Side Channel Attacks on Smart Home Systems: A Short Overview

Mohammad Ali Nassiri Abrishamchi[*1,2], Abdul Hanan Abdullah[1],
Adrian David Cheok[1,2,3] and Kevin S. Bielawski[2]

[1]Faculty of Computing, Universiti Teknologi Malaysia, 81310 Skudai, Malaysia
[2]Imagineering Institute, Iskandar, Malaysia, [3]City, University of London, London, UK

ali@imagineeringinstitue.org, hanan@utm.com,
adrian@imagineeringinstitue.org, kevin@imagineeringinstitue.org

***Abstract*— This paper provides an overview on side-channel attacks with emphasis on vulnerabilities in the smart home. Smart homes are enabled by the latest developments in sensors, communication technologies, internet protocols, and cloud services. The goal of a smart home is to have smart household devices collaborate without involvement of residents to deliver the variety of services needed for a higher quality of life. However, security and privacy challenges of smart homes have to be overcome in order to fully realize the smart home. Side channel attacks assume data is always leaking, and leakage of data from a smart home reveals sensitive information. This paper starts by reviewing side-channel attack categories, then it gives an overview on recent attack studies on different layers of a smart home and their malicious goals.**

Keywords*— *Smart home, Privacy, Side-channel attack

I. INTRODUCTION

As the concept of digitalization becomes a main trend in almost every aspect of modern life, promising applications of the internet of things (IoT) are becoming tangible and practical, from smart phones to smart vehicles and smart living environments [1-3]. Thus, the idea of a "smart home" is much closer to becoming reality. Initial thoughts about smart homes [4-7] have changed in recent years due to significant advancement in IoT-enabler technologies, such as sensor technology, small-sized and affordable processors, small actuators, artificial intelligence techniques, such as machine learning and deep learning, cognitive technologies, and cloud computing. Researchers and developers are now emphasizing the potential of a smart home to improve the quality of human life [8]. Already, products and services for smart home applications are being developed by companies around the world [10]. Despite the desirable qualities offered by a smart home, the smart home can also introduce vulnerabilities related to security and privacy issues [11], [12]. Generally, people spend most of their private moments in their homes. Overcoming smart home privacy issues is a critical challenge for wide adoption of smart homes. Even if personal information is not stolen by adversaries, people still have differing concerns about sharing personal information related to in-home activities [13]. Thus, having practical and efficient solutions for overcoming privacy drawbacks is critical.

The internet of things uses sensors to collect a large amount of data, and all kinds of activities can be detected and recorded by a smart home. Due to the large amount of data being collected, any type of data leakage can cause unpredictable and undesirable consequences.

Data privacy protection falls into two major categories. The first category is protecting sensitive and private content of messages transmitted through the home network. Approaches in this category mainly use cryptographic techniques [14]. In the second category, concerns are about the context of data, such as identities of communicators, temporal data, and absolute or relative locations of the targeted smart devices. Hackers can apply a wide range of side-channel attacks (SCAs) on both privacy protection categories to achieve malicious aims, such as monitoring hidden in-home activity. In this paper, our focus is on SCAs that attack contextual data, i.e. the second category, where exchanged data between home appliances is not as important as their identities, locations, and functions. Fig. 1 shows a classification of data privacy and related attacks and defenses.

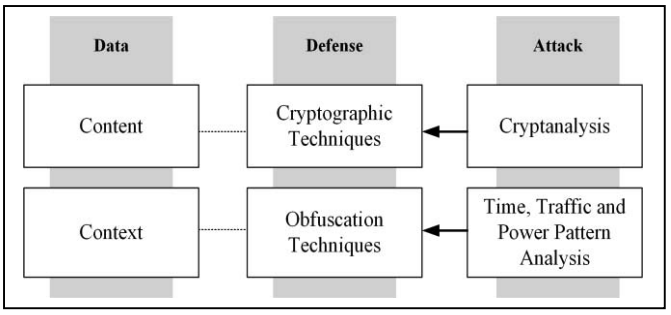


Fig. 1. Types of data privacy, attack methods, and countermeasure techniques.

In this paper, our aim is to provide an overview of potential threats in smart home. It will aid researchers, developers, engineers, and designers in their research or development to propose novel solutions and identify other vulnerabilities.

The reminder of this paper is organized as follows: section II describes the concept of the side-channel attack and different types of SCAs, section III introduces SCAs on smart

978-1-5386-1127-2/17/$31.00 ©2017 IEEE

home systems based on application, and section IV provides a conclusion.

II. Side Channel Attack

From the physical security point of view, attacks can be divided into three classes: invasive, semi-invasive, and non-invasive. An invasive attack needs physical engagement with the device which results in the destruction of the device. An example of an invasive attack is using a chemical approach to determine the layout of a circuit that results in the loss of operation of the circuit. Semi-invasive attacks require physical modification to, but not the destruction of, the target device, such as opening a package for direct access to the enclosed circuits. Non-invasive attacks only utilize externally accessible information, such as power consumption, temporal data, or network traffic [15].

The concept of SCAs assumes that data is always leaking, which provides the possibility for adversaries to exploit data leakage of a smart device to find meaningful correlation patterns between events and/or communication nodes. Consequently, they will be able to obtain some sensitive private data for their malicious misuses [16].

Considering the attack behavior, there are two types of SCAs: passive attacks and active attacks. If an attack only exploits the output of a system, for example, monitoring the network traffic and analyzing the observations to discover desired information, this attack is working passively. On the other hand, an active attack starts from system input and continues collecting system output, such as an attack that provides some predefined events for sensors, then studies the response of the device to those events to find secret information [15]. Fig. 2 shows the relationship between physical security attack and SCAs.

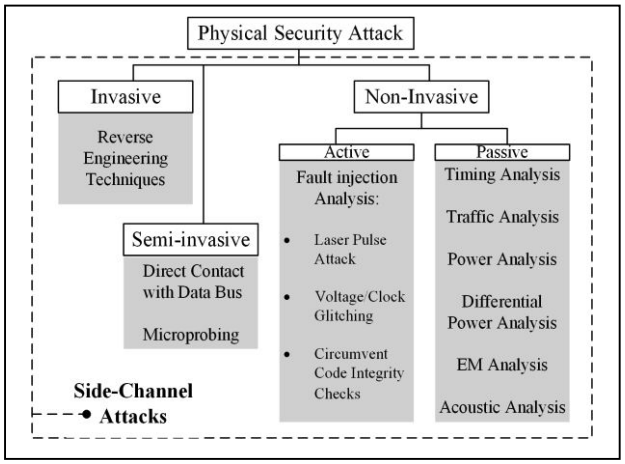


Fig. 2. Taxonomy of physical security attacks.

In addition to performing computing tasks, microelectronic devices generate physical phenomena that makes them vulnerable to side-channel attacks. Each component of a device can be subject to one or multiple SCAs. The following are brief descriptions of the main types of these attacks:

A. Timing Analysis:

A timing analysis investigates the associated timestamps assigned to each event, such as packet transmission in a network or encoding and decoding operations by a smart device. The timing analysis can reveal secret information about the system. This attack is useful for global eavesdroppers when they are looking for contextual information of a wireless network [17], [18].

B. Traffic Analysis:

A traffic analysis involves an attacker that, by monitoring all or a part of network traffic, can track data packets, count packet number, and record their transmission intervals. This analysis is useful when identifying the sender, receiver, or both, and spotting their locations is needed [19].

C. Electromagnetic Analysis:

Cryptographic devices performing encryption or decryption tasks emit power radiation of electromagnetic fields. In this type of attack, adversaries exploit leaked radiation for performing electromagnetic analysis to find correlations between leaked radiation and ciphertext. Since this radiation can be captured remotely, depending on the receiver equipment strength, this side-channel attack can be performed from a distance and hackers do not need to be close to the target [20].

D. Simple Power Analysis (SPA):

Visual observation of consumed power alterations during execution of encryption algorithms enables attackers using a simple power analysis to figure out which encryption method is being applied on the signal. But existence of various current spikes and noises is a challenge for this method [21].

E. Differential Power Analysis (DPA):

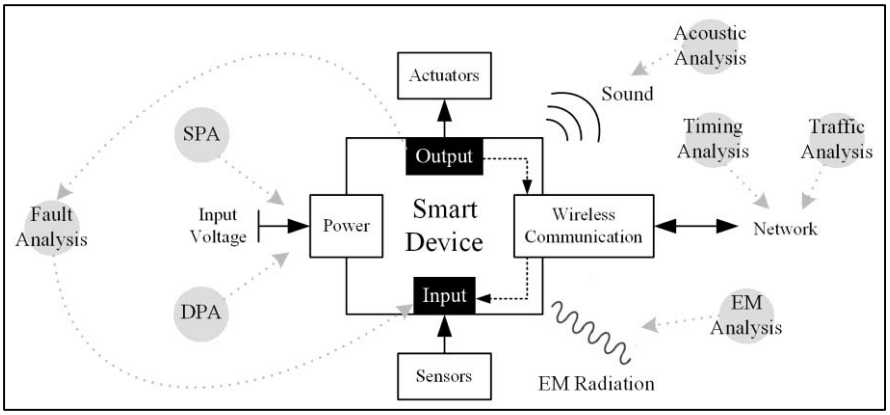
Applying statistical error-correcting methods through visual data monitoring of electrical power can lead to discovering the encryption key through a differential power analysis. Unlike SPA, in this approach analysis of power consumption will be done on both non-cryptographic operations and cryptographic operations, then results will be compared. All cryptographic approaches and their hardware are vulnerable to this class of SCA [15], [22].

F. Fault Analysis:

Fault analysis injects various types of faults into cryptographic devices and analyzes the output of the system. [23] states that useful techniques for finding encryption patterns involve changing physical conditions of the hardware, such as increasing the temperature, injecting fake packets for raising the collision likelihood, or applying a laser beam at a particular frequency.

G. Acoustic Analysis:

Sound produced by electromechanical devices is another source for attackers to gain secret information via analysis of associated acoustic oscillations. A trained model can be capable of distinguishing between sounds that are slightly different. In



Overview of side-channel attacks on a smart device

order to launch this attack, a simple digital sound reordering system can be sufficient, such as a smart phone [24], [25].

Fig. 3. illustrates an overview on a smart device, its components and associated side-channel attacks.

III. Vulnerable Smart home systems

As one of the most promising applications of the IoT, smart homes combine various types of smart systems to provide a better domestic life environment through intelligent interaction with residents. To develop a smart home, four layers of connected automation systems are considered: infrastructure layer, ambient condition management layer, application layer, and security layer. Systems related to multimedia, household appliances, and healthcare monitoring fall into the application layer. The ambient condition management layer includes systems for controlling temperature, humidity, air freshness, and lighting management. The security layer consists of different types of access control solutions, such as access cards, biometric authentication systems, and surveillance approaches. Finally, the infrastructure layer is a group of technologies for dealing with energy and water consumption management, such as smoke detectors and fire extinguishers. Table 1 provides an overview of systems and devices in each layer. This section will provide examples of studies done to compromise devices in each layer.

A. *Application Layer:*

In a practical experiment by [26], four types of smart TVs are investigated to explore possible vulnerabilities. The authors managed to successfully modify firmware of a smart TV. They discussed three types of firmware analysis techniques: firmware updates analysis, physical access, and debugging interfaces. Firmware update analysis involves reverse engineering the update packages, impersonating the TV, or compromising raw binary firmware. In the physical access approach modification is enabled by desoldering the memory chip which contains the firmware and replacing it with a new chip. Finally, to debug interfaces, serial ports and JTAG interfaces are misused. A compromised serial port can give access to the bootloader prompt. JTAG interfaces are used for CPU debugging and allow flash memory modification. In this experiment, physical access to the targeted TV, or access to at least one of the local networks, is needed.

In [27], recognition of the content being watched on TV was discerned from the diffusion of light from the screen. The authors claim this attack is robust and efficient, and light emanation from windows is sufficient to perform their two-stage approach. First, feature extraction is performed from recorded changes in light emission. Second, video retrieval, using a pre-computed library of features is extracted from the reference content.

Voice communication is a common activity in every home. [28] proposed a novel attack to identify speakers despite encrypted voice communication. The authors exploit a technique used for reducing voice traffic loads to save bandwidth. This technique is called voice activity detection (VAD). The authors have shown that using the VAD approach generates patterns in encoded network traffic, and traffic patterns can be associated with the characteristics of the person speaking.

[29] provides an example of an acoustic side-channel attack on printers. In this work, the authors presented a novel attack that can recreate English text that is printed by recording the sound of the printer during the process. This attack benefits from a combination of machine learning, speech recognition, and audio processing. They reported that this attack can be successful on dot matrix printers, which are still in use in many organizations.

[30] describes a new side channel attack called PIN skimmer that targets mobile computers. This attack is able to exploit compromised cameras and microphones installed in the smart home to discover entered PINs in soft keyboards. A microphone detects the touch event, and data from the camera is used to estimate the orientation of the device then correlates it to the position of the tapped area on the screen to find the related digit.

In [31], an eavesdropping attack on a wearable device is implemented. Researchers were successful in detecting physical activity levels based on correlation between sensed in-home activities and changes in the network traffic, which was

Table 1. Devices and systems in each layer of a smart home

Application Layer	Multimedia Systems	Smart TV, Smart audio player, …
	Smart Household Appliances	Smart Fridge, Smart vacuum cleaner, …
	Healthcare Monitoring Systems	Child/Elderly fall detection, …
	Waste Management	Smart recycling system, …
Ambient Condition Management Layer	Smart Air Con	Smart Thermostat
	Smart Lighting System	Natural Light (Curtains, Shades)
		Electrical Light
		Noise Level Control
Security Layer	Access Control Systems	RFID access card system
		Biometric authentication system
	Surveillances System	CCTV
		Sensory Intrusion Detection System
Infrastructure Layer	Communication Network	Wireless Network (WiFi, Bluetooth, Zig
		Wired Network
	Utilities	Energy Management System
		Water Consumption Monitoring System
	Safety	Smoke Detection System
		Fire Extinguisher System
		Gas Leakage Detection

measured using the signal strength. They validated their attack with real data collected from their wearable prototype.

[32] emphasizes privacy threats on smart devices with built-in microphones set to be "always on", for example, smart TVs and their voice searching feature or systems using the Google Chrome search engine for its ability to passively listen for the phrase "OK, Google". Digital assistants, such as Alexa or Siri, are vulnerable in the same way. [33] concentrated on smart toys. They can interact with children and, due to their connection to the network, they can leak private data through online attacks.

B. Ambient Condition Management Layer:

In [34], the authors implemented an experiment on Google's Nest. They argued that, since Nest devices send user data to the server, intercepting this data can reveal sensitive information. They state it can even be done by a script kiddie attack (shared malicious scripts developed by sophisticated hackers, performed by beginner hackers). Due to credential leakage, hackers can take the full control of the device. They suggested that, instead of performing learning algorithms on the server side, the attack can be performed locally by each individual device, and Nest is powerful enough to perform a simple learning algorithm.

In another study on Google's Nest, [35] managed to install malicious software by bypassing firmware verification of the device. As a result, the attacker gains access to all available information stored on the memory. Moreover, attackers can change the behavior of the compromised device and use it to perform similar attacks on other devices within the local network.

In yet another work on Google's Nest [36], the Nest smoke and carbon dioxide detectors are exploited to detect home occupancy. This work shows how it is possible to achieve a high accuracy rate by performing a traffic analysis attack, even if the data is encrypted.

Zigbee Light Link (ZLL), a low power network, is designed to be used by smart lighting systems. [37] introduced a novel attack on smart homes that use this system to take full control of the system after bypassing all pre-designed security defense considerations. They tested three popular smart lighting systems: Osram Litify, Philips Hue, and GE Link, and all of them are vulnerable to this attack.

In research conducted by [38], vulnerability of visual light communication (VLC) is investigated. VLC is considered to be secure from eavesdropping attacks, because, unlike radio waves, light cannot pass through walls. However, the authors showed that a small gap under a door, keyholes, and covered windows can be enough for an attacker to intercept and decode the message packets, even outside of the direct beam. Captured traffic can then be used for timing or traffic analysis attacks.

C. Security Layer

[39] investigates a video surveillance system. The authors reported that difference coding, which is a highly efficient approach for compressing video streams, causes data leakage. Encrypted compressed video shows distinguishable changes in traffic patterns that can be correlated with basic in-home activities. When there is no video stream being transferred, the size of an encrypted data stream is much smaller than that when there is a stream. Authors performed experiments to show that activities such as styling hair, moving, and eating are detectable with high accuracy.

Another work is focused on security of smart locks. Authors investigated number of available smart locks in the market: Kevo, August, Dana, Okidokeys and Lockiton. Most of these locks are using device-gateway-cloud (DGC) architecture. Based on the working mechanism of these devices, two classes of attacks are introduced: revocation evasion and access log evasion. All tested smart locks have an option to revoke other user's access by the owners. This feature can be exploited in a revocation evasion. However, these devices have access logging features to inform owners of unauthorized access. The logging feature can be overcome with an access log evasion, where the attacker prevents the recording process [40].

D. Infrastructure Layer

[41] showed that service providers can exploit power consumption levels to enhance their services. However, these

data can also reveal in-home activity patterns. To investigate the effects of this privacy attack, they implement an attack known as non-intrusive appliance load monitoring (NIALM) to discover how privacy of energy consumption data can be preserved while still providing services. To address this issue, they proposed a masking approach where the smart meter masks data then sends it to the provider. In order to be effective, this masking should not affect the outcome of the aggregating operations.

Table 2. Smart home systems attack overview

Layer	Smart System	Attack Objective	Reference
Application	Smart TV	To take control	[25]
		To Discover content being watched	[26]
	Voice Communication	To Identify speakers	[27]
	Printer	To recreate printed English text	[28]
	Touch screen devices	PIN discovery	[29]
	Wearable devices	To discover in-home activities	[30]
	Devices with built-in microphone	Eavesdropping	[31]
Ambient Condition Control	Smart Thermostat	To access to secret to information	[32]
		To access to data and taking control of device	[33]
		Occupancy detection	[35]
	Smart Lighting	Full control	[31]
	Visual light communication network	Eavesdropping	[37]
Security	Surveillance system	To discover in-home activities	[38]
	Smart lock	To home access	[39]
Infrastructure	Smart metering	To discover in-home activities	[41], [42], [43]
		Occupancy detection	[43]
		Specific activity detection: pair laptop-user	[44]
	Network	To discover in-home activities	[45], [46], [47]

In another work, the possibility of private in-home activity recognition is demonstrated. A NIALM attack is used to reveal private activities, such as how much one sleeps, when one leaves for work, if a child is home alone, and whether one's breakfast is hot or cold. The proposed solution is called zero-knowledge (ZK) billing protocol, consisting of three steps: registration, tuple gathering, and reconciliation. Moreover, a formulated leakage model is presented to ensure adequate privacy [42].

In [43], the authors performed a layered hidden Markov model (LHMM) to discover whether it is possible to deduce activities of daily living (ADL) from patterns of associated power consumption. They found that all ADLs are not detectable with this attack due to low sample size for some activities, such as washing dishes or using air exhaust. To overcome this problem, they proposed a hierarchical Dirichlet process hidden Markov model (HDP-HMM) to model the emission probability with a mixture of gaussian distributions and demonstrated that this method perform better than other models in detecting ADLS.

In [44], the authors conducted an experiment to demonstrate occupancy detection by performing a common classification technique based on data gathered by network-connected energy meter equipment. The authors found that, by considering features such as mean, standard deviation, and sum of the absolute differences of each power phase, it is possible to achieve to up to 80% accuracy in determining home occupancy.

[45] designed a framework called MTPlug using supervised machine learning techniques. This attack aims to detect laptop-users by exploiting power consumption data collected from either household level sensors or wall-socket level sensors. Results show that they can reach to up to 80% accuracy in a relatively short time. This laptop energy trace can lead to privacy threats, for example identification or position tracking.

A fingerprint and timing-based snooping (FATS) attack aims to reveal in-home activities using timing analysis. By logging fingerprints and associated timestamps of communication from each wireless device, the attack performs a four-tier classification to identify each device, its location, and its function. Therefore, each action in the home is exposed to attackers. [46] introduced this attack, and [47], [48] have shown potential solutions to this attack.

Attacks discussed in this section are summarized in Table 2. The table is organized based on the system under attack and the goal of the attack.

IV. Conclusion

The emergence of smart homes affects various aspects of a user's life. They will be monitored by a number of sensors, including cameras, microphones, motion detectors, and activity loggers. All of these systems are intended to provide useful services for a better quality of life; however, they also increase privacy concerns due to data leakage. In this paper, we provided an insight of how adversaries can use side-channel attacks to exploit smart home vulnerabilities. We discussed the significance of privacy issues in smart home environments and how vulnerable they are to side-channel attacks. Seven major types of SCAs were introduced, and a review on recent privacy attacks on different aspects of smart home systems was provided.

REFFERENCES

[1] I. U. Khan, M. U. Shahzad, and M. A. Hassan, "Internet of Things (IoTs): Applications in Home Automation," *IJSEAT,* vol. 5, pp. 079-084, 2017.

[2] F. Wortmann and K. Flüchter, "Internet of things," *Business & Information Systems Engineering,* vol. 57, pp. 221-224, 2015.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems,* vol. 29, pp. 1645-1660, 2013.

[4] S. Davidoff, M. K. Lee, C. Yiu, J. Zimmerman, and A. K. Dey, "Principles of smart home control," in *International Conference on Ubiquitous Computing*, 2006, pp. 19-34.

[5] R. Harper, *Inside the smart home*: Springer Science & Business Media, 2006.

[6] L. Jiang, D.-Y. Liu, and B. Yang, "Smart home research," in *Machine Learning and Cybernetics, 2004. Proceedings of 2004 International Conference on*, 2004, pp. 659-663.

[7] S. H. Park, S. H. Won, J. B. Lee, and S. W. Kim, "Smart home–digitally engineered domestic life," *Personal and Ubiquitous Computing,* vol. 7, pp. 189-196, 2003.

[8] S. Solaimani, W. Keijzer-Broers, and H. Bouwman, "What we do–and don't–know about the Smart Home: an analysis of the Smart Home literature," *Indoor and Built Environment,* vol. 24, pp. 370-383, 2015.

[9] R. S. Ransing and M. Rajput, "Smart home for elderly care, based on wireless sensor network," in *Nascent Technologies in the Engineering Field (ICNTE), 2015 International Conference on*, 2015, pp. 1-5.

[10] M. E. Porter and J. E. Heppelmann, "How smart, connected products are transforming companies," *Harvard Business Review,* vol. 93, pp. 96-114, 2015.

[11] S. Yoon, H. Park, and H. S. Yoo, "Security issues on smarthome in IOT environment," in *Computer Science and its Applications*, ed: Springer, 2015, pp. 691-696.

[12] F. K. Santoso and N. C. Vun, "Securing IoT for smart home system," in *Consumer Electronics (ISCE), 2015 IEEE International Symposium on*, 2015, pp. 1-2.

[13] K. Islam, W. Shen, and X. Wang, "Security and privacy considerations for wireless sensor networks in smart home environments," in *Computer Supported Cooperative Work in Design (CSCWD), 2012 IEEE 16th International Conference on*, 2012, pp. 626-633.

[14] G. C. Kessler, "An Overview of Cryptography (Updated Version 26 February 2017)," 2017.

[15] F.-X. Standaert, "Introduction to side-channel attacks," in *Secure Integrated Circuits and Systems*, ed: Springer, 2010, pp. 27-42.

[16] K. Mai, "Side Channel Attacks and Countermeasures," in *Introduction to Hardware Security and Trust*, ed: Springer, 2012, pp. 175-194.

[17] Y. F. Alias, M. A. M. Isa, and H. Hashim, "Timing Attack: An Analysis of Preliminary Data," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC),* vol. 9, pp. 29-32, 2017.

[18] K. Pongaliur, Z. Abraham, A. X. Liu, L. Xiao, and L. Kempel, "Securing sensor nodes against side channel attacks," in *High Assurance Systems Engineering Symposium, 2008. HASE 2008. 11th IEEE*, 2008, pp. 353-361.

[19] Y.-K. Chen, "Challenges and opportunities of internet of things," in *Design Automation Conference (ASP-DAC), 2012 17th Asia and South Pacific*, 2012, pp. 383-388.

[20] J. Longo, E. De Mulder, D. Page, and M. Tunstall, "SoC it to EM: electromagnetic side-channel attacks on a complex system-on-chip," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2015, pp. 620-640.

[21] S. B. Örs, E. Oswald, and B. Preneel, "Power-analysis attacks on an FPGA–first experimental results," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2003, pp. 35-50.

[22] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," *Journal of Cryptographic Engineering,* vol. 1, pp. 5-27, 2011.

[23] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Smart meters for power grid: Challenges, issues, advantages and status," *Renewable and sustainable energy reviews,* vol. 15, pp. 2736-2742, 2011.

[24] A. Shamir and E. Tromer, "Acoustic cryptanalysis: On nosy people and noisy machines, 2004," *Preliminary Proof-of-Concept Presentation*.

[25] G. Deepa, G. SriTeja, and S. Venkateswarlu, "An Overview of Acoustic Side-Channel Attack," *International Journal of Computer Science & Communication Networks,* vol. 3, p. 15, 2013.

[26] Y. Bachy, F. Basse, V. Nicomette, E. Alata, M. Kaâniche, J.-C. Courrège*, et al.*, "Smart-TV security analysis: practical experiments," in *Dependable Systems and Networks (DSN), 2015 45th Annual IEEE/IFIP International Conference on*, 2015, pp. 497-504.

[27] Y. Xu, J.-M. Frahm, and F. Monrose, "Watching the watchers: Automatically inferring tv content from outdoor light effusions," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 418-428.

[28] M. Backes, G. Doychev, M. Dürmuth, and B. Köpf, "Speaker recognition in encrypted voice streams," in *European Symposium on Research in Computer Security*, 2010, pp. 508-523.

[29] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic Side-Channel Attacks on Printers," in *USENIX Security symposium*, 2010, pp. 307-322.

[30] L. Simon and R. Anderson, "Pin skimmer: Inferring pins through the camera and microphone," in *Proceedings of the Third ACM workshop on Security and privacy in smartphones & mobile devices*, 2013, pp. 67-78.

[31] X. Fafoutis, L. Marchegiani, G. Z. Papadopoulos, R. Piechocki, T. Tryfonas, and G. Oikonomou, "Privacy Leakage of Physical Activity Levels in Wireless Embedded Wearable Systems," *IEEE Signal Processing Letters,* vol. 24, pp. 136-140, 2017.

[32] S. GRAY, "Always On: Privacy Implications of Microphone-Enabled Devices," in *Future of privacy forum*, 2016.

[33] A. Rutkin, "Hello creepy," ed: Elsevier, 2016.

[34] M. Moody and A. Hunter, "Exploiting known vulnerabilities of a smart thermostat," in *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*, 2016, pp. 50-53.

[35] G. Hernandez, O. Arias, D. Buentello, and Y. Jin, "Smart nest thermostat: A smart spy in your home," *Black Hat USA,* 2014.

[36] B. Copos, K. Levitt, M. Bishop, and J. Rowe, "Is Anybody Home? Inferring Activity From Smart Home Network Traffic," in *Security and Privacy Workshops (SPW), 2016 IEEE*, 2016, pp. 245-251.

[37] P. Morgner, S. Mattejat, and Z. Benenson, "All Your Bulbs Are Belong to Us: Investigating the Current State of Security in Connected Lighting Systems," *arXiv preprint arXiv:1608.03732,* 2016.

[38] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. Knightly, "The spy next door: Eavesdropping on high throughput visible light communications," in *Proceedings of the 2nd International Workshop on Visible Light Communications Systems*, 2015, pp. 9-14.

[39] H. Li, Y. He, L. Sun, X. Cheng, and J. Yu, "Side-channel information leakage of encrypted video stream in video surveillance systems," in *Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on*, 2016, pp. 1-9.

[40] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart locks: Lessons for securing commodity internet of things devices," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 2016, pp. 461-472.

[41] P. Barbosa, A. Brito, and H. Almeida, "Defending against load monitoring in smart metering data through noise addition," in *Proceedings of the 30th Annual ACM Symposium on Applied Computing*, 2015, pp. 2218-2224.

[42] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*, 2010, pp. 61-66.

[43] Y. Tang and C. Ono, "Detecting Activities of Daily Living from Low Frequency Power Consumption Data," in *Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2016, pp. 38-46.

[44] W. Kleiminger, C. Beckel, T. Staake, and S. Santini, "Occupancy detection from electricity consumption data," in *Proceedings of the 5th ACM Workshop on Embedded Systems For Energy-Efficient Buildings*, 2013, pp. 1-8.

[45] M. Conti, M. Nati, E. Rotundo, and R. Spolaor, "Mind The Plug! Laptop-User Recognition Through Power Consumption," in *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, 2016, pp. 37-44.

[46] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting your daily in-home activity information from a wireless snooping attack," in *Proceedings of the 10th international conference on Ubiquitous computing*, 2008, pp. 202-211.

[47] H. Park, C. Basaran, T. Park, and S. H. Son, "Energy-efficient privacy protection for smart home environments using behavioral semantics," *Sensors,* vol. 14, pp. 16235-16257, 2014.

[48] M. A. Nassiri Abrishamchi, Abdul Hanan Abdullah, A. David Cheok, and P. K. Nikolic, "A probability based hybrid energy-efficient privacy preserving scheme to encounter with wireless traffic snooping in smart home," presented at the Mobility IoT 2016, Bratislava, 2016.