Introduction to EM Information Security for IoT devices

Yuichi Hayashi
Graduate School of Information Science
Nara Institute of Science and Technology
Nara, Japan
yu-ichi@is.naist.jp

Ingrid Verbauwhede
Department of Electrical Engineering
Katholieke Universiteit Leuven
Leuven, Belgium
Ingrid.Verbauwhede@esat.kuleuven.be

William A. Radasky
Metatech Corporation,
California, USA
wradasky@aol.com

***Abstract*— With the advent of the Internet of Things (IoT), many electronic devices (e.g., smart meters, surveillance cameras, mobile devices, and multiple sensors) are interconnected. Each device gathers data and uploads it to servers via communication networks. Servers store the large volumes of received data in databases. Applications analyze this data and extract valuable information. Finally, based on this information, new services (in domains such as smart cities, public safety, e-commerce, medical, healthcare, or automobile) are provided. In this data flow, systems and applications in the upper layer trust the hardware in the lower layer, which includes data-gathering devices. If the collected information is intentionally modified by adversaries, services in the upper layer could be disrupted. Therefore, to ensure service continuity in the IoT, it is important to secure the hardware layer in which data are harvested and transmitted. In this paper, we focus on hardware-level security in IoT systems and classify the schemes proposed for physical security of IoT into three categories. We also provide examples for each of these and explain threats and countermeasures.**

Keywords—EM information security; Internet of Things; Intentional electromagnetic interference, Hardware Trojan horse

I. INTRODUCTION

Rapid developments in information and communication technologies have resulted in the generation of vast amounts of sensing information from computers and sensors. This data is transmitted over networks, and stored as big data on clouds. These so-called Internet of Things (IoT) systems have led to a new information age, where information about people and things in real space is integrated and used to create new services for everyday use and socioeconomic, educational, and administrative purposes. Numerous people use these services as a social infrastructure. The services created in this manner are offered on the assumption that the vast amount of sensing information collected by computers and sensors is accurate. In other words, high-end terminals that control the terminal nodes of the IoT system must operate as intended. In this system, each layer consists of terminals that operate by trusting the information coming from the layer below them (Fig. 1).

Any vulnerability of hardware at the bottom of an information system could critically decrease its security. Consequently, ensuring the security of the physical layer is a critical issue in IoT systems. This paper focuses on a virtually non-traceable and undetectable vulnerability in the physical layer, namely, that caused by electromagnetic waves.

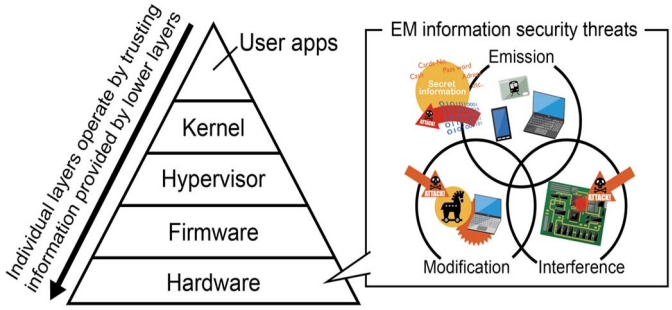

Fig. 1 Trust model and EM information security threats

The vulnerability due to electromagnetic waves can be largely classified into three categories: (1) electromagnetic emanation resulting from information processing within devices, (2) intentional electromagnetic interference to devices, and (3) intentional modification of system circuit configuration (Fig. 1). Ensuring the security of the physical layer can help build a highly reliable infrastructure as the functioning of the IoT relies on the security of the physical layer. This paper uses published studies to summarize threats by classifying them into categories (1) through (3) and introduces countermeasures against these threats.

II. UNINTENTIONAL ELECTROMAGNETIC EMISSION

Data processing in electronic devices results in the propagation and transmission of electrical signals. Time variations in these signals cause electromagnetic radiation, and ultimately, electromagnetic emanation. The level of electromagnetic radiation emitted by information and communication equipment is generally regulated from the viewpoint of electromagnetic compatibility (EMC). Electromagnetic emanation, however, is attributed to the radiated electromagnetic waves that vary with time according to data. Therefore, this could occur even if the strength of the electromagnetic wave signals is less than the regulated level.

Fig. 2 schematically illustrates the mechanism of electromagnetic emanation. When an integrated circuit (IC), a source of leakage, performs data processing, the signals containing the information have frequency components that change as a function of time. The high-frequency components are propagated by electromagnetic coupling to device elements that act as antennas. Subsequently, they are emitted into space depending on the frequency characteristics of the antennas.

Examples of the aforementioned elements that act as antennas include wiring patterns on printed circuit boards, conductors, and lines connected to equipment. These act as unintentional antennas that propagate electromagnetic radiation by mechanisms such as radiation and conduction. Attackers can measure this electromagnetic emanation and obtain the desired information from by statistically processing the measured data. Threats from electromagnetic emanation include theft of monitor screen information from desktops and laptops [1-3], screen information and keystroke information from tablets and smartphones [4], computing information from commercial central processing units inside personal computers [5], printing information from printers [6], input key information from keyboards [7], and secret key information from within the encryption processing devices [8,9]. In particular, information leakage through electromagnetic waves from cryptographic modules is called side-channel attacks.

A possible countermeasure proposed for such threats made electromagnetic emanations from the internal processing constant [10, 11]. Another involved applying random numbers to processed information to scramble the information contained in the radiated electromagnetic waves [12]. Controlling the impedance between the IC and circuit board to prevent information leakage outside an IC was proposed in [13], as another countermeasure.

III. Intentional Electromagnetic Interference

Intentional electromagnetic interference (IEMI) is another threat that disables information and communication equipment by stopping functionality or destroying circuit elements. IEMI uses high-power electromagnetic (HPEM) environments far exceeding the normal tolerance of electronic devices (e.g., EMC immunity levels). In the past, the threat of intentional electromagnetic interference to electronic devices by HPEM was limited to some organizations, such as the military. In recent years, however, compact high-power transmitting devices have been available on the market. This has made the threat of IEMI a reality for the commercial information and communication equipment widely used by consumers. To address this threat, the IEEE Electromagnetic Compatibility Society is actively discussing mechanisms and countermeasures [14, 15], and the International Electrotechnical Commission and International Telecommunication Union are working to establish standards.

Further, a non-invasive threat that creates electromagnetic interference with a much smaller amplitude field or voltage as compared to that of the HPEM has been reported. The attack's effect on devices such as cryptographic modules [16, 17], pacemakers [18], and smartphones [19] has been evaluated. In particular, IEMI against cryptographic module is called fault attack. This type of attack intentionally sends electromagnetic

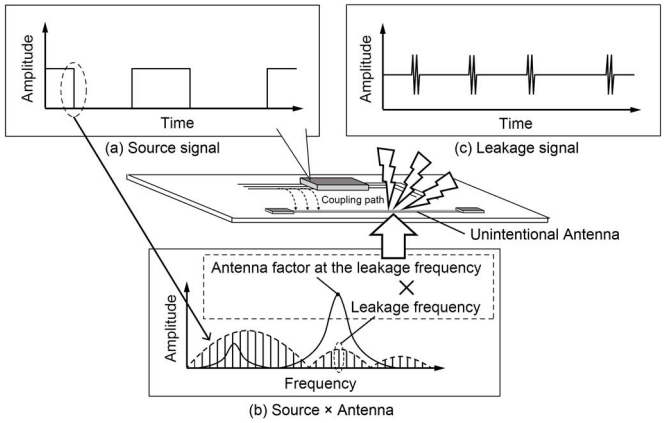

Fig. 2 Mechanism of electromagnetic emanation

waves to trigger a temporary malfunction. The attacker takes advantage of this to reduce the confidentiality and integrity of the equipment by obtaining confidential information, falsifying the data transmitted within the equipment, and issuing random commands.

Effective techniques to counter this type of attack include implementing of a circuit that detects the propagation of unintentional electromagnetic waves inside equipment [20], and achieving EMC within and outside the equipment to prevent propagation of electromagnetic waves [13, 21].

IV. Intentional Modification of Electronic Circuits

In this section, vulnerabilities arising from change in the electromagnetic environment caused by intentional modification of chips and equipment are described.

For reasons such as cost reduction, hardware manufacturers might use third-party foundries where IC chips designed by manufacturers can be produced cheaply. Under such an arrangement, functions not intended by the chip designers could be added during the manufacturing process, and ICs could be destroyed or their security could be made vulnerable to certain attacks. A circuit added against the intentions of the designer is called a Hardware Trojan (HT) and is considered an emerging security threat. Government-level warnings have been issued about this threat, which is a critical security issue.

HTs can be characterized by changed functionality, reduced reliability, information leak, and denial-of-service [22, 23]. HTs leak internal information of equipment by actions not intended by designers (e.g., [24-28]), and therefore, it is important that they be detected. The detection methods considered so far include physical inspection, built-in tests [29], functional testing [30-34], and side channel analyses [35-38]. Especially, the last technique makes good use of EM leakage for detecting HT. The above-mentioned threats and detection methods target the HTs introduced within ICs.

Furthermore, the possibility of HTs being introduced into peripheral circuits has been suggested in recent years [39]. Unlike those on ICs, these HTs do not require installation during the manufacturing stage. Instead, they may be mounted on the electrical circuits of existing parts. A lot of

commercially available equipment could be targeted using this threat, and the range of equipment susceptible to this is more expansive. References indicate that it is possible to measure information leakage using compromising emanations from a distance, even when the strength of emission causing the information leakage is low, and an HT is installed and an electromagnetic wave is directed towards the equipment. In future work, in addition to passive information leaks, vulnerabilities caused by active leaks will also need to be addressed.

V. SUMMARY

This paper classifies hardware security schemes for the IoT into three categories. The threat of electromagnetic emanation is expected to grow with the decrease in price and increase in performance of measurement instruments and computers, as well as the development of analysis technology. To control vulnerabilities due to electromagnetic waves, measures that combine the counteracting technologies in the EMC field with applicability across layers could be effective in supplementing conventional hardware and software countermeasures.

Further, it is expected that IoT system designers will supervise the entire system and its form of usage, examine the degree of security risk at the hardware level, and devise appropriate countermeasures as necessary. In some cases, a countermeasure that could theoretically leak information may be realistically sufficient. Users must also be aware of whether such measures are in place in the products that they use.

REFERENCES

[1] W. van Eck, “Electromagnetic radiation from video display units: An eavesdropping risk?” Comput. Security, vol. 4, pp. 269–286, 1985.

[2] M. G. Kuhn, "Compromising Emanations of LCD TV Sets," in IEEE Transactions on Electromagnetic Compatibility, vol. 55, no. 3, pp. 564-570, June 2013.

[3] H. Sekiguchi and S. Seto, "Study on Maximum Receivable Distance for Radiated Emission of Information Technology Equipment Causing Information Leakage," in IEEE Transactions on Electromagnetic Compatibility, vol. 55, no. 3, pp. 547-554, June 2013.

[4] Y. Hayashi, N. Homma, M. Miura, T. Aoki, H. Sone, “A threat for tablet PCs in public space: remote visualization of screen images using EM emanation,” 21st ACM Conference on Computer and Communications Security (CCS'14), pp. 954-965, Scottsdale, Arizona, USA, November, 2014.

[5] Zajic and M. Prvulovic, “Experimental demonstration of electromagnetic information leakage from modern processor-memory systems,” IEEE Transaction on Electromagnetic Compatibility, vol. 56, no. 4, pp. 885-892, March, 2014.

[6] T. Tosaka, K. Taira, Y. Yamanaka, A. Nishikata, M. Hattori, “Feasibility study for reconstruction of information from near field observations of the magnetic field of laser printer,” 17th International Zurich Symposium on Electromagnetic Compatibility, 2006. EMC-Zurich 2006, pp. 630-633, Singapore, February, 2006.

[7] M. Vuagnoux and S. Pasini, “An improved technique to discover compromising electromagnetic emanations,” IEEE International Symposium on Electromagnetic Compatibility, pp. 121-126, Fort Lauderdale, FL, USA, July 2010.

[8] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in Proc. 19th Annu. Int. Cryptology Conf. Adv. Cryptology, LNCS 1666, 1999, pp. 388–397.

[9] D. Agrawal, B. Archambeault, R. Rao, and P. Rohatgi, “The EM side-channel(s),” in Proc. 4th Int. Workshop Cryptographic Hardware and Embedded Syst., LNCS 2523, Aug. 2002, pp. 29–45.

[10] M.G. Kuhn, Ross J. Anderson, “Soft tempest: hidden data transmission using electromagnetic emanations,” Information Hiding, Second International Workshop, IH’98, pp. 124-142, Portland, Oregon, USA, April, 1998.

[11] K. Tiri and I. Verbauwhede, "Design method for constant power consumption of differential logic circuits," Design, Automation and Test in Europe, 2005, pp. 628-633 Vol. 1.

[12] T. Watanabe, H. Nagayoshi, T. Urano, T. Uemura, and H. Sako, “Counter-measure for electromagnetic screen image leakage based on color mixing in human brain,” in Proc. IEEE International Symposium on Electromagnetic Compatibility, pp. 138–142, 2010.

[13] N. Miura, D. Fujimoto, Y. Hayashi, N. Homma, T. Aoki, M. Nagata, "Integrated-circuit countermeasures against information leakage through EM radiation." (EMC), in Proc. IEEE International Symposium on Electromagnetic Compatibility, pp. 748-751, 2014.

[14] W. A. Radasky, C. E. Baum and M. W. Wik, "Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI)," in IEEE Transactions on Electromagnetic Compatibility, vol. 46, no. 3, pp. 314-321, Aug. 2004.

[15] W. A. Radasky, "Fear of frying electromagnetic weapons threaten our data networks. Here's how to stop them," in IEEE Spectrum, vol. 51, no. 9, pp. 46-51, Sept. 2014.

[16] P. Maurine, "Techniques for EM Fault Injection: Equipments and Experimental Results," 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, 2012, pp. 3-4.

[17] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki and H. Sone, "Transient IEMI Threats for Cryptographic Devices," in IEEE Transactions on Electromagnetic Compatibility, vol. 55, no. 1, pp. 140-148, Feb. 2013.

[18] D. F. Kune et al., "Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors," 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, 2013, pp. 145-159.

[19] C. Kasmi and J. Lopes Esteves, "IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones," in IEEE Transactions on Electromagnetic Compatibility, vol. 57, no. 6, pp. 1752-1755, Dec. 2015.

[20] El-Baze, D., Rigaud, J. B., & Maurine, P. (2016, August). An Embedded Digital Sensor against EM and BB Fault Injection. In Fault Diagnosis and Tolerance in Cryptography (FDTC), 2016 Workshop on (pp. 78-86). IEEE.

[21] Paul, Clayton R. Introduction to Electromagnetic Compatibility. Vol. 184. John Wiley & Sons, 2006.

[22] Tehranipoor, Mohammad, and Cliff Wang. Introduction to hardware security and trust. Springer Science & Business Media, 2011.

[23] Tehranipoor, Mohammad, and Farinaz Koushanfar. "A survey of hardware trojan taxonomy and detection." IEEE design & test of computers 27.1 (2010).

[24] K. Yang, M. Hicks, Q. Dong, T. Austin, D. Sylvester, “Analog malicious hardware,” In Security and Privacy, IEEE Symposium on In Security and Privacy, pp. 18-37, 2016.

[25] Z. Gong and M. X. Makkes "Hardware Trojan side-channels based on physical unclonable functions", WISTP 2011, LNCS 6633 pp. 293-303, 2011.

[26] R. M. Rad, X. Wang, M. Tehranipoor, and J. Plusquellic, "Power supply signal calibration techniques for improving detection resolution to hardware trojans," IEEE/ACM International Conference on Computer-Aided Design (ICCAD '08), pp. 632-639, 2008.

[27] J. Yier, N. Kupp, Y. Makris, "Experiences in Hardware Trojan design and implementation," IEEE International Workshop on Hardware-Oriented Security and Trust (HOST 2008), pp. 50-57, July 2009.

[28] J. Clark, S. Leblanc, S. Knight, "Risks associated with USB Hardware Trojan devices used by insiders," 2011 IEEE International on Systems Conference (SysCon), pp. 201-208, April 2011.

[29] L. W. Kim and J. D. Villasenor, "A System-On-Chip Bus Architecture for Thwarting Integrated Circuit Trojan Horses," in IEEE Transactions

on Very Large Scale Integration (VLSI) Systems, vol. 19, no. 10, pp. 1921-1926, Oct. 2011.

[30] R. Rad, J. Plusquellic, M. Tehranipoor, "Sensitivity analysis to hardware Trojans using power supply transient signals," IEEE International Workshop on Hardware-Oriented Security and Trust (HOST 2008), pp. 3-7, June 2008.

[31] M. Banga and M. Hsiao, "A Region Based Approach for the Identification of Hardware Trojans," Proc. IEEE International Workshop Hardware-Oriented Security and Trust, 2008, pp. 40-47.

[32] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, "MERO: a statistical approach for hardware Trojan detection," Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, 2009, pp. 396-410.

[33] S. Jha and S. K. Jha, "Randomization Based Probabilistic Approach to Detect Trojan Circuits," Proc. 11th IEEE High Assurance Systems Engineering Symp. , IEEE CS Press, 2008, pp. 117-124.

[34] F. Wolff, C. Papachristou, S. Bhunia, and R. S. Chakraborty, "Towards Trojan-Free Trusted ICs: Problem Analysis and Detection Scheme," Design, Automation and Test in Europe, pp. 1362-1365, March 2008.

[35] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, B. Sunar, “Trojan detection using IC fingerprinting,” IEEE Symposium on In Security and Privacy, pp. 296-310, 2007.

[36] L. Lin, W. Burleson, and C. Paar, "MOLES: malicious off-chip leakage enabled by side-channels," IEEE/ACM International Conference on Computer-Aided Design (ICCAD '09), pp. 117-122, 2009.

[37] S. Bhasin, J.-L. Danger, S. Guilley, X. T. Ngo, L. Sauvage, "Hardware Trojan Horses in Cryptographic IP Cores," Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pp. 15-29, Aug. 2013.

[38] J. Balasch, B. Gierlichs and I. Verbauwhede, "Electromagnetic circuit fingerprints for Hardware Trojan detection," 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC), Dresden, 2015, pp. 246-251.

[39] M. Kinugawa, Y. Hayashi,“Evaluation of Information Leakage caused by Hardware Trojans Implementable in IC Peripheral Circuits, 2016 Asia-Pacific Symposium on Electromagnetic Compatibility, 2016.