Identifying Vulnerabilities in Security and Privacy of Smart Home Devices

Chola Chhetri[1] and Vivian Motti[1]

George Mason University, Fairfax VA 22030, USA,
{cchhetri,vmotti}@gmu.edu

Abstract. Smart Home Devices (SHDs) offer convenience that comes at the cost of security and privacy. SHDs can be subject to attacks and they can be used to conduct attacks on businesses or governments providing services to individuals. In this paper, we report vulnerabilities that have been published in research papers in IEEE Xplore digital library and ACM digital library. We followed a systematic approach to search for vulnerabilities in the literature, analyzed them and placed them in common categories. The study resulted in 153 vulnerabilities. The categories are based on the place of occurrence or component of smart home architecture, such as device, protocol, gateway, network, and software architecture. We also identified areas of research and development that have been underexplored in the past and need further efforts. Researchers, developers and users will benefit from this comprehensive analysis and systematic categorization of smart home vulnerabilities.

Keywords: vulnerabilities, smart home devices, internet of things, security, privacy

1 Introduction

With over 20 billion Internet of Things (IoT) devices projected to be used globally by 2020, home automation is changing the way people interact and live, through the use of intelligent voice assistants, smart door locks, light bulbs, etc. [32]. Smart Home Devices (SHDs) pose threats to the security and privacy of individuals, businesses, and the society [72, 13, 5]. Unauthorized actors have hacked baby monitors [72], IoT search engines have provided public access to baby videos [29], toys have leaked parent-child conversations [38], drones have controlled home lights by flying above houses [13], and malware attacks on vulnerable IoT devices have brought down prominent Domain Name System (DNS) infrastructure affecting many large businesses, such as Dyn [5]. Information about smart home vulnerabilities (SHV) is scattered across a large number of research articles in databases. This paper systematically catalogs SHVs from research articles published in IEEE digital library and ACM digital library from 2010 to 2019.

Security vulnerabilities are closely linked with privacy, as they can lead to privacy violations. For instance, a security vulnerability may allow an adversary to hack into a baby monitor, and get audio, as well as video recordings of a child, thus violating the child's privacy. Hence, addressing SHD vulnerabilities helps resolve not only security concerns but also privacy concerns. Furthermore, unaddressed concerns leads to non-adoption and rejection of technology, such as the past case in Netherlands, where a rollout of smart meters had led to failure [30].

To the best of our knowledge, this paper is the first to systematize SHV information through literature review. Anwar et al. (2017) proposed a taxonomy for smart home that broadly classified smart home security threats into three types: (a) intentional/abuse, (b) malfunctions/failures, and (c) unintentional. Intentional threats include threats from an adversary, e.g. denial of service, identity fraud, manipulation of information, eavesdropping/traffic hijacking. Malfunctions include interruptions or disruptions caused by failures in devices, communication, network, power, third party services, and Internet. Unintentional threats are accidental abuses, such as accidental sharing of sensitive data, policy flaws, design flaws, among others [6].

Anwar's taxonomy serves as a preliminary frame for reference. However, its scope was limited to a small set of the literature (15 references) and the threats classified were non-device-specific [6]. Mosenia and Jha (2016) studied 20 IoT security threats and divided them into three layers: Edge nodes (Computing nodes and radio frequency identification), Communication, and Edge computing [55].

Our comprehensive study of SHD vulnerabilities synthesizes 153 SHVs, categorizes them, the scope of attacks in the smart home, and identifies research areas that need further exploration. Our study is a part of research aimed at exploring SHVs and designing user-centric privacy controls for SHDs [15]. In this paper, we report on the following:

1. We perform a systematic literature review of **1**19 articles and catalog SHV information published in selected databases (Section 3).
2. We categorize the SHVs into four categories, each category containing subcategories. This could serve as vulnerabilities taxonomy for the smart home domain (Section 3).
3. We synthesize the solutions to SHVs from our literature review (Section 4). Some solutions are specific to a vulnerability and/or a device, while others are general and do not address a specific vulnerability.
4. We identify research gaps and opportunities in the security and privacy of smart home. (Section 5)

2 Methodology

In this section, we describe the scope, inclusion criteria and exclusion criteria of our systematic literature review.

2.1 Databases and Keywords

We performed full-text literature search on IEEE Xplore Digital Library [1] and ACM Digital Library[2] from October 2018 to March 2019. We used the following keywords in the search:

- smart AND home AND vulnerabilities
  - In Abstract
  - In Document Title

2.2 Inclusion and Exclusion Criteria

We read all papers in the search results to determine if they were relevant to the study. For a paper to be considered as 'relevant', it had to discuss or contain information about smart home vulnerabilities (SHV). We read the abstract first and then the paper to determine SHV content. If a paper did not contain SHV information, we considered it 'irrelevant' to the study.

For each paper in the search results, the following steps were followed in order:

1. Read abstract.
2. If the abstract contains SHV information, include it.
3. If the abstract does not contain SHV information, read the paper.
4. If paper contains SHV information, include it.
5. If paper does not contain SHV information, exclude it.

Outcomes: The search in the two databases returned a total of 119 papers, among which 98 papers were included and 21 were excluded (see Table 1). Publication dates ranged from 2010 to 2019. ACM papers were published in 33 proceedings and one periodical. IEEE papers were published in 73 conferences, and 11 journals and magazines.

Source	**# Papers**	**# Included**	**# Excluded**
IEEE	85	73	12
ACM	34	25	9
Total	119	98	21

Table 1. Number of papers included in and excluded from the study.

For papers included in the study, a systematic cataloging of SHV information was done, following a template we developed for this purpose. In the catalog, we included the name of the vulnerability, name/type of device, explanation of the vulnerability, solution, explanation of the solution, who implements the solution (user or developer), and drawbacks of the solution, when available in the paper.

[1] ieeexplore.ieee.org

[2] dl.acm.org

3 Vulnerabilities of the Smart Home

In this section, we discuss the vulnerabilities found in the study. The cataloging process resulted in 153 SHVs. SHVs existed in various parts of the SH network, including the device, SHD applications (such as voice assistants), software architectures and frameworks, communication protocols (such as WiFi, 802.15.4, Zigbee, Routing for Low Power and Lossy Network (RPL), Precision timing protocol (PTP), etc.), smart home network, operating system (such as Android), and authentication systems (such as Zigbee Light Link).

Among the SHVs, 75 were device specific. The papers identified the devices with the vulnerability discussed. Devices with vulnerabilities included cameras (such as TP Link), Belkin motion sensor, Withings scale, light bulbs (Philips Hue, LIFX), Chromecast, Google home, Hello Barbie talking doll, Haier Smartcare, HP Envy printer, hubs/controllers, TP Link power switch, thermostat (Nest), smart meters, smart speakers, SmartThings, and Voice Control System. The 78 remaining vulnerabilities were generic (non-device-specific) and related to communication protocols, software architectures, communication, voice assistants (such as Alexa), operating systems, applications, and authentication mechanisms.

3.1 Device Vulnerabilities

The papers included in our study revealed vulnerabilities in SHD hardware or in the software running in the device. We divided the device vulnerabilities in eight categories:

1. Authentication Vulnerabilities
2. Information Leakage or Disclosure
3. Data Protection Vulnerabilities
4. Data Manipulation
5. Voice Interface Vulnerabilities
6. User Behavior Detection
7. Service Disruption
8. Other Vulnerabilities

Authentication Vulnerabilities Authentication in an SHD ensures that only legitimate user or software process have access to the device features, control and operation [20]. Authentication vulnerabilities include lack of authentication, default credentials, hard-coded credentials, leaked credentials, weak authentication, flawed authentication protocol, and de-authentication attack. We will describe each of these briefly in the following sub-sections:

Lack of Authentication Ma et al. (2018) showed that an attacker can post a message (text, audio, video) on the user's TV/Chromecast screen without requiring any authentication [48]. Mahadewa et al. (2018) demonstrated that any SHD in a home network can control the light bulbs available. Chromecast allowed private YouTube videos to be cast on television without requiring any authentication [49].

Default Credentials While the SHD industry as a whole has not caught up in implementing authentication credentials in devices [48, 49], some manufacturers allow the set up of credentials, such as passwords and pins, in their devices. However, many devices run with their default credentials [54, 31] and users are not aware about how to change them. Adversaries can easily find default credentials on the Internet. There are also search engines available that allow public access to SHDs (such as cameras) online [12]. Papers included in our study reported the use of default credentials in cameras [60, 4], routers [51], thermostats [54], plugs [43], printers [63], light bulbs and motion sensors [63]. An adversary does not need to be technically savvy to learn default credentials. S/he needs to be able to search the Internet and have access to an Internet-connected device.

Hard-coded Credentials When credentials are hard-coded into the device and changes are not allowed, the device becomes vulnerable to attacks irrespective of other security and privacy mechanisms implemented in the device [12, 43]. SHDs with image, audio and video recording capability can easily compromise the privacy and security of individuals, if they are operate with hard-coded credentials that can not be changed by the user.

Leaked Credentials Saleh et al. (2018) demonstrated that credentials (username and password) of motion sensor and a Closed-circuit television (CCTV) camera were leaked to any observer of smart home traffic. Authentication credentials were not protected from being visible to a passive observer [60].

Weak Authentication Prior research presents evidence of poorly implemented authentication, that allows an adversary to gain access to cameras [60, 41, 63]. Saleh et al. (2018) conducted penetration testing on a camera used to monitor a home smart meter using the Kali[3] operating system, which allowed the investigators access to the camera using default username-password combination [60]. This means an adversary could have full access to the smart camera without the user's knowledge. Authors claim that surveillance cameras of this type are used to monitor smart grid for security. Vulnerable CCTV cameras, thus lead to vulnerable smart grids [60].

According to Lei et al. (2018), Alexa used a voice word (analogous to a password) for user authentication. However, the person speaking the voice word did not have to be an authenticated user; it could be any one who knew the voice word [41]. Similarly, Sivanathan et al. (2017) showed that an attacker was able to send commands to control a light bulb, a power switch and a printer due to poor authentication [63]. In another experiment, Alharbi and Aspinall (2018) found that the Web interface of a camera used a weak password policy, did not require complex passwords and was prone to a brute-force password attack [4].

Flawed Authentication Protocol In some SHDs, such as Philips hub, authentication is implemented; however, the authentication protocol used has security

[3] kali.org

flaws. Mahadewa et al. (2018) found that the Philips Hue hub generates authentication tokens for all devices, whether they are authenticated or not. This results in unauthenticated and malicious devices being able to connect to Philips hub and control the smart home network or eavesdrop [49].

De-authentication attack Sun et al. (2018) showed that sending 802.11 de-authentication frame to disconnect a light bulb from the access point disabled home Internet connection or forced light bulb to connect to rogue access point. The light bulb was designed to remember the state (on/off) in case it was disconnected, and it lacked a physical power switch (on/off). Consequently, if the attacker turned off the light bulb and then performed de-authentication attack, the user could not turn it back on. In the same experiment, a camera was also found vulnerable to such de-authentication attack, which could render the camera unusable to the user [65].

Information Leakage or Disclosure Papers included in our analysis show the potential of leakage of information collected by SHDs [4, 36, 65, 67]. We have divided the information leakage or disclosure-related vulnerabilities into the following 5 sub-categories:

Log File Information Leakage Alharbi and Aspinal (2018) found that the Android app of a camera stored the personal information of end users (such as home address, encryption keys, and WiFi credentials) in a log file, easily accessible to an adversary [4]. They also showed that in some SHD apps, system crashes could lead to leakage of sensitive data, such as device Unique Identifier (UID), email address, phone number, Global Positioning System (GPS) location, text messages, and log messages [4]. Johnson et al. (2018) claimed that SHD vendors could write this information from Android log file to another file and malicious apps could deliberately cause crashes to obtain this information. This information could be used for user tracking, user behavior prediction, and location determination [36].

Device Information Leakage SHDs have unique identifiers, such as Media Access Control (MAC) addresses and serial numbers. When revealed, such identifiers can be used to permanently track the device and/or its owner. Alharbi and Aspinall (2018) found that cameras were revealing MAC addresses, device serial numbers, and device passwords, making it convenient for an adversary to access the camera without any sophisticated attack [4].

Personal Information leakage Tekeogl and Tosun (2015) showed that an adversary could passively listen to a Chromecast device and obtain unencrypted information, which included google account username, video id, time, operating system (OS) name, OS version, device brand and model. In addition, they conducted black box tests to reveal the leakage of remote information (name, brand, model, OS name, and OS version) to an observer [68].

Information Disclosure Sivanathan et al. (2017) showed that unencrypted messages (including audio and video) were disclosed by smart home devices, such as Belkin Motion Sensors, TP Link cameras, Withings scales, and Phillips Hue light bulbs [63]. They also found that an Internet Protocol (IP) printer exposed the last scanned document to an attacker who controlled the printer via its web interface [63]. Bugeja et al. (2018) found similar information disclosure vulnerabilities in ‘connected’ cameras [12] .

Device and Occupant Localization Vulnerable smart cameras connected to the home network can reveal sensitive information not just about location but also about occupants in the home. Sun et al. (2018) showed that an adversary could perform traffic analysis by passively sniffing home network traffic to obtain knowledge about the number of occupants and the in-house location of occupants. The attacker would also not risk being detected due to the attack’s passive nature [65]. Jia et al. (2017) showed that an adversary could effectively perform geo-location prediction in Google Home [34].

Data Protection Vulnerabilities It is important that data in a smart home be protected. The data life cycle in a smart home includes collection from SHDs, transmission to hub and/or cloud, storage in hub and/or cloud, and processing [16]. In our categorization, data protection vulnerabilities include Lack of Encryption, Weak Encryption, and Weak Server-side Protection.

Lack of Encryption True end-to-end encryption, when implemented well, can provide confidentiality of data in transit and also at rest in a storage device or cloud. Most smart phones today have feature of encryption; however, this feature may not be enabled by default [17]. Zhang et al.(2016) mentioned that most phones lacked encryption, which allowed an adversary to obtain SHD data easily in case the adversary established physical or remote access to the phone controlling SHDs [73]. Alharbi and Aspinall (2018) found that a Ring doorbell smart camera lacked encryption of video stream from the camera to server [4].

Weak Encryption Encryption is a commonly discussed solution for sensitive data protection [8]. However, weakly implemented encryption can provide an additional attack vector in case an adversary were to break the encryption. For instance, Sivanathan et al. (2017) showed that a TP Link power switch could be easily broken into due to weak encryption [63]. Encryption vulnerabilities found in the literature review also included plain text key exchange in camera apps [4] and clear text communication from device to cloud in a Chromecast device [68].

Weak Server-side Protection Attackers could easily steal personal information and listen to conversations in a Hello Barbie talking doll due to the lack of data protection in the server [63]. Server-side data protection is an important issue. Users of SHDs tend to trust their vendors in protecting their data [16]. In the event that data related to users is breached, companies not only lose trust of their customers but also bear huge financial losses [1].

Data Manipulation This category of SHD vulnerabiities includes vulnerabilities that allow an adversary to change configurations, alter data or modify applications in a home network. Pricing cyberattack falls under this category.

Pricing Cyberattack Past research has demonstrated that an adversary could change the data regarding electricity usage by gaining access to a smart meter [34, 47]. This could result in altered utility bill (e.g. higher electricity bills) for a smart meter user and an attacker could reduce his/her bill but increase community peak energy usage as well as other users' energy bill [34]. Various detection frameworks have been proposed to solve this problem. Researchers have evaluated vulnerabilities in some presented frameworks, such as the lack of net metering in detection frameworks [47].

Voice Interface Vulnerabilities The domain of smart speakers and voice enabled devices has presented new vulnerabilities in the SHD domain. This category includes vulnerabilities in devices with Voice User Interface (VUI).

Voice Command Attack According to Alanwar et al. (2017), audible voice commands (generated by devices such as televisions) and inaudible voice commands (generated by malicious speakers) were able to activate smart speakers and force them to perform actions even when the legitimate user was not present [3]. An adversary with access to speaker-enabled devices in a smart home network could issue malicious commands, leading to fake transactions, burglary, or other unintended actions. For example, in 2015, Amazon Echo devices in users' homes played Christmas music in response to a television advertisement for Alexa, which confused and frustrated many users [11].

Hidden Command Attack Voice commands can be hidden in a way that they appear as noise to human ears. Meng et al. (2018) found that an attacker was able to conduct a spoofing attack on a Voice Command System (VCS) and issue a hidden voice command to an SHD [52]. Hence, what appears as noise could be a command given by an adversary to open a garage door, or to unlock the house, or turn up the thermostat [52].

Inaudible Command Attack Meng et al. (2018) also found that voice commands can be made inaudible to the human ears, and a spoofing attack in which an attacker inputs inaudible voice commands to a VCS is known as inaudible command attack [52].

Replay Audio(RA) Attack Replay audio attack is a spoofing attack in which the attacker uses pre-recorded voice of a user to fool the voice control system of a SHD [52]. Malik et al. (2019) found that smart speakers such as Amazon Echo and Google Home were subject to replay attacks, in which an adversary could place fake orders, reveal personal information (such as the owner's name), and control IoT devices, such as smart doors [50].

User Behavior Detection Apthorpe et al. (2017) showed that an observing entity, such as a service provider or an adversary, can analyze traffic generated from SHDs to predict the user presence (i.e. whether a user is home), sleep patterns, appliance usage patterns, occupancy patterns (i.e. how frequently a user is home), and the frequency of user motion [9]. In this paper, we refer to this inference as user behavior detection.

Pattern-of-Life Modeling Beyer et al. (2018) set up a test bed network including a camera, outlet, motion sensor, and television, and used pattern-of-life analysis tool to analyze data leakage. They found that an adversary could infer the types of SHDs used in the home, identify events (such as user presence), track the user, map the smart home network, and gain access to the home [10].

User Presence Detection Gong and Li (2011) showed that smart meters with differential transmission scheme (DTS) were vulnerable to user presence detection and that an adversary eavesdropping the traffic could infer whether the user is home [27]. DTS is a method for tracking electricity usage of a consumer by reporting power consumption to the utility company only when consumption changes. Since transmission frequency is proportional to power consumption, the attacker can reveal user presence by observing this transmission [27]. Li et al. (2012) discussed a similar attack on smart meters and called it Presence Privacy Attack (PPA) [42].

Service Disruption Any vulnerability on SHD that can cause partial or complete interruption of access to SHD or its service is categorized as Service Disruption. Hence, this category includes jamming, denial of service, impersonation and replay.

Jamming An adversary can disrupt network communication by introducing powerful jamming signals leading to interruption of service and battery drains [39]. Jamming attacks were previously demonstrated using smart meters [56].

Denial of Service Denial of Service (DoS) attack on 802.15.4 Media Access Control (MAC) in Zigbee devices was shown to cause disruption of service [70].

Impersonation Smart meters were shown to be vulnerable to impersonation, where an adversary could introduce rogue (or fake) device to appear legitimate [56].

Replay In LIFX lightbulb system, an attacker was able to intercept and replay User Datagram Protocol (UDP) packets to eavesdrop the network and control a light bulb [49]. Feng et al. (2017) showed that an attacker could replay pre-recorded video frames without motion to replace those with motion, to compromise the alert/alarm system of security cameras and hide the malicious behavior [22].

Other Vulnerabilities Twenty-six other vulnerabilities were found in various SHDs. In Table 2, we show the names of these additional vulnerabilities, the devices they were found in, and the references to related articles.

Vulnerability	**Device**	**Reference**
Access to Remote Data	Nest Thermostat	[54]
Account Lockout Mechanism	Camera	[4]
Authorization Code Compromise	Google Home	[35]
Brute-force attack	Plug (Edimax SP-2101W)	[43]
Cross-protocol vulnerability	Cross-protocol devices	[63]
Cross-site request forgery	Camera	[12]
Cross-site scripting	Camera	[12]
Design flaw	Haier SmartCare	[71]
Device scanning attack	Plug (Edimax SP-2101W)	[43]
Firmware attack	Plug (Edimax SP-2101W)	[43]
Flawed/lacking TLS implementation	Camera	[4]
Home Area Network Id (HANID) conflict attack	Smart meter	[24]
Intrusion	Smart grid	[53]
Key management (SILDA protocol)	Smart grid	[62]
Lack of Control to Administration Commands	Hub	[49]
Light bulb attack	lightbulb	[69]
Mis-response to Discovery Request	hub, Chromecast	[49]
Overprivilege	SmartThings	[28]
Over-privileged app	Camera	[4]
Rogue controller injection	Z-wave controller/gateway	[25]
SEP vulnerabilities	Smart grid	[7]
SH network compromise	Google Home	[35]
Spoofing attack	Plug (Edimax SP-2101W)	[43]
Unnecessary open ports	Camera	[4]
Unprotected WiFi Hotspot in SHD	Lightbulb	[49]
Use of Insecure Underlying Protocols	Hub	[49]

Table 2. Vulnerabilities in SHDs.

3.2 Application Vulnerabilities

SHDs are usually controlled by users through associated applications running on smartphones. We found two application vulnerabilities in our literature review: home network infiltration and data leakage.

Home Network Infiltration Malicious apps can make their way through app stores and then to the home network to cause larger attacks such as distributed denial of service (DDoS) [64].

Data Leakage Ahmad et al. (2015) showed that mobile OSs, such as Android, had limitations that allowed data leakage from end-user devices to vendor servers as well as unintended recipients [2].

3.3 Communication Vulnerabilities

In this section, we discuss Data Leakage and Protocol Vulnerabilities.

Traffic Analysis Sanchez et al. (2014) showed that even with proper encryption, an attacker could analyze WiFi traffic to infer sensitive information, such as inventory of SH devices, device functions and relationships, and user behavior [61].

Protocol Vulnerabilities Past research has revealed weaknesses in the RPL protocol [26] and proposed improvements [18, 26]. Fan et al. (2019) discussed time synchronization issues in PTP protocol (also called IEEE 1588 Precision clock synchronization protocol), which could cause inaccurate device functions due to device receiving wrong time information [21].

Past research also shows the possibility of following attacks on SHD communication:

- Jamming: An adversary can disrupt the network communication by introducing strong jamming signals leading to denial of service attack as well as SHD battery drains [39].
- Guaranteed Time Slot (GTS) attack: An attacker can disrupt the communication between SHD and its gateway, causing collision, corruption and retransmission of packets. This leads to a loss of communication and DoS attack [39].
- Acknowledgement (ACK) attack: An attacker eavesdrops communication, hijacks packet and sends fake ACK to trick the sender. This leads to the attacker taking control over the smart home network communication [39].
- XMPPloit: XMPPloit can force a SHD to not encrypt the communication, allowing eavesdropping and data leakage [39].
- Eavesdropping: Unencrypted communication allows an attacker to decipher sniffed communication causing a breach of confidentiality [33].
- Denial of Service: Attacker can use malicious traffic to render the home network unresponsive and the user cannot access the home network services [33].

3.4 Software Architecture Vulnerabilities

Liu et al. (2017) found the following vulnerabilities in the Joylink home automation architecture [44]:

WiFi credential theft WiFi credentials were transmitted after being encoded one character at a time following the IP address. This allowed an adversary to easily steal WiFi credentials and access home WiFi without authentication [44].

Vulnerable crypto key management The Joylink architecture utilized a vulnerable key generation technique and a local adversary could launch a man in the middle (MiTM) attack [44].

Traffic decryption The Joylink architecture utilized a vulnerable crypto key management technique and a local adversary could launch MiTM attack and decrypt all traffic, thus allowing breach of confidentiality of sensitive information [44].

Device hijacking The Joylink architecture utilized a weak communication security and a local adversary can obtain the MAC address of a user device, log into its own cloud account, hijack the device and control it remotely [44].

Out of band device control An attacker was able control the SHD by creating a fake server, without accessing the cloud account or the app [44].

Device impersonation The Joylink architecture's lack of authentication allowed an attacker to log in to a cloud account, activate a user device with a spoofed MAC address that was easy to obtain due to poor crypto management [44].

Firmware modification The Joylink architecture's lack of verification of downloaded firmware made it vulnerable to malicious firmware from attackers [44].

Visible data/communication Control commands and uploaded data were visible to an observer, that could lead to private information being revealed [44].

WiFi credentials on the Cloud WiFi credentials were uploaded to the cloud server, even when there was no need for this private user information to be sent to the cloud [44].

Weak key The Joylink architecture used a timestamp value as an Advanced Encryption Standard (AES) key, made it easy for an adversary to predict the key (due to a small key space) and to reveal information collected by the SHD app [44].

Reverse engineering and source code analysis of SmartApps performed by Fernandes et al. (2016) showed that more than half of the 499 apps were **over-privileged**, and apps retained unnecessary permissions even when the user denied them [23]. OpenHAB[4] and IoTOne were presented as solutions to this issue [28].

Web attacks, such as **SQL injection** and **unauthorized access to sensitive data**, were possible due to poor use (or exploitation) of Application Programming Interfaces (API) in the Spring framework, an open source framework for apps.

4 Solutions to SHD Vulnerabilities

In this section, we discuss the solutions to SHD vulnerabilities proposed by investigators of past research.

Main solutions to **authentication vulnerabilities** in SHDs included the use of the following authentication mechanisms [43, 60, 60, 41, 63, 49]:

1. Requiring the use of credentials, such as username-password combination,
2. Enforcing the change of credentials,
3. Protecting the authentication credentials, and
4. Ensuring that the authentication protocols used are up-to-date, strong and unbroken.

Two-factor authentication has been investigated as a potential approach to strong authentication in SHDs. Crossmand and Liu (2015) proposed the Smart Two-Factor Authentication, in which a company gives its user a smart card that

[4] https://www.openhab.org/

produces (and stores) a token for two-factor authentication at the request of the user [19]. Researchers have recommended that SHDs must have a physical switch for the user to manually turn the device on/off, and a default fail-over state so that an adversary can not render the device unusable [65].

Solutions to **information leakage and exposure** included limiting or restricting the use of personal information for logging and debugging purposes [4], protecting sensitive device information [4], and encrypting sensitive information [25, 73, 4].

Data collected by SHDs needs to be protected in all stages: collection, transmission (device to hub, hub to cloud), storage (in hub or cloud), and processing. Encryption is often used to protect data, but it needs to be implemented without flaws and encryption keys need to be protected too [73, 4, 33, 54, 25, 59]. Salami et al. (2016) proposed the Lightweight Encryption for Smart homes (LES), an encryption technique with low overhead and computation requirement, and identity-based stateful key management [59]. Further research is needed though to evaluate the use of such encryption techniques in various categories of SHDs.

Maintaining data integrity in smart meters is crucial for the accuracy of electricity bill and protection of smart meters and the smart grid from data manipulation attacks. Various pricing cyber attack detection frameworks have been proposed, such as the Electricity Pricing Manipulation Detection Algorithm [46], Partially observable Markov decision process (POMDP) based smart home pricing cyberattack detection framework [47], and single event detection technique based on support vector regression [45].

As a solution to audio vector attacks, Alanwar et al. (2017) proposed EchoSafe, a sound navigation ranging (SONAR) based active defense mechanism, that checks for the presence of the user as soon as the smart speaker is activated, to ensure that commands are executed only if the user is present nearby (in the room) [3]. To protect from hidden and inaudible command voice attacks, Meng et al. (2018) proposed Wivo, a tool that authenticates the voice input with mouth motions of the user (liveness detection) [52]. Replay attack detection approaches include Higher-order spectral analysis(HOSA)-based replay attack detection approach [50] and Wivo [52].

User presence attack and behavior inference attack are usually mitigated by introducing fake traffic into a user's smart home network to minimize the likelihood of an inference to occur. Beyer et al. (2018) proposed a technique called MIoTL (Mitigation of IoT Leakage), which introduces fake traffic to the home network using (a) a device shadow to protect from identifying and classifying devices, and (b) a MAC shadow to mitigate user tracking [10]. Gong and Li (2011) proposed a similar approach for addition of null packets to the smart meter traffic during idle times to emulate busy times, confuse the observer, and mitigate user presence detection [27]. Li et al. (2012) proposed a similar method called Artificial Spoofing Packet(ASP), which added dummy packets to the transmission to trick an eavesdropper and mitigated user presence detection [42].

To mitigate denial of service attack in the Zigbee protocol, Whitehurst et al. (2014) proposed integrity checks on received packets (including acknowledgments) to make it difficult for an adversary to forge packets [70]. Namboodiri et al. (2014) proposed SecureHAN to combat jamming, impersonation, replay, and repudiation attacks [56]. Feng et al. (2017) showed that video replay attack in cameras could be thwarted by hardware isolation of the motion detection module [22].

To prevent home network infiltration via SHD apps, developers could employ network traffic analysis [64]. Data leakage through apps could be prevented by restricting app downloads only from home automation app stores, and by establishing fine grained policies to improve the communication between home automation apps and non-home-automation apps [36].

Finally, 5 articles in our data set have presented intrusion detection systems (IDS) as a method of protecting the home network [24, 57, 58, 14, 66]. The proposed IDS solutions are proofs of concept and prototypes. SHD users will benefit from fully functional tools available for consumer use.

5 Discussion

The systematic literature review showed 153 vulnerabilities in 75 devices. We found little consensus in the naming of the vulnerabilities. So, we categorized them based on vulnerabilities characteristics and similarities of the attacks. Based on the architectural components these vulnerabilities were found in, the smart home network presents many attack surfaces, making it harder to fully protect the home network from adversaries. The attack surface of a home network includes:

- smart home device, including hardware, operating system, and applications,
- communication protocols, that run on the SHD, controller or hub, and home router or gateway,
- smart phones used to control SHDs, including phone hardware, operating system, and applications,
- home automation software or software framework, and
- software securing the home network.

The attack surface increases as the number of devices and features in the smart home grows. New methods of attack are also introduced, such as home burglary and fake orders through attacks on VUI [40]. Thus, providing security and privacy in the smart home is challenging.

It is clear that the authentication vulnerabilities category was the largest, with 8 sub-categories. The lack of authentication poses threats to a smart home. An attacker may be able to control someone's door lock, garage door opener, thermostat or coffee maker and issue malicious commands. Evidently, there is a need for SHD manufacturers to implement authentication properly to address this issue and allow only authorized users to control an SHD.

In section 3.1, we presented that research literature showed default credentials vulnerability was found in 7 SHDs. It is argued that market competition and the pressure to create low-cost SHDs in a short time frame has led to the issues lacking or poorly implemented authentication, which provide an additional (and easy) vector for adversaries to enter into the private home network. Baby monitor hacks [72] and Mirai botnet [37] that appeared widely in news were primarily possible due to default credentials. In order to prevent large scale attacks like Mirai in the future, default credentials vulnerability must be addressed in all SHDs. The issue of lack of authentication can be addressed by manufacturers requiring authentication credentials in their SHDs, and by developers requiring the user to change default credentials during device setup [51, 4].

Past user studies have shown that users care about data protection and their privacy, but trust the vendors to provide appropriate data security and privacy protection [16, 72, 38]. Manufacturers need to reduce vulnerabilities in their SHDs by following secure development practices and also use up-to-date, secure protocols for communication with other devices to reduce cross-protocol vulnerabilities.

It is challenging for SHDs with limited memory and computational power to locally encrypt data before sending to a cloud server. The data in transit, thus, risks potential breach of confidentiality. So, encryption techniques suited for such environments need to be evaluated.

Next, we will summarize open research areas in the area of smart home security and privacy, and discuss the limitations of our work.

5.1 Open Research Areas

We have identified the following open research areas in the security and privacy of SHDs:

- Security analyses of SHDs, protocols, and software frameworks, especially of newer models, to find out vulnerabilities and develop solutions.
- Authentication mechanisms suitable for low power, low-resource, low-cost SHDs.
- User-centric methods of enforcing change of default credentials and setting up strong credentials.
- Secure methodologies for storing and managing credentials in the smart home network.
- Data protection techniques, such as encryption, customized to SHD environment.
- Study of whether data manipulation attacks, similar to those in smart meters, are possible in other SHDs, and development of solutions, if necessary.
- Development and evaluation of solutions to voice interface vulnerabilities, as VUI attacks are evolving with the popularity of voice interfaces.
- Best practices in data protection at various stages of data life cycle including use, rest and transit.

5.2 Limitations

Our study has several limitations. Our study excludes papers not published on ACM and IEEE databases. It does not include research papers about SHD vulnerabilities from other databases that did not appear in the selected databases. Another limitation is that we have included articles published only in English and not included articles published after March 2019.

Moreover, the literature search keywords were chosen to match the goal of our study as much as possible. However, the search keywords used might have left out articles that included SHV information but did not use the selected keywords.

Finally, many manufacturers and vendors do update their software with patches as soon as a vulnerability is published, and protocols with flaws are updated. Thus, a limitation of our paper is that some vulnerabilities may no longer exist. However, the vulnerabilities information, categorization and taxonomy will serve as a basis for future research in newer types, brands and models of SHDs and their components.

6 Conclusion

We performed a systematic literature review to study 153 SHD vulnerabilities from 98 papers, categorized the vulnerabilities based on their characteristics, and proposed a taxonomy for the attacks. We also discussed solutions to these vulnerabilities from research literature and presented potential opportunities in the area of SHD security and privacy research.

A smart home is a mix of heterogenous devices, controllers, protocols, and software from wide variety of vendors and manufacturers. In addition to the efforts of adding security and privacy tools to SHDs, more research is necessary to design SHDs with security and privacy in mind. A combination of built in security and privacy features with home network protection tools can make mitigation stronger.

Most of the solutions proposed are prototypes, not fully functional tools ready for consumer use. SHD users will benefit from deployable tools. Future work should focus on developing more working solutions that can be made available to the consumers for the protection of the smart home.

References

1. Cost of Data Breach Study (2018), www.ibm.com/security/data-breach
2. Ahmad, W., Sunshine, J., Kaestner, C., Wynne, A.: Enforcing fine-grained security and privacy policies in an ecosystem within an ecosystem. In: Proceedings of the 3rd International Workshop on Mobile Development Lifecycle. pp. 28–34. MobileDeLi 2015, ACM, New York, NY, USA (2015), http://doi.acm.org/10.1145/2846661.2846664

3. Alanwar, A., Balaji, B., Tian, Y., Yang, S., Srivastava, M.: Echosafe: Sonar-based verifiable interaction with intelligent digital agents. In: Proceedings of the 1st ACM Workshop on the Internet of Safe Things. pp. 38–43. SafeThings'17, ACM, New York, NY, USA (2017), http://doi.acm.org/10.1145/3137003.3137014
4. Alharbi, R., Aspinall, D.: An iot analysis framework: An investigation of iot smart cameras' vulnerabilities. In: Living in the Internet of Things: Cybersecurity of the IoT - 2018. pp. 1–10 (March 2018)
5. Antonakakis, M., April, T., Bailey, M., Bursztein, E., Cochran, J., Durumeric, Z., Alex Halderman, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., Zhou, Y.: Understanding the Mirai Botnet. In: Proceedings of the 26th USENIX Security Symposium. pp. 1093–1110. Vancouver, BC, Canada (2017), https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis
6. Anwar, M.N., Nazir, M., Mustafa, K.: Security threats taxonomy: Smart-home perspective. In: 2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall). pp. 1–4 (2017)
7. Aouini, I., Ben Azzouz, L., Jebali, M., Saidane, L.A.: Improvements to the smart energy profile security. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC). pp. 1356–1361 (June 2017)
8. Apthorpe, N., Reisman, D., Feamster, N.: A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. In: Data and Algorithmic Transparency Workshop (DAT). New York (2016), http://datworkshop.org/papers/dat16-final37.pdf
9. Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A., Feamster, N.: Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. arXiv Preprint (2017), http://arxiv.org/abs/1708.05044
10. Beyer, S.M., Mullins, B.E., Graham, S.R., Bindewald, J.M.: Pattern-of-life modeling in smart homes. IEEE Internet of Things Journal 5(6), 5317–5325 (Dec 2018)
11. Braga, M.: People Are Complaining That Amazon Echo Is Responding to Ads on TV (2015)
12. Bugeja, J., Jönsson, D., Jacobsson, A.: An investigation of vulnerabilities in smart connected cameras. In: 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). pp. 537–542 (March 2018)
13. Chang, V., Chundury, P., Chetty, M.: "Spiders in the Sky": User Perceptions of Drones, Privacy, and Security. Chi'17 (2017), https://hci.princeton.edu/wp-content/uploads/sites/459/2017/01/CHI2017{_}CameraReady.pdf
14. Chatfield, B., Haddad, R.J.: Rssi-based spoofing detection in smart grid ieee 802.11 home area networks. In: 2017 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT). pp. 1–5 (April 2017)
15. Chhetri, C.: Towards a smart home usable privacy framework. In: Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing. p. 43–46. CSCW '19, Association for Computing Machinery, New York, NY, USA (2019), https://doi.org/10.1145/3311957.3361849
16. Chhetri, C., Motti, V.G.: Eliciting Privacy Concerns for Smart Home Devices from a User Centered Perspective. In: Taylor, N.G., Christian-Lamb, C., Martin, M.H., Nardi, B. (eds.) Information in Contemporary Society. pp. 91–101. Springer International Publishing, Cham (2019), https://doi.org/10.1007/978-3-030-15742-5{_}8
17. Cipriani, J.: What you need to know about encryption on your phone (2016), https://www.cnet.com/news/iphone-android-encryption-fbi/

18. Conti, M., Kaliyar, P., Rabbani, M.M., Ranise, S.: Split: A secure and scalable rpl routing protocol for internet of things. In: 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). pp. 1–8 (2018)
19. Crossman, M.A., Hong Liu: Study of authentication with iot testbed. In: 2015 IEEE International Symposium on Technologies for Homeland Security (HST). pp. 1–7 (April 2015)
20. Das, A.K., Zeadally, S., Wazid, M.: Lightweight authentication protocols for wearable devices. Computers & Electrical Engineering 0, 1–13 (2017), http://linkinghub.elsevier.com/retrieve/pii/S0045790617305347
21. Fan, K., Wang, S., Ren, Y., Yang, K., Yan, Z., Li, H., Yang, Y.: Blockchain-based secure time protection scheme in iot. IEEE Internet of Things Journal pp. 1–1 (2019)
22. Feng, X., Ye, M., Swaminathan, V., Wei, S.: Towards the security of motion detection-based video surveillance on iot devices. In: Proceedings of the on Thematic Workshops of ACM Multimedia 2017. pp. 228–235. Thematic Workshops '17, ACM, New York, NY, USA (2017), http://doi.acm.org/10.1145/3126686.3126713
23. Fernandes, E., Jung, J., Prakash, A.: Security analysis of emerging smart home applications. In: 2016 IEEE Symposium on Security and Privacy (SP). pp. 636–654 (2016)
24. Fouda, M.M., Fadlullah, Z.M., Kato, N.: Assessing attack threat against zigbee-based home area network for smart grid communications. In: The 2010 International Conference on Computer Engineering Systems. pp. 245–250 (Nov 2010)
25. Fuller, J.D., Ramsey, B.W.: Rogue z-wave controllers: A persistent attack channel. In: 2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops). pp. 734–741 (Oct 2015)
26. Gawade, A.U., Shekokar, N.M.: Lightweight secure rpl: A need in iot. In: 2017 International Conference on Information Technology (ICIT). pp. 214–219 (Dec 2017)
27. Gong, S., Li, H.: Anybody home? keeping user presence privacy for advanced metering in future smart grid. In: 2011 IEEE GLOBECOM Workshops (GC Wkshps). pp. 1211–1215 (Dec 2011)
28. Gyory, N., Chuah, M.: Iotone: Integrated platform for heterogeneous iot devices. In: 2017 International Conference on Computing, Networking and Communications (ICNC). pp. 783–787 (Jan 2017)
29. Hill, K.: How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old. Forbes.com (2013)
30. Hoenkamp, R., Huitema, G.B., Vugt, A.J.C.D.M.V.: The Neglected Consumer : The Case of the Smart Meter Rollout in the Netherlands. Renewable Energy Law and Policy 4(November 2011), 269–282 (2014)
31. Hsieh, W., Leu, J.: A dynamic identity user authentication scheme in wireless sensor networks. In: 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC). pp. 1132–1137 (July 2013)
32. Hung, M.: Leading the IoT. Gartner, Inc. (2017), https://www.gartner.com/imagesrv/books/iot/iotEbook{_}digital.pdf
33. d. J. Martins, R., Schaurich, V.G., Knob, L.A.D., Wickboldt, J.A., Filho, A.S., Granville, L.Z., Pias, M.: Performance analysis of 6lowpan and coap for secure communications in smart homes. In: 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA). pp. 1027–1034 (March 2016)

34. Jia, X., Li, X., Gao, Y.: A novel semi-automatic vulnerability detection system for smart home. In: Proceedings of the International Conference on Big Data and Internet of Thing. pp. 195–199. BDIOT2017, ACM, New York, NY, USA (2017), http://doi.acm.org/10.1145/3175684.3175718
35. Jia, Y., Xiao, Y., Yu, J., Cheng, X., Liang, Z., Wan, Z.: A novel graph-based mechanism for identifying traffic vulnerabilities in smart home iot. In: IEEE INFOCOM 2018 - IEEE Conference on Computer Communications. pp. 1493–1501 (April 2018)
36. Johnson, R., Elsabagh, M., Stavrou, A., Offutt, J.: Dazed droids: A longitudinal study of android inter-app vulnerabilities. In: Proceedings of the 2018 on Asia Conference on Computer and Communications Security. pp. 777–791. ASIACCS '18, ACM, New York, NY, USA (2018), http://doi.acm.org/10.1145/3196494.3196549
37. Kolias, C., Kambourakis, G., Stavrou, A., Voas, J.: Ddos in the iot: Mirai and other botnets. Computer 50(7), 80–84 (2017)
38. Lau, J., Zimmerman, B., Schaub, F.: Alexa, Are You Listening? Privacy Perceptions , Concerns and Privacy-seeking Behaviors with Smart Speakers. In: Proceedings of ACM Human-Computer Interaction. vol. 2, pp. 102:1–31 (2018)
39. Lee, C., Zappaterra, L., Kwanghee Choi, Hyeong-Ah Choi: Securing smart home: Technologies, security challenges, and security requirements. In: 2014 IEEE Conference on Communications and Network Security. pp. 67–72 (Oct 2014)
40. Lei, M., Yang, Y., Ma, N., Sun, H., Zhou, C., Ma, M.: Dynamically enabled defense effectiveness evaluation of a home internet based on vulnerability analysis and attack layer measurement. Personal Ubiquitous Comput. 22(1), 153–162 (Feb 2018), https://doi.org/10.1007/s00779-017-1084-3
41. Lei, X., Tu, G., Liu, A.X., Li, C., Xie, T.: The insecurity of home digital voice assistants - vulnerabilities, attacks and countermeasures. In: 2018 IEEE Conference on Communications and Network Security (CNS). pp. 1–9 (May 2018)
42. Li, H., Gong, S., Lai, L., Han, Z., Qiu, R.C., Yang, D.: Efficient and secure wireless communications for advanced metering infrastructure in smart grids. IEEE Transactions on Smart Grid 3(3), 1540–1551 (Sep 2012)
43. Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., Fu, X.: Security vulnerabilities of internet of things: A case study of the smart plug system. IEEE Internet of Things Journal 4(6), 1899–1909 (Dec 2017)
44. Liu, H., Li, C., Jin, X., Li, J., Zhang, Y., Gu, D.: Smart solution, poor protection: An empirical study of security and privacy issues in developing and deploying smart home devices. In: Proceedings of the 2017 Workshop on Internet of Things Security and Privacy. pp. 13–18. IoTS&#38;P '17, ACM, New York, NY, USA (2017), http://doi.acm.org/10.1145/3139937.3139948
45. Liu, Y., Hu, S., Ho, T.: Leveraging strategic detection techniques for smart home pricing cyberattacks. IEEE Transactions on Dependable and Secure Computing 13(2), 220–235 (March 2016)
46. Liu, Y., Hu, S., Ho, T.Y.: Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks. In: Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design. pp. 183–190. ICCAD '14, IEEE Press, Piscataway, NJ, USA (2014), http://dl.acm.org/citation.cfm?id=2691365.2691404
47. Liu, Y., Hu, S., Wu, J., Shi, Y., Jin, Y., Hu, Y., Li, X.: Impact assessment of net metering on smart home cyberattack detection. In: Proceedings of the 52Nd Annual Design Automation Conference. pp. 97:1–97:6. DAC '15, ACM, New York, NY, USA (2015), http://doi.acm.org/10.1145/2744769.2747930

48. Ma, X., Goonawardene, N., Tan, H.P.: Identifying elderly with poor sleep quality using unobtrusive in-home sensors for early intervention. In: Proceedings of the 4th EAI International Conference on Smart Objects and Technologies for Social Good. pp. 94–99. Goodtechs '18, ACM, New York, NY, USA (2018), http://doi.acm.org/10.1145/3284869.3284894
49. Mahadewa, K.T., Wang, K., Bai, G., Shi, L., Dong, J.S., Liang, Z.: Homescan: Scrutinizing implementations of smart home integrations. In: 2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS). pp. 21–30 (Dec 2018)
50. Malik, K.M., Malik, H., Baumann, R.: Towards vulnerability analysis of voice-driven interfaces and countermeasures for replay attacks. In: 2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR). pp. 523–528 (March 2019)
51. McMahon, E., Patton, M., Samtani, S., Chen, H.: Benchmarking vulnerability assessment tools for enhanced cyber-physical system (cps) resiliency. In: 2018 IEEE International Conference on Intelligence and Security Informatics (ISI). pp. 100–105 (Nov 2018)
52. Meng, Y., Wang, Z., Zhang, W., Wu, P., Zhu, H., Liang, X., Liu, Y.: Wivo: Enhancing the security of voice control system via wireless signal in iot environment. In: Proceedings of the Eighteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing. pp. 81–90. Mobihoc '18, ACM, New York, NY, USA (2018), http://doi.acm.org/10.1145/3209582.3209591
53. Menon, D.M., Radhika, N.: Anomaly detection in smart grid traffic data for home area network. In: 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT). pp. 1–4 (March 2016)
54. Moody, M., Hunter, A.: Exploiting known vulnerabilities of a smart thermostat. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST). pp. 50–53 (Dec 2016)
55. Mosenia, A., Jha, N.K.: A Comprehensive Study of Security of Internet-of-Things. IEEE Transactions on Emerging Topics in Computing 5(4), 586–602 (2016)
56. Namboodiri, V., Aravinthan, V., Mohapatra, S.N., Karimi, B., Jewell, W.: Toward a secure wireless-based home area network for metering in smart grids. IEEE Systems Journal 8(2), 509–520 (June 2014)
57. Roux, J., Alata, , Auriol, G., Kaâniche, M., Nicomette, V., Cayre, R.: Radiot: Radio communications intrusion detection for iot - a protocol independent approach. In: 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA). pp. 1–8 (Nov 2018)
58. Roux, J., Alata, , Auriol, G., Nicomette, V., Kâaniche, M.: Toward an intrusion detection approach for iot based on radio communications profiling. In: 2017 13th European Dependable Computing Conference (EDCC). pp. 147–150 (Sep 2017)
59. Salami, S.A., Baek, J., Salah, K., Damiani, E.: Lightweight encryption for smart home. In: 2016 11th International Conference on Availability, Reliability and Security (ARES). pp. 382–388 (Aug 2016)
60. Saleh, M., Al Barghuthi, N.B., Alawadhi, K., Sallal, F., Ferrah, A.: Streamlining x201c;smart grid end point devices x201d; vulnerability testing using single board computer. In: 2018 Advances in Science and Engineering Technology International Conferences (ASET). pp. 1–6 (Feb 2018)
61. Sanchez, I., Satta, R., Fovino, I.N., Baldini, G., Steri, G., Shaw, D., Ciardulli, A.: Privacy leakages in smart home wireless technologies. In: 2014 International Carnahan Conference on Security Technology (ICCST). pp. 1–6 (Oct 2014)

62. Shen, T., Ma, M.: Security enhancements on home area networks in smart grids. In: 2016 IEEE Region 10 Conference (TENCON). pp. 2444–2447 (Nov 2016)
63. Sivanathan, A., Loi, F., Gharakheili, H.H., Sivaraman, V.: Experimental evaluation of cybersecurity threats to the smart-home. In: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). pp. 1–6 (Dec 2017)
64. Sivaraman, V., Chan, D., Earl, D., Boreli, R.: Smart-phones attacking smart-homes. In: Proceedings of the 9th ACM Conference on Security &#38; Privacy in Wireless and Mobile Networks. pp. 195–200. WiSec '16, ACM, New York, NY, USA (2016), http://doi.acm.org/10.1145/2939918.2939925
65. Sun, A., Gong, W., Shea, R., Liu, J.: A castle of glass: Leaky iot appliances in modern smart homes. IEEE Wireless Communications 25(6), 32–37 (December 2018)
66. Tabrizi, F.M., Pattabiraman, K.: Intrusion detection system for embedded systems. In: Proceedings of the Doctoral Symposium of the 16th International Middleware Conference. pp. 9:1–9:4. Middleware Doct Symposium '15, ACM, New York, NY, USA (2015), http://doi.acm.org/10.1145/2843966.2843975
67. Tekeoglu, A., Tosun, A.: Blackbox security evaluation of chromecast network communications. In: 2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC). pp. 1–2 (Dec 2014)
68. Tekeoglu, A., Tosun, A.: A closer look into privacy and security of chromecast multimedia cloud communications. In: 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). pp. 121–126 (April 2015)
69. Trimananda, R., Younis, A., Wang, B., Xu, B., Demsky, B., Xu, G.: Vigilia: Securing smart home edge computing. In: 2018 IEEE/ACM Symposium on Edge Computing (SEC). pp. 74–89 (Oct 2018)
70. Whitehurst, L.N., Andel, T.R., McDonald, J.T.: Exploring Security in ZigBee Networks. In: Proceedings of the 9th Annual Cyber and Information Security Research Conference. pp. 25–28. CISR '14, ACM, New York, NY, USA (2014), http://doi.acm.org/10.1145/2602087.2602090
71. Wurm, J., Hoang, K., Arias, O., Sadeghi, A., Jin, Y.: Security analysis on consumer and industrial iot devices. In: 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC). pp. 519–524 (Jan 2016)
72. Zeng, E., Mare, S., Roesner, F.: End User Security & Privacy Concerns with Smart Homes. In: Symposium on Usable Privacy and Security (SOUPS) (2017)
73. Zhang, M., Liu, Y., Wang, J., Hu, Y.: A new approach to security analysis of wireless sensor networks for smart home systems. In: 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS). pp. 318–323 (Sep 2016)