Attack mapping for the Internet of Things

Authors
William Bathgate, MSc (Royal Holloway, 2021)
Salaheddin Darwish, ISG, Royal Holloway

Abstract

There are currently more devices connected to the Internet than people on this planet. These objects which connect to the Internet to share data and resources are known as Internet of Things (IoT) devices. The rate of adoption across various fields in our modern society is increasing rapidly and nowadays, these devices are widely integrated within homes in hopes of improving ones' lifestyle. However, with this comes an increase in the attack surface.
The challenge with smart home IoT devices is ensuring that the devices, approaches, and frameworks used are secure, both at present and in the future as new technologies are developed. This is particularly difficult as developers do not necessarily know what environment their device will be operating in. What country their device may end up in, and what technologies and devices it will be operating and communicating with are both unknown to the developer. Furthermore, with the introduction of each IoT device in a home network the attack surface and risks of a security threat increase.
This article puts forward a practical model for investigating the security of a home network to evaluate and track what pathways an attacker may use to compromise it. The model allows an individual to understand the attacks, evaluate whether the attack is feasible within the context of a specific network, and finally action it, reducing the risk. [a]

[a] This article is published online by Computer Weekly as part of the 2022 Royal Holloway information security thesis series `https://www.computerweekly.com/ehandbook/Headline-Royal-Holloway-Attack-mapping-for-the-internet-of-things`. It is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at `https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/`.

Introduction

Juniper Research[1] predicts that by 2024 the total number of IoT connections will reach 83 billion. These devices, machines, or 'things', use the Internet's infrastructure to communicate and exchange data without the need for human interaction. However, in the case of the smart home, which is the focus of this article, humans will regularly interact with these devices. These 'things' communicating over the Internet are collectively known as the Internet of Things (IoT). It has been adopted by a range of domains including the industrial sector (which covers the smart grid, transport and logistics, factories and production, retail and consumer, healthcare), as well as the connected home and smart cities

Interoperability between these devices is an extremely complex issue. This is due largely to the rapid growth and adoption of the IoT, coupled with the sheer variety of devices, utilising different wireless technologies, standards, platforms, operating systems, and software. In addition to this, these devices must work within different countries across the globe all with unique requirements. These complexities introduce vulnerabilities, as specific configurations are left poorly tested, exploitable, and released due to the demand of the consumer market. As a consequence of the global pandemic, more and more people are working from home. Further to this, advancements in technology have enabled employees to effectively operate remotely. Home networks that were once used for personal reasons are now

[1] Juniper Research. (2022). IoT Connections to Reach 83 Billion by 2024, Driven by Maturing Industrial Use Cases. Juniperresearch.com. https://www.juniperresearch.com/press/iot-connections-to-reach-83-bn-by-2024. Published 2022. Accessed February 28, 2022.

transmitting sensitive business-related data. This makes individuals and home networks a valued target of cybercriminals.

This article proposes an IoT smart home attack map that allows an individual to evaluate the security of a network and reduce risks. This practical model demonstrates pathways an attacker may take to compromise a network. It first identifies a specific artefact an attacker may use to gain an initial foothold on the network, then it identifies methods to laterally move across the network to launch further attacks.

Impact

Home networks are being targeted by cybercriminals. In support of this, at Black Hat Europe 2020, Sygnia[2] described how an Eastern European cybercrime organisation (referred to as "Elliptical Spider") had exploited vulnerabilities in TP-Link home routers from individuals working from home. From this initial attack, they subsequently targeted a pharmaceutical company, attempting to extort $300,000,000.00 in Bitcoin.

Pentest Partners[3] have demonstrated many different scenarios where they have successfully exploited flaws in IoT devices. In 2021 they were able to hack into a home network and car by exploiting a deauthentication bug in Google Chromecast which was first discovered in 2014. The attacker can make the Chromecast connect to the attacker rather than the home network. The attacker can upload a YouTube video with verbal commands which will get sent to the Chromecast and consequently played through the television, which will then be picked up by the Alexa. Any device connected to the Alexa may then be controlled by the attacker.

Gmail user's credentials from a Samsung smart fridge (model RF28HMELBSR) were proven to be obtainable[4]. This is extremely dangerous as email is one of the main forms of communication users use to sign up for many services, be it e-commerce, social networking or business-related. If an attacker gains those details it could lead to further attacks such as blackmail and financial extortion, denial of availability to services by changing passwords on accounts, gathering further information and banking information from users, and taking control of any online accounts.

Smart home attack surfaces and common IoT attacks

Smart home attack surfaces could be grouped into the following:

- **Sensitive data storage.** Devices may store sensitive information such as credentials that an attacker can access, e.g., data stored in the hub before it is transmitted to the server. If this data is not encrypted, it can be readable to the attacker.
- **Access controls.** If an attacker gain access to the system, even as a standard user, they may be able to find a way to escalate their privileges to become a root user or administrator, or at least run commands as a root user.
- **Firmware attacks.** Another attack is when the firmware is changed or replaced by the attacker when there are no security controls or validation in place. This could prevent legitimate updates or security vulnerabilities from being patched, or even updated to have backdoors.

[2]Finkelstein, A., Warshavski, D. and Wasserman, B. 2020. Extortion Attack: A View From the Frontlines of Cyber. Black Hat Europe 2020, 9 Dec., Online (Sygnia Virtual Booth).

[3]Pentest Partners LLP. Hacking with Chromecast and Alexa | Pen Test Partners. Pentestpartners.com. https://www.pentestpartners.com/security-blog/hack-demo-video/hacking-a-home-and-a-car-with-chromecast-and-alexa/. Published 2021. Accessed February 24, 2021.

[4]Neagle C. Smart refrigerator hack exposes Gmail account credentials. Network World. https://www.networkworld.com/article/2976270/smart-refrigerator-hack-exposes-gmail-login-credentials.html. Published 2015. Accessed February 1, 2021.

- **System configuration.** This involves misconfigurations or resetting the device to an insecure state. This may be done accidentally by the user or perhaps by a maintenance engineer. However, it may also be done purposefully by an attacker, for example, disabling 2FA (Two-Factor Authentication).
- **Ports.** Attacks may be launched against services running on the network such as FTP, SSH, SNMP and Telnet. This can allow an attacker to remotely connect, access, and tamper with files, as well as take control of the vulnerable IoT device.
- **Backend.** If the IoT device makes use of a cloud service, a vulnerable cloud application may be exploited by an attacker.

Even if the hardware and device are secure, a vulnerability in the mobile application may be exploited. It only takes one weakness in the entire system for an attacker to gain an initial foothold. If the IoT device uses a web application in part of its framework, then web attacks may also be common.

Common IoT attacks

- Distributed Denial of Service (DDoS) attack. Bots in a botnet (a network of compromised devices) can send many requests and flood the IoT devices, gateways or applications, and cloud servers with packets rendering the service unavailable.
- Radio attack. An example of a radio attack is the rolling code attack. Rolling code is often found in doors that are within the smart home such as car doors or garage doors. An attacker may intercept a signal and jam it or replay it.
- Jamming attack. This type of attack jams a signal (Wi-Fi, GPS, etc.) and therefore prevents two devices from communicating with one another. This type of attack is both cheap and easy to carry out.
- BlueBorne attack. This type of attack exploits IoT devices that utilize Bluetooth wireless communications technology and results in the attacker gaining unauthorized access to devices.
- Backdoor. This attack makes it possible for an attacker to gain remote access to the vulnerable IoT device.

Other common attacks include eavesdropping, man-in-the-middle attacks, forged malicious devices, side-channel attacks, and ransomware attacks.

When multiple components are working alongside one another as part of an IoT infrastructure, if one is vulnerable it may impact and affect another device or component. For example, if the router is tampered with, then this will affect the IoT hub. This is **cross-contamination**.

The attack map

An attack map for smart homes could be designed and sorted in a variety of ways. For example, it could be designed by device, by layer of IoT infrastructure, by type of vulnerability, by impact, and so on. Our attack map is organised via stages similar to that of the 'Cyber Kill Chain' and 'MITRE ATT&CK' frameworks. Table 1 gives a comparison of the stages a penetration tester or attacker might use.

If the attack map was developed with all these stages, technologies, and vulnerabilities within a smart home, the attack map would be extremely vast. Additionally, the threat landscape is ever-evolving with new technologies being introduced and adapted which would mean that the attack map would become obsolete sooner rather than later. With this in mind, our attack map has purposefully been designed to simplify the stages of an attack into the following:

Table 1: Cyber Kill Chain/MITRE ATT&CK Stage Comparison

Cyber Kill Chain	MITRE ATT&CK
Reconnaissance	Initial Access
Intrusion	Execution
Exploitation	Persistence
Privilege Escalation	Privilege Escalation
Lateral Movement	Defense Evasion
Obfuscation/Anti-forensics	Credential Access
Denial of Service	Discovery
Exfiltration	Lateral Movement
	Collection
	Exfiltration
	Command and Control

1. **Reconnaissance/Initial Access.** This is how an attacker identifies a bug and establishes initial access. For example, wardriving allows them to identify a smart home network that has a vulnerable Chromecast.

2. **Execution/Exploitation.** These are the attacks that are carried out. They can be categorized under headings such as credential access, whereby a man-in-the-middle attack might be used.

3. **Cross-Contamination.** This is how an attacker uses one compromised device to impact or attack another device, for example, using a Chromecast to voice control an Alexa to unlock the front door, or perhaps as part of a DDoS attack where a device may be hijacked and become a bot within a botnet, remotely controlled and commanded to carry out attacks.

4. **Privilege Escalation.** This is how an attacker can escalate their privileges to become a user with more control and access rights.

5. **Persistence.** This is how an attacker ensures that remote access and control is persistent and sustained.

Table 2: Connection Justification Sample

Connector Label No.	Connection	Justification
1	Social engineering to searching of technical databases	Any social engineering activity may lead to the discovery of device information, such as device name, model, and version. This can give the attacker information which can be queried in a technical database to search for vulnerabilities and exploits. Thus, allowing them to target the victim.
4	Various forms of social engineering attacks connect to information disclosure.	All types of different social engineering techniques may lead to the victim disclosing confidential information to the attacker. Details such as usernames, passwords, emails, PINs and PII, etc. may be disclosed. This information could be used in further attacks to overcome 2FA and multi-factor authentication, as well as access to other services and applications.
14	Social engineering techniques to downloading of malware onto victim machine	A variety of social engineering techniques may be employed by an attacker to get the victim to download malware onto their system. It may be a link an email, an attachment, “technical support” instructions over the phone, by email, by letter, by text, or another tactic.

Stages 1 and 2 are combined into the first map, whereas stages 3 to 5 are combined into the second.

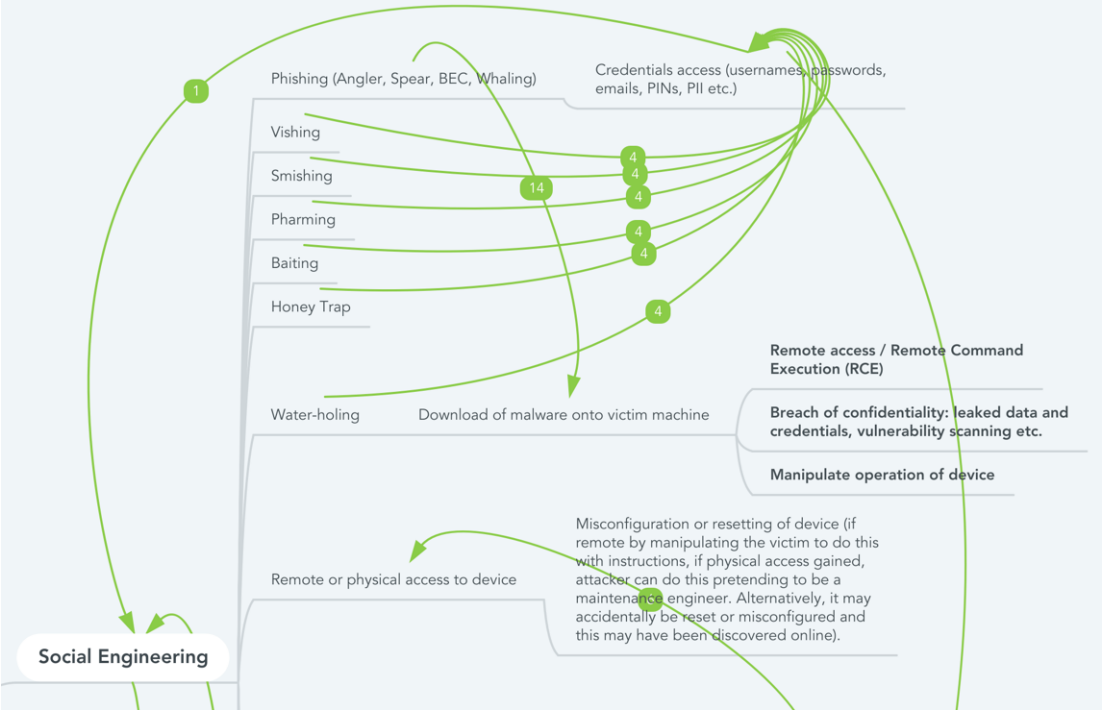

Figure 1: Reconnaissance/Initial Access – Social Engineering Subsection

The attack maps are stored in a variety of formats on the Github repository at: `https://github.com/uKUp9mxQSJ/IoTAttackMap`. The file 'TheIoTAttackMap.pdf' includes connection justification tables which include descriptions of how one technique may lead to another phase, attack technique, or tool. This model differs from other frameworks as it not only examines the different phases of an attack, but it describes how an attacker thinks and may laterally move across a network launching subsequent attacks.

How to use the attack maps

- **Step 1:** Decide what stage of the attack is to be evaluated. If an IoT or network device has been compromised view the second map, and if not, view the first.
- **Step 2:** Examine a specific method and evaluate the risk associated with it.

  As an example, Figure 1 shows a subset of social engineering techniques such as phishing, vishing, and smishing. Examining the numbers on each connection gives further information.

  From Figure 1 and Table 2 we can see the many paths an attacker can use to get to the result of '**Remote access/Remote Command Execution**'. For example, an attacker could use smishing to get credential access (an email address), which they use in a subsequent social engineering attack. They perform a phishing attack on the obtained email address which downloads malware onto the victim's machine. This malware could lead to a variety of further attacks such as remote access, ransomware, spyware and botnet.
- **Step 3:** Examine the Cross-Contamination Map. Identify which device has been compromised, then examine what impact this might have by following the connectors and viewing the connection justification table as in Step 2.

Each phase of the attack should be carefully examined to assess the risk of a realised threat on a given network environment.

Conclusion

The attack surface of most home networks is extremely vast and as such, there is always a risk of attack. The risk may not be eliminated entirely but instead, mitigated, through:

- **Risk avoidance.** Turn off features within IoT devices that are not needed. For example, turn off the microphone that is listening all the time The smart device may even be completely removed.
- **Risk acceptance.** Acceptance of the risk, and the impact it may have on assets and any organisation or individual connected to the victim. If the risk is accepted, backup plans should be in place to mitigate risk.
- **Risk limitation.** Reduce the risk by implementing security controls such as a firewall, intelligent email filters, or malware scanning and removal software.
- **Risk transference.** Pass the responsibility of the risk onto a third party.

The most important thing is to stop that initial attack from being successful. This prevents any lateral movement or further attacks from being launched on the network. It is of vital importance to identify and address any entry points that an attacker may use to gain an initial foothold.

Biographies

William Bathgate received his MSc in Information Security at Royal Holloway, University of London in 2021. He is at present working as a secondary school teacher of Computer Science in Surrey and freelance penetration tester and security consultant. Prior to this, he worked as a security consultant for Deloitte, Dublin.

Salaheddin Darwish works as a lecturer and a senior cyber security analyst at Royal Holloway, University of London. His research interests are privacy and security in distributed systems such as MANETs, the Internet of Things (IoT) especially in the healthcare domain, and Blockchain. He was involved with some research projects that addressed IoT and software security at Royal Holloway and University of Surrey. He received his Master and PhD at Brunel University London.

Series editor: S.- L. Ng