Effect Mitigation of IoT Attacks in Future Internet Architectures

Benjamin Rothenberger, Adrian Perrig

June 23, 2017

1 Introduction

In the era of *Internet of Things (IoT)* and *"smart" home*, there is an on-going trend to connect devices to the Internet. We are continuing to proliferate our homes, cars and even businesses with Internet-connected devices. Smart thermostats are used to automatically adjust temperature settings depending on the time of the day and presence of people in the apartment. Smart fire and burglar alarms address safety issues through sensors and alerts. We even wear smart devices. Computer-enabled medical devices and healthcare, fitness trackers and ultimately our smart phones become an indispensable part in our daily life.

While these smart devices enable convenience and safety benefits, they also create security and privacy risks. IoT devices are often targeted by malware to turn them into remotely controlled "bots", that can be used as part of a botnet in large-scale network attacks. Recent attacks have shown how a botnet consisting of millions of IoT devices can perform distributed denial of service (DDoS) attacks to effectively disrupt the Internet [3]. Further, an Austrian hotel lost the ability to create new room keys due to a ransomware attack [5]. And regarding privacy, there have been numerous incidents where the live feeds from consumers' smart cameras have been available on the Internet [1].

In this recent disruption attack, the botnet called *Mirai*, made up of devices like routers and web-cams, was sending massive numbers of requests to a domain name service provider (Dyn). Mirai scans the Internet for vulnerable devices and infects them by exploiting a vulnerability or using a common username/password combination. The infected devices themselves start scanning for other vulnerable devices. Generally, the devices remain fully functional, except having an increased use of bandwidth. This attack affected customers of the DNS provider and knocked off parts of Twitter's network, as well as hundreds of other sites.

2 Problem Characterization

Security is an arms race between attackers and defenders. With the downside that attacking a system is easier than defending it due to the complexity of systems. The more complex a system is, the larger is its attack surface. Consider that a defender has to uphold attacks against the entire attack surface, while an attacker has to find a single vulnerability. Further, when considering the security of a network, we have to be concerned about the "best" attacker possible, because he will build an attack tool and the discovered techniques will be adapted to other malware projects.

Security of current devices mostly relies on extensive testing and quick patching if a vulnerability has been found [4]. Unfortunately, this practice cannot be applied for embedded systems. They are often built by offshore third parties, which often don't even have the expertise to build secure devices, and sold at a lower margin than other devices. Thus, the budget is spent on features and usability, at the expense of security and reliability. After a vulnerability has been found, the consumer has no choice than to unplug the device or risk to get exploited.

Threats against IoT devices come in many different forms and with different purpose. Malicious entities try to launch attacks on privacy (extract personal information), blackmail people using ransomware that encrypts our data and demands payment for the unlock key (e.g., health data) or cause congestion on either network or host using a DDoS attack. Further, the sheer amount of data that IoT devices can generate is staggering and thus a valuable target for malicious entities.

The Internet of things is a highly complex systems with millions of different devices. This complexity leads to more parts, more interactions, and possibly more mistakes in the design and development process. But, even though more people become aware of the danger from attacks via IoT devices, budgets and resources are not growing as quickly and the problem seems *unsolvable* in the short term. It is so momentous, that the Federal Trade Commission (FTC) announced a competition that challenges the public to create a technical solution to guard against security vulnerabilities in IoT devices [2]. The

solution could be anything from a physical device added to the consumer's network to an app providing information about specific devices. However, this technical solution will not lead to a secure IoT, because it will not change the solve the fundamental problems behind building secure devices. IoT devices will still be exposed to the open Internet, remain outdated, or can be accessed using the factory-default password.

3 Defense Mechanisms

The Internet is an open space, where everyone can connect to and possibly interact with other entities. Due to its heterogeneity solutions that lead to a secure IoT seem evasive, but we need to arrive at an *actionable* solution in the mid-term. Otherwise IoT-fueled attacks will remain a problem. As the threats posed by IoT devices become greater and more catastrophic, regulation will be inevitable. For the Internet, where its permissionless nature is the foundation for its influental innovation, this will be very difficult.

The most *important* observation is that even though we cannot prevent attacks from happening, the effects of attacks can be mitigated. Therefore, the intermediate goal for a secure IoT must be to prevent malicious devices to harm others, so that in the worst case only the user itself is harmed. This means that the network itself needs to prevent "collateral" damage towards other users and eliminate negative externalities of insecure devices.

To achieve this, SCION offers the following mechanisms that alleviate the impact of DDoS attacks:

- **Prevent network-based congestion (using SIBRA).** SIBRA offers differentiated inter-domain resource allocation for fine-grained control to individual flows. End hosts can use these allocations to obtain bandwidth guarantees that can be used to defend against network-based congestion. SIBRA achieves botnet-size independence which means that a legitimate flow's allocated bandwidth does not diminish below a guaranteed allocation when the number of bots increases.
- **Multipath communication.** Unlike in today's Internet, SCION allows entities to make use of multiple paths concurrently, requiring an adversary to simultaneously flood all upstream links of a victim. Thus, multipath communication is a powerful mechanism to enhance availability.
- **"Hidden" network paths.** In case a victim wants to continue make paths available but only to a subset of authorized senders, SCION allows to distribute non-registered and thus "hidden" paths in an out-of-band process. This prevents adversarial traffic if the adversary is not contained in this subset.
- **Source-AS authenticated request packets.** DoS attacks in today's Internet often use packet reflection to redirect large volumes of traffic to a specific entity and hide the origin of their attack. Using source authentication on AS-level, the origin of the request cannot be arbitrarily spoofed, but only within the egress AS. This relies on ASes as administrative domains and managing network traffic.

References

[1] Insecam. `https://www.insecam.org/`, 2017.

[2] IoT Home Inspector Challenge. `https://www.federalregister.gov/documents/2017/01/04/2016-31731/iot-home-inspector-challenge`, 2017.

[3] Sean Gallagher. Double-dip Internet-of-Things botnet attack felt across the Internet. `https://arstechnica.com/security/2016/10/double-dip-internet-of-things-botnet-attack-felt-across-the-internet/`, 2016.

[4] Bruce Schneier. Security and the Internet of Things. `https://www.schneier.com/crypto-gram/archives/2017/0215.html`, 2017.

[5] James Vincent. Don't believe the story about hackers locking guests in their rooms at a luxury hotel. `http://www.theverge.com/2017/1/30/14438226/hackers-austrian-hotel-bitcoin-ransom-ransomware`, 2017.