IoE Security Threats and You

Jungwoo Ryoo*, Soyoung Kim†, Junsung Cho†, Hyoungshick Kim†, Simon Tjoa‡, Christopher V. DeRobertis§
*Penn State Altoona, 3000 Ivyside Park, Altoona PA 16601
jryoo@psu.edu
†Sungkyunkwan University
{ksy2608, js.cho, hyoung}@skku.edu
‡JRZ TARGET, St. Pölten University of Applied Sciences
Simon.Tjoa@fhstp.ac.at
§IBM
dero@us.ibm.com

***Abstract*—Internet of Everything (IoE) is a newly emerging trend especially in homes. Marketing forces towards smart homes are also accelerating the spread of IoE devices in households. An obvious danger of rapid adoption of these gadgets is that many of them lack controls for protecting the privacy and security of end users from attacks designed to disrupt lives and incur financial losses. Our research goal for this paper is to develop an IoE threat model geared specifically for home users who are often unaware of the privacy and security threats which the IoE appliances pose. Our ultimate goal is to propose an effective solution to alerting users of imminent IoE security threats and offering actionable steps to mitigate them through an intuitive and friendly user interface design. There have been ample security research on individual elements of IoE. In particular, there are many publications on Internet of Things (IoT) security. What differentiates our research from the existing IoT works is that we are treating IoT as a component of an IoE ecosystem and developing our threat model in the more comprehensive context of how other pieces of the equation, such as people and data as well as processes fit together to result in formidable security threats.**

I. Introduction

The Internet of Everything (IoE) encompasses data, people, Internet of Things (IoT), and processes. IoE builds on the concept of IoT which focuses on connecting network devices equipped with specialized sensors through the Internet. The sensors can detect and respond to changes in their environment, including light, temperature, sound, vibration, etc. IoE dramatically expands the scope of IoT by adding components that can further provide richer experiences for businesses, individuals, and countries. For example, instead of simply relying on things to interact with their environments, as shown in Figure 1, IoE can leverage all related data and processes to make IoT more relevant and valuable to people. The ultimate goal of IoE is to boost operational efficiency, offer new business opportunities, and improve the quality of our life. To better relate to this idea, take the scenario of a person who is not sure about closing a gas valve at home. An IoE solution allows a user to automatically check the status of the gas valve and can close it remotely if necessary.

However, despite all of its potential rewards, IoE could also pose significant security threats to its adopters. The number of IoE devices around us is steadily increasing, and IoE is

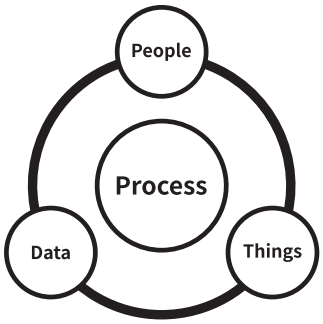

Fig. 1. Definition of Internet of Everything (IoE)

starting to play a more important role in our everyday lives. In particular, the link between the physical world and cyberspace established by IoE increases the risk of cyber attacks targeting IoE devices, since attacks against IoE can directly impact the health and welfare of their end users. Building on our gas valve scenario, you can easily imagine a threat scenario in which an attacker causes a gas leak on purpose.

Even more alarming is the fact that we are often oblivious to the quantity and nature of the IoE devices surrounding us, not to mention the potential security risks they represent. The recent security incidents resulting from IoE security vulnerabilities corroborate this observation. In particular, one of them is a Distributed Denial of Service (DDoS) attack against Dyn [1] in October 2016. This incident involved a botnet called Mirai, consisting of approximately 100,000 IoE hosts, including digital cameras and routers. The Mirai botnet launched DDoS attacks against Dyn and brought down its Domain Name Servers (DNS). This, in turn, resulted in outage of major commercial websites (e.g., Netflix and CNN).

Although not publicized as an IoE attack, the Target data breach in 2013 [2] is now traced back to a vulnerability in their Heating, Ventilation and Air Conditioning (HVAC) system that was connected to the rest of the company network, including Target retail stores. It turns out that Target provided network access to a third-party vendor that needed it for controlling and monitoring their HVAC system. Attackers obtained a user credential of the HVAC company network, which eventually

allowed them to access Target's Point of Sale (PoS) devices.

Due to these emerging threats, it is imperative to raise awareness on potential IoE security risks among end users through systematic risk assessment and effective visualizations. Home users are especially vulnerable because they are increasingly surrounded by IoE appliances (e.g., hands-free speakers, baby monitors, security cameras, etc.) but lack the resources and skills to identify their own IoE-related threats, remediate them, and ultimately minimize the potential security risks. Therefore, the overall research goal of this paper is to establish an IoE threat model geared toward home users to help them better protect their home network environments.

To accomplish this goal in home networks, we first identify IoE assets that could be susceptible to cyber security attacks. Next, we analyze a typical home network system and its entry points that can eventually lead to unauthorized access to household IoE devices. We then elicit and document threats in the form of threat scenarios. Once specified, we prioritize the threats according to their risk levels. Finally, we discuss some potential solutions to address security issues in home networks.

II. Related work

The IoE connects people, data, things, and processes to make inter-connectedness easier and more far reaching than ever before [3]. As such, everyday appliances should be subjected to rigorous cyber security testing to the same degrees that these appliances are tested and measured for traditional qualities (e.g., durability, fit-for-purpose, maintenance, etc.); unfortunately, standardized and independent verification of IoE devices, in terms of security, is in its nascent stage, along with IoE security being the focus of legislation and common security criteria [4].

There have been cybersecurity incidents related to IoE in various industries and sectors, such as nuclear facilities, steel mills, energy grids, water supplies, hospitals, and so on [5]. It is expected that the amount of damage will rise by 32%, or 17.7 trillion dollars, by 2020 [6].

Many researchers [7], [8], [9] have tried to address the security issues in Internet of Things (IoT) as an isolated topic unlike our attempt to bring it into the context of a more comprehensive system including additional elements such as people, data, and process (i.e., IoE). For example, Atamli and Martin [10] conducted a threat-based security analysis for IoT. In their paper they develop a threat model consisting of sources of threats, classes of attack vectors, attack impacts, etc. Wang et al. [11] propose a privacy enhancement protocol over Bluetooh Low Energy (BLE) advertising channels. It is based on a 3-way handshake protocol between the peripheral and the gateway for nonce R's deployment. However, this enhancement is really impractical, which requires changing both the protocol and the peripheral.

Bangali et al. [12] propose an IoE-driven security system that utilizes a web camera to detect the motion of an intruder in the camera range when the owner is away from the home. When an intrusion is detected, a security alert is delivered to the owner, which relies on a Short Message Service (SMS) based on the GSM (Global System for Mobile communications) technology.

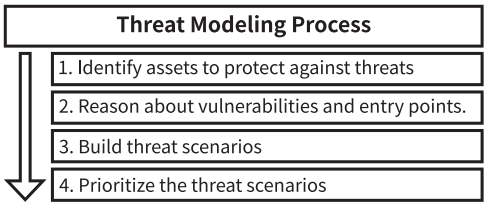

Fig. 2. Threat Modeling Process

Our paper complements their work by providing an IoE-centric network security solution. The physical security service becomes useless when the home network infrastructure is compromised, which could, in turn, make the webcam-based system fail. Ensuring home network security is integral to physical security especially when considering the presence of many IoE-based physical security devices that rely on the integrity of the home network. Therefore, developing an IoE threat model for home users who are often unaware of the privacy and security threats is the first step towards improving home physcial security.

III. Threat modeling

In this paper, we use the Microsoft SDL tool [13] which lays out the steps to take to prioritize security risks and develop ways to efficiently mitigate them in a systematic manner (see Figure 2). In the Microsoft's SDL process, the first step is to identify assets to be protected against threats. In our research, a majority of these assets are household appliances connected to a home network. The next step is to reason about vulnerabilities and entry points. We examine specific vulnerabilities associated with home IoE devices and entry points into a network in which the target devices of potential attacks exist. Knowing these weaknesses facilitated the process of building threat scenarios which concretely show how attackers can launch various attacks against IoE devices in a home setting. The last step in the Microsoft's SDL process was to prioritize the threat scenarios so that its users become aware of what threats to be addressed first.

To support its threat modeling process, Microsoft also developed a threat classification model called STRIDE [14], which stands for Spoofing identity, Tampering with data, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege. In the following sections, we will use the STRIDE model to aid in producing threat models.

IV. Household IoE assets

Due to the recent advances in *Smart Home* technologies, we are beginning to see more household appliances (see Figure 3) getting connected to our home network [15]. For instance, it is now possible to purchase smart smoke detectors [16]. These detectors are designed to be connected to the Internet and send push notifications to your phone when they detect smoke or if

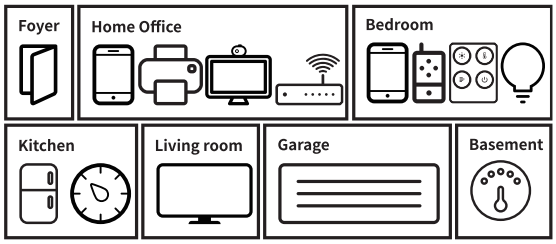

Fig. 3. Household Internet of Everything Assets

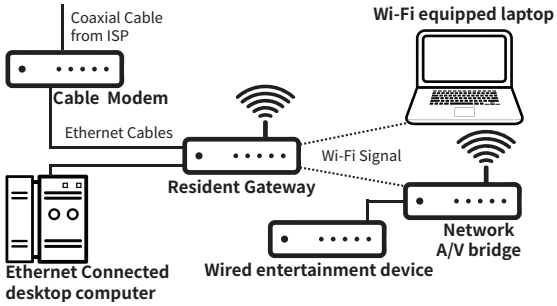

Fig. 4. Example of Home Networks

their battery level is low. Users can also turn off false alarms remotely. The danger here is an attacker taking control over your smart smoke detector and turning it on and off at will.

A. Home Office

Your home office is where this phenomenon is most obvious. In this case, the IoE devices include your cable modem, wireless router, computers, printers, web cameras, and mobile devices like cellular phones and tablets. What about other areas of your residence? In this section, we attempt to enumerate as many home IoE devices as possible by considering the locations where they are usually found.

B. Bedrooms

Some bedrooms are no longer private. Many people keep their cellular phone near their bed when they sleep. Baby monitors are commonplace. Thermostats and light switches are also getting smarter, and people can remotely control them though the Internet. Voice-activated digital assistants such as Amazon Echo are on the rise, too.

C. Kitchen

Among the many appliances found in a kitchen, refrigerators seem to be the first to be connected to the Internet. Smoke alarms are also beginning to be networked. It is also a matter of time for many other kitchen appliances to be part of the rapidly growing home network.

D. Living room

These days living rooms often feature smart TVs. There have already been security incidents involving smart TVs. For example, it was reported recently that ransomware can infect smart TVs [17]. We are also learning that hackers can spy on consumers through the microphone and camera built into a smart TV [18].

E. Foyer

Your front door is a main entrance to your house. It is a critical physical security component regardless of whether your home is smart or not. Smart door locks are available in the market, and an increasing number of households are adopting them.

F. Garage

As with the front door example, garage door is another prime target for smart technology adoption. Criminals may be lurking around your house to scan and record signals from your garage door opener. A simple replay attack is all it takes to open your garage door in this case.

G. Basement

A number of smart devices can be found at your basement, including smart meters for your electricity, gas, and water.

V. Home network architecture and vulnerabilities

Your home network is a microcosm of a full-blown corporate network. It has all the essential elements of a typical computer network. For example, home networks today feature modems, routers, wireless Access Points (APs), switches, repeaters, computers, tablets, Wi-Fi-enabled phone, and other mobile devices. In fact, the only difference between home and corporate networks is the scale. Figure 4 shows a sample home network architecture.

Most homes have a cable or DSL modem that converts analog signals into its digital version. The modem is connected to a router which often serves as a wireless AP, too. Unless the home user is highly proficient with computer networking, the network is usually configured to be monolithic (i.e., a single network without subnets).

A. Entry Points

There are a number of ways for attackers to gain access to your home network.

1) Wireless Signals: Due to the prevalence of Wi-Fi APs, the task is getting even easier. Many of home APs have weak security settings, which include the adoption of no or obsolete encryption and the use of weak or default passwords.

In addition to Wi-Fi, Bluetooth signals are also common in a home environment. Individuals are beginning to acquire an increasing number of Bluetooth devices for personal uses (e.g., Fitbit, scales, headsets, etc.). If inappropriately secured, these Bluetooth devices can easily become gateways to a Wi-Fi or wired network.

There also other types of wireless signals such as ZigBee, but they are much less widespread than Wi-Fi and Bluetooth.

2) Wired Connections: At a minimum, a router connected to a modem has a public IP and is therefore accessible from the Internet. As a result, an Internet-facing router serves as a major entry point to a home network and susceptible to various intrusion attempts.

B. Vulnerabilities

The monolithic network architecture used by households is a major vulnerability. Once intruders bypass the security countermeasures placed at the entry points discussed in section V-A, they have access to the entire home network.

The entry points associated with the wireless signals are vulnerable to Denial of Service (DoS) attacks, eavesdropping, Man-In-The-Middle (MITM) attacks, message modification, and resource misappropriation. They are also at the mercy of more specific threats taking advantage of known vulnerabilities stemming from improper implementation of wireless specifications as well as flaws in the wireless standards themselves [19].

VI. Threat scenarios

In this section, we present concrete IoE threat scenarios as one of the final steps of the Microsoft threat modeling process. To build our threat scenario, we first consider one or more IoE assets to be affected. We then elaborate on the entry points and vulnerabilities associated with the assets. Finally, we will complete our threat scenarios by applying one or more of STRIDE threats (i.e., Spoofing, Tampering, Repudiation, Information Disclosure, DoS, and Elevation of Privilege). Table I summarize the approach we are using for developing our threat scenarios.

When deploying or using a new IoT device, stakeholders should analyze threats with the STRIDE model.

Spoofing a person or device in an IoE household can be a serious threat that should be considered. Due to the lack of authorization mechanisms for some IoE devices in the households, it may be possible to change physical settings through digital commands. Examples would include opening Bluetooth smart locks by spoofing passwords transmitted in plain text [21]. Further, recording and audio devices could be used to make orders by using voice-based order assistants such as Alexa [22].

Tampering violates the integrity security property. In a tampering attack parameters can be changed by the attacker causing a different behavior of the devices. Examples would include the alteration of HTTP requests which are sent by GET or POST. Any application on an IoE device which does not check the validity and integrity of messages could become a victim of this attack. Another example would be a SQL injection flaws such as those discovered in various IoT devices [23]

Information leakage causes data which are private to get disclosed to unauthorized users. Home IoE devices record our most sensitive data including conversations [24], videos and pictures [25], or even the most intimate sexual details [26].

Using IoE devices to support and control our daily lives is, without a doubt, a great technological advancement. However, DoS attacks can cause serious problems for home users. A growing threat is ransomware attacks which can be used to hold hostage of devices such as thermostats [27] or smart watches [28]. In order to get their functionality back a ransom has to be paid.

Elevation of privilege attacks use functions which are intended for more privileged accounts. Due to the lack of awareness one of the most common threats is the usage of standard passwords which enable external attackers to act as the administrator of IoE devices. Well known past attacks are Mirai and Hajime [29].

Due to the enormous number of threat scenarios we can develop this way, we limit ours to those most probable and impactful in the home IoE environment based on our own risk assessment.

A. Scenario 1: Compromise

Cyber-attacks are a critical threat to IoE devices. IoE devices use a huge variety of operating systems (and their versions) and applications. The resulting heterogeneity increases the complexity, especially for home users, and therefore complicates the protection. Aggravating this situation is the extensive interconnectedness of IoE devices. In order to stay interoperable with all other IoE systems it is often necessary by default to use insecure communication channels, which further increases the attack surface.

Once an IoE device is compromised, adversaries can use it in several ways for conducting cyber-criminal activities. Firstly, IoE devices under an attacker's control can be federated to a botnet, such as Mirai botnet. Secondly, compromised IoE devices can violate a user's privacy by revealing information such as conversations, video recordings, or use behavior. Thirdly, using ransomware, attackers are able to manipulate or deactivate a device's capability to blackmail users.

Vulnerabilities which could lead to comprises include insecure account settings, outdated operating systems or vulnerable applications.

B. Scenario 2: Eavesdropping and Information Leakage

Home IoE devices are going to monitor and control nearly every facet of our future life. Connected webcams track user behavior, smart devices control the home environment (e.g. heating, air-conditioning, lighting, etc.) or connected security systems (e.g. door locks, alarm systems, etc.) designed to protect the privacy of the family.

As mentioned earlier, information leakage or eavesdropping can cause serious privacy breaches. Video systems, which are implemented to monitor the security of a household, could leak private pictures or videos. Further, smart TVs, game consoles or other voice controlled devices can be used to eavesdrop on conversations. The rich source of information (e.g., TV channels watched, shopping habits using Alexa or similar devices, etc.) about habits and behaviors of home users

STRIDE	Entry Points/Vulnerabilities	Possible Impacts on Assets
Spoofing	replay attacks, session hijacking, unencrypted network traffic, ARP spoofing, IP spoofing, DNS spoofing, sensor data spoofing	packets replayed to open smart locks configuration session captured to change temperature device characteristics (IP, ARP, etc.) spoofed to send commands from a trusted rogue device
Tampering	apps used to change device properties, changing IoT device files, installing backdoors or unwanted programs, modifying network packages, injection attacks, malicious software updates	ransomware attacks encrypting data files devices turned into bots private data (e.g., videos) retrieved through the lack of input validation
Repudiation	transactions carried out in the name of a user	Ordering of new services and products
Information Disclosure	cleartext account credentials, unencrypted network traffic (e.g., pictures, conversations, etc.), loss of personal data (e.g., stored pictures, videos, etc.), profiling behaviors (e.g., daily routines, personal preferences, etc.)	private information (e.g. conversations, videos, habits, etc.) or sensitive information (e.g., health information, personal preferences, etc.) revealed
DoS	account lockouts, malware (e.g., ransomware), jamming, wireless signal interference, exploitation of protocol weaknesses	home device operations interrupted
Elevation of privilege	weak passwords, default account settings, buffer overflows, outdated software versions, weak access control or password reset mechanisms	IoT devices used to conduct espionage or to perform DDoS attacks (e.g., Mirai)

TABLE I
IOE THREAT SCENARIOS BASED ON SELECTED ATTACK SURFACE AREAS [20]

could be exploited to perform tailored marketing activities or social engineering attacks.

In order to improve interoperability, IoE devices often use weak or no encryption . Further, vulnerabilities in applications could cause information leakage.

C. Scenario 3: Jamming, Interference and DoS Attacks against IoE

More and more devices are going to affect our daily lives in the future. The vision of IoE is to connect a myriad of existing household devices and help innovations emerge.

A denial of critical IoE services could lead to severe damage depending on the type of devices. Jamming devices, which are only connected by wireless means (e.g. wireless connected surveillance and alarming devices), cause a denial of services of these smart homes services.

Missing protection against physical attacks, such as jamming of wireless signals, is a significant threat to future IoE systems. Further, the large increase of wireless devices transmitting various types of signals could lead to more interference among IoE devices.

VII. FUTURE RESEARCH

Threat modeling is just a beginning in the pursuit of our IoE security research agenda. As discussed in sections I and VIII, our ultimate goal is to facilitate home users to better protect themselves from attacks against their IoE devices. By completing the threat modeling phase of our research, we are now ready to tackle the next step of our research, that is, detecting IoE security threats so that we can eventually alert home users of the impending attacks.

A. Threat detection

IoE security threats manifest themselves in many forms. End users are usually oblivious about them when they are in the vicinity of IoE devices at home or at work on a daily basis. In fact, it is often the case that they don't even know what IoE sensors are around them, not to mention the threat they pose.

Therefore, knowing what IoE devices are present near a user is the first step in identifying an IoE security threat. We can accomplish this by scanning a network for various hosts.

A number of these IoE hosts use wireless connections and depend on a wireless access point (AP) as their gateway. This predominant dependence of IoE devices on the access point makes it a source of significant IoE security threats.

For example, if the access point gets compromised, an attacker can obtain the visibility of all the connected IoE devices as well as their traffic. Another important threat scenario is the possibility of an evil twin, that is, IoE devices connecting to a wrong access point disguising as the authentic access point. In this case, the fake access point can launch a phishing attack against unsuspecting IoE devices trying to get connected to the home or work network.

These threat scenarios make the access point a centerpiece in our attempt to defend trusted IoE devices against attackers and rogue IoE devices. Due to this important role of access points, we believe that it is necessary to develop a more IoE-conscious access point this is designed to withstand IoE-specific attacks and to provide better visibility towards IoE devices in our home or work network, which can potentially be vulnerable to attacks.

Since all the IoE devices using wireless technologies should be connected to it, an access point is a natural place where

we can conduct our intelligence gathering efforts for suspicious IoE devices. Since all new IoE devices should also be connected to it, the access point can provide information on changes in the IoE devices in a network (e.g., the total number of IoE devices today vs. yesterday).

VIII. Conclusion

Our ultimate goal is to build a system for home users to keep them aware of IoE security threats and to empower them to mitigate the risks associated with the threats by offering actionable advice.

As our first step towards this overarching research goal, this paper focused on establishing a threat model that is customized and optimized for home IoE devices. This involved enumerating home IoE assets, identifying entry points and vulnerabilities including human weaknesses, and creating threat scenarios according to the STRIDE model.

Developing an exhaustive set of home IoT threat scenarios is beyond the scope of our paper. Rather, our aim is to develop a straightforward methodology for producing IoE-specific threat scenarios so that we can eventually automatically generate them with minimal user inputs.

Although, having avoided documenting all the possible threat scenarios, we still provide high-impact threat scenarios which most home users are likely to encounter frequently.

Acknowledgment

The authors would like to thank IBM for funding this research through its IBM Faculty Award. The financial support by the Austrian Federal Ministry of Science, Research and Economy and the National Foundation for Research, Technology and Development is also gratefully acknowledged. This work was also supported by ITRC (IITP-2017-2015-0-00403).

We also thank Ryan Leirvik and Aaron Carreras at Grimm-co.com for sharing their insights and experiences with Howdy Neighbor: an IoT Capture The Flag (CTF) competition they organized [30].

References

[1] "DDoS attack that disrupted Internet was largest of its kind in history, experts say," (Date last accessed 26-May-2017). [Online]. Available: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

[2] "Target hackers broke in via HVAC company," (Date last accessed 3-May-2017). [Online]. Available: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company

[3] A. J. Jara, L. Ladid, and A. F. Gómez-Skarmeta, "The Internet of Everything through IPv6: An analysis of challenges, solutions and opportunities." *JoWua*, vol. 4, no. 3, pp. 97–118, 2013.

[4] "Here are the biggest IoT security threats facing the enterprice in 2017," date last accessed 25-May-2017. [Online]. Available: http://www.techrepublic.com/article/here-are-the-biggest-iot-security-threats-facing-the-enterprise-in-2017/

[5] "The 10 most terrifying IoT security breaches you aren't aware of (so far)," date last accessed 25-May-2017. [Online]. Available: https://www.linkedin.com/pulse/10-most-terrifying-iot-security-breaches-so-far-you-arent-montgomery

[6] "IoT security damage expected to grow 32% for next four years," date last accessed 25-May-2017. [Online]. Available: http://www.businesskorea.co.kr/english/news/ict/16618-iot-security-first-iot-security-damage-expected-grow-32-next-four-years

[7] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *2013 Ninth International Conference on Computational Intelligence and Security*, Dec 2013, pp. 663–667.

[8] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–1, 2017.

[9] D. Chen, G. Chang, L. Jin, X. Ren, J. Li, and F. Li, "A novel secure architecture for the Internet of Things," in *International Conference on Genetic and Evolutionary Computing*, Aug 2011, pp. 311–314.

[10] A. Atamli and A. Martin, "Threat-based security analysis for the Internet of Things," in *Proceedings of the 2014 International Workshop on Secure Internet of Things*. IEEE, Sep. 2014, pp. 35–43.

[11] P. Wang, "Bluetooth low energy-privacy enhancement for advertisement," Master's thesis, Institutt for telematikk, 2014.

[12] J. Bangali and A. Shaligram, "Design and implementation of security systems for smart home based on GSM technology," *International Journal of Smart Home*, vol. 7, no. 6, pp. 201–208, 2013.

[13] "Threat modeling," date last accessed 6-May-2017. [Online]. Available: https://msdn.microsoft.com/en-us/library/ff648644.aspx

[14] "The STRIDE threat model," date last accessed 6-May-2017. [Online]. Available: https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[15] "Your hackable house," date last accessed 14-May-2017. [Online]. Available: http://money.cnn.com/interactive/technology/hackable-house/

[16] "Smart smoke detector buying guide," date last accessed 18-May-2017. [Online]. Available: https://www.cnet.com/news/smart-smoke-detector-buying-guide/

[17] "Ransomware on Smart TVs is here and removing it can be a pain." date last accessed 18-May-2017. [Online]. Available: http://www.pcworld.com/article/3154226/security/ransomware-on-smart-tvs-is-here-and-removing-it-can-be-a-pain.html

[18] "Worried the CIA hacked your Samsung TV? here's how to tell," date last accessed 18-May-2017. [Online]. Available: https://www.wired.com/2017/03/worried-cia-hacked-samsung-tv-heres-tell/

[19] "Guide to Bluetooth security," date last accessed 19-May-2017. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-121/sp800_121_r2_draft.pdf

[20] OWASP, "IoT attack surface areas," https://www.owasp.org/index.php/IoT_Attack_Surface_Areas, 2017, accessed June 2017.

[21] I. Thomson, "If you use smart Bluetooth locks, you're asking to be burgled," https://www.theregister.co.uk/2016/08/08/using_a_smart_bluetooth_lock_to_protect_your_valuables_youre_an_idiot/, 2016.

[22] A. Liptak, "Amazons Alexa started ordering people dollhouses after hearing its name on tv," https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse, 2017.

[23] CSO Online, "SQLi, XSS zero-days expose Belkin IoT devices, Android smart phones," http://www.csoonline.com/article/3138935/security/sqli-xss-zero-days-expose-belkin-iot-devices-android-smartphones.html.

[24] P. Oltermann, "German parents told to destroy doll that can spy on children," https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children, 2017.

[25] M. Smith, "Peeping into 73,000 unsecured security cameras thanks to default passwords," http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html, 2014.

[26] R. Chirgwin, "Wi-Fi sex toy with built-in camera fails penetration test," https://www.theregister.co.uk/2017/04/04/intimate_adult_toy_fails_penetration_test/, 2017.

[27] IoT Security Foundation, "The IoT ransomware threat is more serious than you think," https://iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/.

[28] Symantec, "The dawn of ransomwear: How ransomware could move to wearable devices," https://www.symantec.com/connect/blogs/dawn-ransomwear-how-ransomware-could-move-wearable-devices, 2015.

[29] J. Leyden, "Mysterious Hajime botnet has pwned 300,000 IoT devices," https://www.theregister.co.uk/2017/04/27/hajime_iot_botnet/, April 2017.

[30] "Stuxnet-like attack could compromise your house," date last accessed 27-May-2017. [Online]. Available: https://www.newswire.com/news/stuxnet-like-attack-could-compromise-your-house-19266338