5-25-2018

Survey of Security in Home Connected Internet of Things

Benjamin Spriggs
Portland State University

Survey of Security in Home Connected Internet of Things

by
Benjamin Spriggs

An undergraduate honors thesis submitted in partial fulfillment of the
requirements for the degree of
Bachelor of Science
in
University Honors
and
Computer Science

Thesis Adviser
Suresh Singh

Portland State University
2018

Survey of Security in Home Connected Internet of Things

Portland State University
bspriggs@pdx.edu
Portland State University
singhsp@pdx.edu

ABSTRACT

Security and privacy have been increasingly important issues, especially surrounding privacy in consumer's homes. Internet of things devices, while providing opportunity, also provide danger through poor or inconsistent implementation of security protocols or hardening techniques. Security research around home connected internet of things devices must then have more significant and summative research and literature to combat these dangers. This paper presents an overview of existing research focusing on internet of things devices intended for consumers in the home, discusses some specific case studies of vulnerabilities in existing and common devices, overviews some best practices as they're suggested in various papers, and finally adds some discussion on interesting solutions to security in the connected internet of things home. This paper finds that many home connected internet of things devices are lacking minimal security, and that both consumption and production of home connected internet of things devices require a security focus in order to provide a stable foundation for this rapidly proliferating infrastructure.

KEYWORDS

Internet of things, Internet of things security, connected home devices, connected home device security, privacy issues, security issues, security vulnerabilities, NIST

1 INTRODUCTION

The internet of things, as a concept, simultaneously has the potential to be one of the things that revolutionize markets, practices, industries and lifestyles as we know it, and to be something that grinds the progress of society to a halt with miscommunication and sabotage. As it was coined in 1999 [9], the "internet of things" loosely has the idea of a network of devices that live in things, in the objects that we use to perform normal tasks, and which allow for a constant stream of communication, data-collection, and computation [11] to allow for more and more ridiculous Star Trek-like feats of industry [10]. There are many domains to this wide-reaching concept of "the internet of things" , that can be somewhat nebulously divided into categories like medical, industrial, commercial, retail, consumer, transportation, vehicles, and on and on [17]. Think Amazon Alexa to smart conveyor belts [3] to smart biodigesters and in-hospital newborn-locators [7].

Security in the internet of things, then, needs to be a high priority, since the more things you can do, and the more data you have, the greater the potential for exploitation and manipulation.

In practice, things (their internet, and their security) are more complicated.

This paper surveys the state of connected home internet of things devices, highlighting existing literature on the topic of security of internet of things devices, documented and researched vulnerabilities as they appear in common connected home devices, and best practices for manufacturers, developers, and consumers of connected home internet of things devices to mitigate potential risks and vulnerabilities in their devices.

Quality of papers talking about IoT security and devices is quite variable. Security and home IoT devices have hundreds of proposed solutions, but very few comprehensive surveys of connected home IoT security. Interesting surveys and white-papers will be mentioned later.

Additionally, this paper builds on existing research, laying out the vulnerabilities for select devices and grouping similar vulnerabilities into the following categories:

(1) Application layer - data access/ recovery attacks, authentication issues
(2) Network layer - network protocol problems, port hardening, reflection etc
(3) Perception layer - attacks dealing with fake IoT nodes, side channel/ replay attacks, et cetera

This paper will not spend too much time on a multitude of specific devices, since there's often a security vulnerability in the components that compose many different IoT products [16] and engaging a more holistic approach to talking about security will begin to tackle the issue of security at scale for a diverse range of devices [31]. This paper will instead choose various characteristic devices that represent a common category of consumer-focused, connected home IoT devices.

There are many other efforts at cataloging common IoT vulnerabilities, such as this list of common vulnerabilities [1], and this paper will not go into too much depth into those lists, since themes will tend to appear when looking at various IoT device security vulnerabilities.

Finally, this paper will highlight best security practices for users and producers of connected home internet of things devices, as well as discussing a few interesting potential solutions to various inherent problems to securing internet of things devices.

2 EXISTING LITERATURE

In [28], the authors give a detailed survey of inherent security vulnerabilities (via protocols or compromised techniques or practices) and privacy challenges in the three layers of IoT devices (perception, application, network). The authors organize the survey to help with the state of security in IoT devices as of publication, as well as potential steps for further securing IoT devices in the future.

This survey addresses the same problem and goes about solving it in a similar way to the current paper, cataloging vulnerabilities and challenges in IoT devices as well as providing a taxonomy of the field as it stands with respect to security. The difference between

work of the two is that the Mendez survey catalogs IoT security in general, tackling a wide variety of protocols and software intended to address different domains of IoT devices. This paper focuses more specifically on connected home IoT devices, providing a more focused look at security in a domain of IoT devices that has a huge potential for affecting lives of general consumers of new connected smart home devices. As well as focusing on this specific domain, this paper references other related work in this field, providing a larger network of security research for manufacturers, developers, and security researchers to draw on to develop more secure IoT devices.

The Open Web Application Security Project (OWASP) Internet of Things Project is designed to "help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies." [8] A number of the documents that this project has produced overlap with the scope of this survey, and include:

- IoT Attack Surface Areas
- IoT Testing Guides
- IoT Security Guidance
- Principles of IoT Security
- IoT Framework Assessment

The project looks at various specific vulnerabilities (memory overflow, weak passwords in authentication web pages and user software, etc) and open attack surfaces present on IoT devices, and address them with general security guidelines since the scope of the project is attempting to address universal testing surfaces for IoT devices [29]. This survey addresses the same problem of security vulnerabilities affecting multiple IoT devices, but goes about addressing the problem by highlighting existing solutions and best practices rather than developing a testing framework that would secure against common attack surfaces.

In [12], the authors do a thorough security analysis of always-on, customer oriented devices with potential to impact the physical environment they're in significantly if hacked. Their methodology was to install and configure each device according to manufacturer instruction, and run each devices separately through a variety of tests that either involved inspecting network traffic, reverse engineering device software, or impersonating captured traffic. The authors found that "product manufacturers weren't focused enough on security and privacy, as a design priority, putting consumers at risk for an attack or physical intrusion."

In [23], the authors:

(1) Discuss the differences between CPS (cyber-physical systems) and IoT - IoT being more focused on the networking/ communication potential of multiple CPS
(2) Discuss the architecture of the IoT (same three layers as used in the specific devices section in this paper)
(3) Discuss enabling technologies and challenges in the different layers of architecture for the IoT
(4) Discuss security and privacy drawbacks and benefits from using IoT
(5) Discuss integrating Fog/ Edge computing and the IoT

The authors are looking at a higher level than the specifics of connected home IoT, but discussion in it and related papers affect this field.

This survey addresses a different problem than what the authors of this survey were trying to accomplish, since their survey lays out IoT and CPS in a fog/edge computing context, and less so in a connected home context, as well as listing potential drawbacks and benefits of IoT devices rather than practical ones. This survey spends more time on existing vulnerabilities and existing solutions to security and privacy issues concerning IoT devices in the field.

The authors of this paper [24], binary analysis, network analysis, etc to show the inherent vulnerabilities in one JoyLink SDK solution.

The authors also point to work on security analysis of different specific devices, namely the Philips Hue lightbulb and various devices developed by FitBit, highlighting the focus of these papers on specific device security over general security and privacy concerns.

Regarding protocols used commonly by smart home devices, the authors highlight various flaws found in the Zigbee and BLE protocols respectively by this paper [30] and this paper [4].

In [26], the authors catalog the current status of IoT security, at the level of the different common application designs and vulnerabilities in most IoT devices. The paper uses the perception-application-network layering for IoT devices, and talks about the security features and principles required for IoT device security. Namely: confidentiality, integrity, availability, authentication, "light solutions" , heterogeneity, "policies" , and having "key management systems" . The paper lists security challenges for each layer, and a small list of countermeasures that can be taken to secure each layer.

The authors also highlight the state of IoT security research, mostly being that it is full of potential countermeasures that are limited in addressing the concerns presented.

3 CASE STUDIES OF SAMPLE DEVICE SECURITY VULNERABILITIES

3.1 Introduction

This section will cover specific vulnerabilities of specific devices, each chosen to be somewhat representative of a larger majority of devices similar to it in design, either architecturally or through software.

The devices are:

- Samsung SmartCam
  - Chosen as an example of an IP Camera that receives some software updates after initial release
- Sricam SP009 IP Webcam
  - Chosen as an example of an IP camera that receives no software updates after initial release
- Nest Smoke Alarm
  - Chosen as an example of a connected home safety device and home sensor. Similar devices might include the Philip Hue Lightbulb, Belkin Smart Switch, Pixstar Photo Frame, Withings Home baby monitor, etc
- Hello Barbie
  - Chosen as an example of a connected home smart toy, or home entertainment device

- Amazon Echo
  - Chosen as an example of a digital voice assistant. Similar devices might include the Google Home, Amazon Echo Dot, Apple HomePod, Insignia Voice, etc
- HP Envy Printer
  - Chosen as an example of a WiFi enabled printer with mobile print capabilities that is open to internet connections

3.2 Samsung SmartCam

3.2.1 Intended Use. The Samsung SmartCam is an internet-enabled remote monitoring camera with real-time alarm and audio/video recording, two way audio, and low light video conditions that is meant for connected home security systems. The idea is that this allows a homeowner to have a available-anywhere private video and audio feed to important areas to their home. There were apps available for Android and iOS to enable homeowners to also check these feeds using their phones.

3.2.2 Application Layer Vulnerabilities.

Remote root command execution. Remote management software for the device failed to properly escape user input while accepting firmware upgrades, providing attackers a vector for remote root command execution.

DNS Spoofing. The Samsung SmartCam fails to implement DNSSEC protocols that prevent DNS spoofing attacks. This gives attackers a vector to impersonate server or user traffic mid-transaction, possibly capturing sensitive information.

Open and Vulnerable Ports (TCP/UDP). The Samsung SmartCam has many open and responsive ports listening on the public internet, one of which is vulnerable to automated discovery. This, coupled with other network vulnerabilities, cause this device to be vulnerable either to denial of service attacks to itself, or reflecting traffic from one malicious source to another target.

3.2.3 Network Layer Vulnerabilities.

Reflection attacks. This device is vulnerable to a number of different reflection attacks[1], where network traffic from a malicious source is reflected by a compromised device to a target.

3.3 Sricam SP009 IP Webcam

3.3.1 Intended Use. The Sricam SP009 IP Webcam is intended to be an easy to use, quick to setup home or business security solution, providing wireless video monitoring, night-time video, and audio recording.

3.3.2 Application Layer Vulnerabilities.

Easily Discoverable Video Feed URLs. Researchers were able to discover an unencrypted video feed broadcast by the IP camera using a list of commonly used video feed URLs for the video broadcast protocol used by the camera. Streams were unencrypted, and required no authentication in order to view them, posing a privacy risk to users of this camera.

[1] ICMP Reflection. SNMP Reflection. SNMP Public Community String Reflection. See this paper [25] for details.

Plain Text Mobile Application Credentials. In the companion mobile application for the camera, researchers were able to discover the IP camera's credentials being stored in a plain text format, posing authentication issues for users of the accompanying mobile app and this camera.

3.3.3 Network Layer Vulnerabilities.

Unencrypted communication. All communications between IP Camera, phone, and server were broadcast in plain text, which is a significant security risk. Researchers were able to capture network credentials by inspecting data in-transit.

3.4 Nest Smoke Alarm

3.4.1 Intended Use. The Nest Smoke Alarm is intended to a be an easy to use, quick to setup smoke alarm that gives the user the ability to check carbon dioxide levels, mute false alarms, give phone and voice alerts when the alarm is about to go off, and periodically tests its own battery and speaker to ensure it's able to respond in an emergency.

3.4.2 Network Layer Vulnerabilities.

DNS Spoofing. The Nest smoke alarm fails to implement DNSSEC protocols that prevent DNS spoofing attacks. This gives attackers a vector to impersonate server or user traffic mid-transaction, possibly capturing sensitive information.

Fake Server. This device communicates with a server that fails to identify itself as valid, giving attackers a vector at spoofing and capturing user data via MiTM attacks.

Open Ports. This device has open but not vulnerable ports.

Reflection Attacks. This device is vulnerable to ICMP reflection attacks.

3.5 Hello Barbie

3.5.1 Intended Use. Hello Barbie is a toy developed by Mattel that responds to user voice commands via a companion phone app by playing different pre-defined lines in response [5].

3.5.2 Application Layer Vulnerabilities.

Weak Passwords. The mobile API and Toytalk website allow users to use weak passwords, which leaves user accounts open to brute force and dictionary password attacks.

No Password Brute Force Protections. The mobile API and Toytalk website allow unlimited password guesses, which combined with allowing weak passwords open user accounts open to brute force and dictionary password attacks.

URL Redirect. Clients of the Hello Barbie Companion application can be sent malicious toytalk.com links, which might redirect users to phishing websites, or an HTTP version of toytalk.com that might expose session cookies.

Mutual Configuration Authentication. The Hello Barbie Companions use the same mutual certificate for authentication and

configuration of the device. This opens user devices to being configured by a malicious actor with access to this certificate, without asking for additional per-device authentication.

Password Reset Page Expiration. The password reset page for user accounts does not expire. This opens users to an attack where a user clicks on a link which resets their password, opening their password to be set by an attacker later.

Unauthenticated Audio File Access. There is no authentication to access audio files uploaded by the Hello Barbie Companion to cloudfront.net, which opens up the possibility of user content being consumed by malicious actors without permission.

Username Enumeration. The mobile API allows attackers to be able to verify that certain user accounts exist.

3.5.3 Network Layer Vulnerabilities.

Sensitive Information via HTTP. Several layers in the application use HTTP instead of HTTPS.

Stored Cross-Site Scripting. Malicious Javascript stored on the tools.toytalk domain could be used to allow persistent backdoor access.

Improper Cookie Storage. The secure flag for cookies stored on the Hello Barbie Companion website is not set, which can allow for cookies to be sent insecurely over HTTP.

Unencrypted WiFi Pairing. While pairing, the Hello Barbie Companion uses an unencrypted WiFi network to pair and configure the device.

Logged Application IDs. The application ID is stored in Logcat for the Android application, which opens up user session hijacking if Logcat output is leaked.

Unlimited CORS. CORS requests are not constrained to application websites, which opens up any website to be able to make Cross-Origin requests to puppeteer.toytalk.com.

DNS Spoofing. The Samsung SmartCam fails to implement DNSSEC protocols that prevent DNS spoofing attacks. This gives attackers a vector to impersonate server or user traffic mid-transaction, possibly capturing sensitive information.

3.6 Amazon Echo

3.6.1 Intended Use.

"The Amazon Echo is a hands-free, voice-activated, virtual assistant that uses the Amazon Alexa service to answer questions or to allow you to give commands such as to play music, set alarms or to control smart home devices that are Alexa-compatible." [13]

3.6.2 Perception Layer Vulnerabilities.

Malicious Voice Command. As is the case with any improperly-configured interactive voice assistant, not constraining the voices that are able to make commands to the Amazon Echo can have unintended side effects. [15]

Non-human Voice Command. Related to vulnerabilities in other interactive voice assistants, commands can be sent to the Amazon Echo via means not intelligible or discernible to humans, as described in this paper. [6] This leaves the option of large numbers of interactive voice assistants, like the Amazon Echo, to be controlled with television advertising or by playing audio into a home.

3.6.3 Application Layer Vulnerabilities.

Gaining Root-Level Access to System. Through a process outlined by these [20] researchers (and alternative route here[2]), root-level access of the Amazon Echo can be gained by an attacker of the device. Many hardware-level root attacks have been fixed by Amazon as they've been reported.

3.6.4 Network Layer Vulnerabilities.

Replay Attacks. Researchers were able to replay packets sent from the Amazon Echo. [20] This leaves open the possibility for attackers, possibly knowing the contents of the already encrypted HTTPS packets, replaying a purchase or transaction repeatedly to deplete a user's card or bank account.

METADATA. Researchers found that it's possible in theory, and specifically for four devices, to use characteristics of encrypted data streams coming into and out of an ISP to glean sensitive information about users. For example, sleep and other health monitors broadcasting information to backend or third-party servers could give away users' sleep patterns and nighttime habits to a passive observer, based on a three step strategy used in the paper.

3.7 HP Envy Printer

3.7.1 Intended Use.

The HP Envy printer is a wireless all-in-one printer and scanner intended to be easy to setup and quick to use for home printing needs. The printer communicates with a mobile application that allows printing from various mobile devices.

3.7.2 Application Layer Vulnerabilities.

Plaintext Device to User Application Communication. The HP Envy printer allows plain text device to user application communication, which leaves users of the printer and user application vulnerable to attackers either obtain sensitive information via inspecting network packets, or by rendering the printer unusable through issuing simple commands without encryption or authentication.

Replay Attacks. Researchers found that the HP Envy printer was vulnerable to replay attacks, where an attacker would obtain a network packet in-transit to the printer, and replay the communication repeatedly to render the printer unusable.

Fake Server. This device communicates with a server that fails to identify itself as valid, giving attackers a vector at spoofing and capturing user data via MiTM attacks.

3.7.3 Network Layer Vulnerabilities.

[2] https://github.com/echohacking/wiki/wiki/Echo got fixed too

Open and Vulnerable Ports (TCP/UDP). The HP Envy printer has many open and responsive ports listening on the public internet, all of which are open to automated discovery, and to telnet connections. This, coupled with other network vulnerabilities, cause this device to be vulnerable either to much more complex denial of service attacks to itself, or reflecting traffic from one malicious source to another target.

Reflection attacks. This device is vulnerable to a number of different reflection attacks[3], where network traffic from a malicious source is reflected by a compromised device to a target.

DNS Spoofing. The HP Envy printer fails to implement DNSSEC protocols that prevent DNS spoofing attacks. This gives attackers a vector to impersonate server or user traffic mid-transaction, possibly capturing sensitive information.

4 BEST PRACTICES

4.1 OWASP Security Guidance

OWASP gives a categorized list of security best practices for manufacturers, developers, and users of IoT devices as part of its IoT project, launched January 2017 to help improve IoT device security.

Briefly, those categories are as follows:

(1) Insecure Web Interface
(2) Insufficient Authentication/ Authorization
(3) Insecure Network Services
(4) Lack of Transport Encryption
(5) Privacy Concerns
(6) Insecure Cloud Interface
(7) Insecure Mobile Interface
(8) Insufficient Security Configurability
(9) Insecure Software/ Firmware
(10) Poor Physical Security

As well, a general guideline offered by this document is to enable updates for all IoT devices, to mitigate the risk of common vulnerabilities being propagated by un-updateable product releases.

4.2 Choosing Secure Communication Protocols

The authors of this paper[4] review various high-use smart home IoT protocols, their architecture and known vulnerabilities, and arrived at Z-Wave, with caveats[5], as a best candidate for a secure communications protocol.

4.3 Taking Inventory of Vulnerabilities

Many security researchers and major companies developing IoT devices [2] take regular inventory of vulnerabilities discovered for similar devices[6], and engage in penetration testing on their own devices. Tools like Nessus, Qualys, Burp Suite that are targeted towards finding common vulnerabilities in devices can be used to harden existing devices.

[3] ICMP Reflection. SNMP v1 Reflection. See this paper [25] for details.
[4] An overview of wireless IoT protocol security in the smart home domain
[5] The authors highlight that attacks on insufficient implementations of Z-Wave don't compromise the security of the protocol as a whole.
[6] Through a security vulnerability database like NIST.

4.4 Taking steps within a Home

The authors of this paper [14] offered four strategies consumers might use to make their own homes secure, all of which focused on masking sensitive characteristics of network traffic and nodes in a home WiFi network.

5 DISCUSSION

As it stands, security research and practice has a ways to go in the domain of connected home internet of things devices, especially as it's reviewed in literature and reflected in practice, security and privacy are often lower priorities than convenience in newer fields of technology. I want to bring some attention to some interesting propositions for securing the widely expanding, mostly insecure IoT network that went beyond specifying a new protocol or highlighting weaknesses in existing ones. [19] [22] [27] [30] [32]

In [21], the authors lay out a gateway based firewall solution (named Heimdall) for the problem of distributed denial of service attacks coming from many, non updated IoT devices. The idea is that the cost of updating devices will continue to drive manufacturers to not continue providing security updates for their products, and solutions for security have to go beyond securing the software on the device and the physical device itself.

In [33], the authors demonstrate a systematic, scalable, scanning approach to identifying vulnerable devices exposed to the public internet, and highlight the vulnerable state of the internet of things. Using a search engine targeted for the IoT[7], researchers were able to target pervasive consumer grade products and scan them using a security vulnerability scanner, and demonstrate that a significant portion of the internet was vulnerable to attacks similar to ones described earlier.

In [18], the authors propose a virtualization based framework to securing IoT devices, where the computation and control of a device's sensors would be handled by a virtualized cluster that would handle computation and network tasks, which then wouldn't suffer the same lightweight and low-impact security protocol requires for existing devices. Continued research has yet to be done on the feasibility of a framework like this one.

6 CONCLUSION

There have been many initiatives to bring more focus to the subject [34], but there's still a long way to go before we stop seeing the same or similar vulnerabilities appear on broad swaths of consumer-available IoT devices. Hopefully the work presented, as well as continued efforts to highlight the growing need for security and privacy as first-class citizens in all aspects of technology, will spark continued discussion on security for connected home IoT devices.

REFERENCES

[1] [n. d.]. CWE - CWE-1026: Weaknesses in OWASP Top Ten (2017) (3.1). https://cwe.mitre.org/data/definitions/1026.html
[2] [n. d.]. DDoS_White_Paper.Pdf. https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf
[3] [n. d.]. Engineers Develop Smart Conveyor Rollers for the Factory of the Future. https://phys.org/news/2016-03-smart-conveyor-rollers-factory-future.html
[4] [n. d.]. Explicating SDKs: Uncovering Assumptions Underlying Secure Authentication and Authorization | USENIX. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/wang_rui

[7] shodan.io

[5] [n. d.]. Hello BarbieâĎć Companion App. https://toytalk.com/product/hello-barbie/

[6] [n. d.]. Hidden Voice Commands | USENIX. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/carlini

[7] [n. d.]. Internet of Things in Healthcare Keeps Patients Healthy, Safe. http://internetofthingsagenda.techtarget.com/feature/Internet-of-Things-in-healthcare-keeps-patients-healthy-safe

[8] [n. d.]. OWASP Internet of Things Project - OWASP. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main

[9] [n. d.]. That 'Internet of Things' Thing - 2009-06-22 - Page 1 - RFID Journal. http://www.rfidjournal.com/articles/view?4986

[10] [n. d.]. Was Star Trek the Start of IoT? https://www.ibm.com/blogs/internet-of-things/star-trek/

[11] International Telecommunications Union . [n. d.]. Internet of Things Global Standards Initiative. https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

[12] Veracode . [n. d.]. The Internet of Things: Security Research Study. https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf

[13] Tony Anscombe. [n. d.]. IoT AND PRIVACY BY DESIGN IN THE SMART HOME. https://www.welivesecurity.com/wp-content/uploads/2018/02/ESET_MWC2018_IoT_SmartHome.pdf

[14] Noah Apthorpe, Dillon Reisman, and Nick Feamster. [n. d.]. A Smart Home Is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. ([n. d.]). arXiv:cs/1705.06805 http://arxiv.org/abs/1705.06805

[15] Hyunji Chung, Michaela Iorga, Jeffrey Voas, and Sangjin Lee. [n. d.]. âĂIJAlexa, Can I Trust You?âĂİ. 50, 9 ([n. d.]), 100–104. https://doi.org/10.1109/MC.2017.3571053

[16] Lucian Constantin. 2017-01-17T06:44-05:00. Critical Flaw Lets Hackers Take Control of Samsung SmartCam Cameras. https://www.csoonline.com/article/3158468/security/critical-flaw-lets-hackers-take-control-of-samsung-smartcam-cameras.html

[17] Lippo Group Digital. 03:33:56 UTC. Domain Specific IoT. (03:33:56 UTC). https://www.slideshare.net/khusuma/domain-specific-iot

[18] M. A. ElAffendi and A. L. Alamudy. [n. d.]. Could Virtualization Be the Ultimate Solution for IoT Resource Constrained Devices Problem? A Multilevel Security Framework Based on Device Virtualization. In *2017 International Conference on Computer and Applications (ICCA)* (2017-09). 232–237. https://doi.org/10.1109/COMAPP.2017.8079750

[19] J. Granjal, E. Monteiro, and J. SÃą Silva. thirdquarter 2015. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. 17, 3 (thirdquarter 2015), 1294–1312. https://doi.org/10.1109/COMST.2015.2388550

[20] William Haack, Madeleine Severance, Michael Wallace, and Jeremy Wohlwend. [n. d.]. Security Analysis of the Amazon Echo. ([n. d.]), 14.

[21] J. Habibi, D. Midi, A. Mudgerikar, and E. Bertino. [n. d.]. Heimdall: Mitigating the Internet of Insecure Things. 4, 4 ([n. d.]), 968–978. https://doi.org/10.1109/JIOT.2017.2704093

[22] M. T. Hammi, E. Livolant, P. Bellot, A. Serhrouchni, and P. Minet. [n. d.]. A Lightweight IoT Security Protocol. In *2017 1st Cyber Security in Networking Conference (CSNet)* (2017-10). 1–8. https://doi.org/10.1109/CSNET.2017.8242001

[23] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao. [n. d.]. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. 4, 5 ([n. d.]), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200

[24] Hui Liu, Changyu Li, Xuancheng Jin, Juanru Li, Yuanyuan Zhang, and Dawu Gu. [n. 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* (2017) *(IoTS&P '17)*. ACM, 13–18. https://doi.org/10.1145/3139937.3139948

[25] Franco Loi, Arunan Sivanathan, Hassan Habibi Gharakheili, Adam Radford, and Vijay Sivaraman. [n. d.]. Systematically Evaluating Security and Privacy for Consumer IoT Devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy* (2017) *(IoTS&P '17)*. ACM, 1–6. https://doi.org/10.1145/3139937.3139938

[26] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan. [n. d.]. Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (2015-12). 336–341. https://doi.org/10.1109/ICITST.2015.7412116

[27] S. Marksteiner, V. J. E. Jimenez, H. Valiant, and H. Zeiner. [n. d.]. An Overview of Wireless IoT Protocol Security in the Smart Home Domain. In *2017 Internet of Things Business Models, Users, and Networks* (2017-11). 1–8. https://doi.org/10.1109/CTTE.2017.8260940

[28] Diego M. Mendez, Ioannis Papapanagiotou, and Baijian Yang. [n. d.]. Internet of Things: Survey on Security and Privacy. ([n. d.]). arXiv:cs/1707.01879 http://arxiv.org/abs/1707.01879

[29] Daniel Miessler. 15:54:32 UTC. IoT Attack Surfaces – DEFCON 2015. (15:54:32 UTC). https://www.slideshare.net/danielmiessler/iot-attack-surfaces-defcon-2015

[30] E. Ronen, A. Shamir, A. O. Weingarten, and C. OâĂŹFlynn. [n. d.]. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. In *2017 IEEE Symposium on Security and Privacy (SP)* (2017-05). 195–212. https://doi.org/10.1109/SP.2017.14

[31] Vinay Sachidananda, Shachar Siboni, Asaf Shabtai, Jinghui Toh, Suhas Bhairav, and Yuval Elovici. [n. d.]. Let the Cat Out of the Bag: A Holistic Approach Towards Security Analysis of the Internet of Things. ACM Press, 3–10. https://doi.org/10.1145/3055245.3055251

[32] V. Sharma, A. Vithalkar, and M. Hashmi. [n. d.]. Lightweight Security Protocol for Chipless RFID in Internet of Things (IoT) Applications. In *2018 10th International Conference on Communication Systems Networks (COMSNETS)* (2018-01). 468–471. https://doi.org/10.1109/COMSNETS.2018.8328246

[33] R. Williams, E. McMahon, S. Samtani, M. Patton, and H. Chen. [n. d.]. Identifying Vulnerabilities of Consumer Internet of Things (IoT) Devices: A Scalable Approach. In *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)* (2017-07). 179–181. https://doi.org/10.1109/ISI.2017.8004904

[34] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu. [n. d.]. Handling a Trillion (Unfixable) Flaws on a Billion Devices: Rethinking Network Security for the Internet-of-Things. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks* (2015) *(HotNets-XIV)*. ACM, 5:1–5:7. https://doi.org/10.1145/2834050.2834095