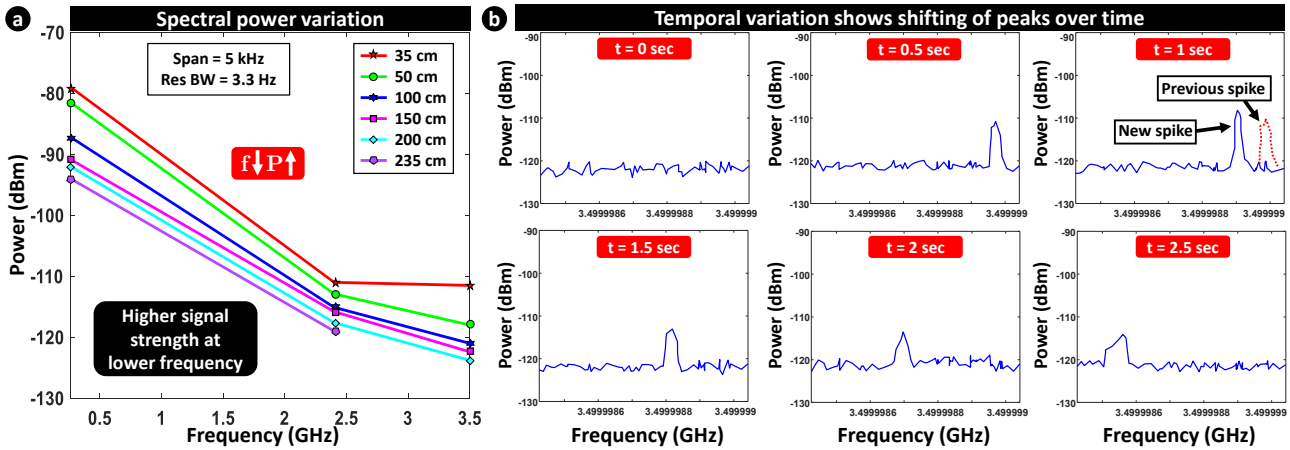

Fig. 3. (a) Spectral power variation shows that low-frequency emissions are much stronger compared to their high-frequency counterpart (b) Emission peaks shift towards left (and later towards right) with time. The shifting is <1 PPM and can be attributed to the booting process.

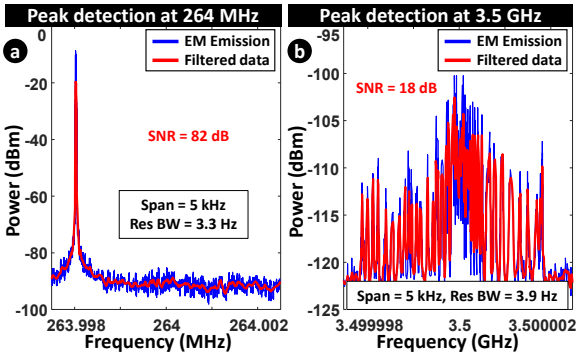

Fig. 4. Peak detection for at (a) 264 MHz and (b) 3.5 GHz for the detection of rogue device onset.

Alireza et al. used emanations to detect malware [4], while we have used it to detect the start-up of a PC. A comparison of these two works is given in Table 1.

V. Conclusion

In this work, we have analyzed the electromagnetic emission from a desktop computer and found that the emission pattern follows Fresnel and Fraunhofer region behavior just like a monopole antenna. Detailed spectral analysis reveals that low-frequency peaks are stronger. Nonetheless, we can detect a high frequency (3.5 GHz) peak at a 200 cm distance using an RF antenna. We have performed temporal analysis and used both near and far-field emissions to detect the onset of a rogue device. This work paves the way for detecting rogue devices in security-critical rooms using far-field unintended emanations leading to the advancement of state-of-the-art emission security.

Acknowledgment

This research was supported by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via contract: 2021-21062400006. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ODNI, IARPA, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes not withstanding any copyright annotation thereon.

REFERENCES

[1] "Eavesdropping On the Electromagnetic Emanations of Digital Equipment: The Laws of Canada, England and the United States," Intelligence Resource Program. [Online]. Available: https://irp.fas.org/eprint/tempest.htm. [Accessed: 07-Dec-2021].

[2] "SCISRS - Securing Compartmented Information with Smart Radio Systems," IARPA. [Online]. Available: https://www.iarpa.gov/index.php/research-programs/scisrs. [Accessed: 07-Dec-2021].

[3] W. van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?," Computers & Security, vol. 4, no. 4, pp. 269–286, Dec.1985, doi: 10.1016/0167-4048(85)90046-X.

[4] A. Nazari et al., "EDDIE: EM-based detection of deviations in program execution," in 2017 ACM/IEEE 44th Annual International Symposium on Computer Architecture (ISCA), 2017, pp. 333–346. doi: 10.1145/3079856.3080223.

[5] G. Camurati et al., "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 163–177. doi: 10.1145/3243734.3243802.

[6] J. Danial et al., "EM-X-DL: Efficient Cross-Device Deep Learning Side-Channel Attack with Noisy EM Signatures," ACM Journal on Emerging Technologies in Computing Systems, vol. 18, no. 1, pp. 1–17, Nov. 2020, doi: 10.1145/3465380.

[7] D. Das et al., "X-DeepSCA: Cross-Device Deep Learning Side Channel Attack," in 2019 56th ACM/IEEE Design Automation Conference (DAC), 2019, pp. 1–6.

[8] D. Das et al., "EM and Power SCA-Resilient AES-256 Through >350× Current-Domain Signature Attenuation and Local Lower Metal Routing," in IEEE Journal of Solid-State Circuits, vol. 56, no. 1, pp. 136-150, Jan. 2021, doi: 10.1109/JSSC.2020.3032975.

[9] D. Das and S. Sen, "Electromagnetic and Power Side-Channel Analysis: Advanced Attacks and Low-Overhead Generic Countermeasures through White-Box Approach," Cryptography, vol. 4, no. 4, p. 30, Oct. 2020, doi: 10.3390/cryptography4040030.

[10] D. Das et al., "EM SCA White-box Analysis Based Reduced Leakage Cell Design and Pre-Silicon Evaluation," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, doi: 10.1109/TCAD.2022.3144369.

[11] M. Nath, D. Das and S. Sen, "A Multipole Approach Toward On-Chip Metal Routing for Reduced EM Side-Channel Leakage," in IEEE Microwave and Wireless Components Letters, vol. 31, no. 6, pp. 685-688, June 2021, doi: 10.1109/LMWC.2021.3062809.