Bailey Metz

Csilla Farkas

CSCE 522

Milestone 1 Papers

1 October 2018

In the article “A Lightweight Vulnerability for Mitigation Framework for IoT devices”, the authors Noy Hadar, Shachar Siboni, and Yuval Elovici have proposed an interesting implementation method to protect IoT devices. This is very important because IoT devices are becoming more and more popular with both the general public as well as businesses and organizations. The issues with IoT vulnerability are mainly the threats of IoT malware because IoT devices are constrained and have weaker computing power than that of other regular day to day computers. Typically, they have nothing to execute software patches and updates. To absolve this, these engineers have attempted to describe a solution to IoT Network security other than CUJO since CUJO is targeted for remote deployments of IoT devices that are part of a smart home network or a company/organizational network. Their solution is a cloud-based framework running on an internet connected appliance that connects to the IoT device and focuses on known vulnerabilities instead of preventing intrusions that exploit the connection between devices within the network. These vulnerabilities are collected from public data sources of Common Vulnerabilities and Exposures (CVE). Their proposed framework targets vulnerable IP-connected devices that exploit their open CVEs.

I feel this framework does not cover all the bases of an attack on an IoT device. What would protect the IoT device if the cloud-based vulnerability mitigation service went down, was hacked or attacked, or failed to push a necessary update to the IoT devices? If any of these happened, EVERY device would be at risk of unauthorized access giving one person (or a group of people) virtually unlimited control over all these devices connected across the grid.

My suggestion would be to implement some form of individual, randomly-generated encryption over these devices to keep each individual IoT device’s connection to the cloud-based service unique.

In the article “Systematically Evaluating Security and Privacy for Consumer IoT Devices”, the authors Franco Loi, Arunan Sivanathan, Hassan Habibi Gharakheili, Adam Radford, and Vijay Sivaraman propose an effective implementation method for testing IoT device security. By targeting and fortifying many different aspects of IoT security (confidentiality, integrity, authentication, and availability), their method of research can be used to greatly decrease the possibility for IoT attacks on consumer devices as advancements in IoT technology are accomplished. This, however, does not come without its shortcomings. These engineers took a variety of devices and subjected them to rigorous forms of cyberattacks. They then made several charts and graphs to depict the results of each type of attack on each IoT device. The results were very eye-opening, but not entirely reassuring.

Many devices, specifically Phillips Hue lightbulbs, Belkin power switches, HP Envy printers, TP Link cameras, and Belkin motion sensors, communicated in plaintext and disclosed private information, for example, whether the Belkin power switch was on/off, or when the Phillips Hue lightbulb was last used. This clearly shows while some devices have moderate protection from some kinds of attacks, more IoT devices are highly susceptible to other attacks.

This article accurately describes thorough testing of IoT devices and shows that cyber security analysts have a long way to go when it comes to strengthening the security of IoT devices many of us already have and use in our homes and businesses. These testing implementation methods are an excellent starting point for discovering vulnerabilities in IoT systems. In addition to these methods of testing, I would also recommend testing areas of availability as well non-repudiation so that all bases of the fundamentals of computer security vulnerabilities will be evaluated.

From "Systematically Evaluating Security and Privacy for Consumer IoT Devices"

This page contains the graph depicting various IoT devices subjected to various cyberattacks and the results of those cyberattacks (as mentioned in the paper above).

The legend is as follows:

Green (A): Secure

Yellow (B): Moderately Secure/Insecure

Red (C): Insecure

Table 3: Security rating

	Confidentiality										Integrity and Authentication			Access Control							Reflection Attacks			
	Device to Server			Device to Application			Application to Server			All														
Devices	Plaintext	Protocol	Entropy	Plaintext	Protocol	Entropy	Plaintext	Protocol	Entropy	Privacy	Replay Attack	DNS Spoofing	Fake Server	Open Ports (TCP)	Open Ports (UDP)	Vulnerable Ports	Weak Passwords	ICMP DoS	UDP DoS	No. of TCP Connections	ICMP Reflection	SSDP Reflection	SNMP Reflection	SNMP Public Community String
Phillip Hue lightbulb	A	A	A	C	C	C	A	A	A	C	C	C	C	C	C	C	A	B	C	C	C	C	A	A
Belkin Switch	B		A	C	C	C	A	A	A	C	C	C	A	C	C	A	A	C	C	C	C	C	A	A
Samsung Smart Cam	A		A	A	A	A	A	A	A	A	A	C	A	C	C	C	A	C	C	C	C	A	C	C
Belkin Smart Cam	A		A	A	A	A	A	A	A	A	A	C	A	C	C	C	A	C	B	C	C	C	A	A
Awair air monitor	A	A	A	A	A	A	A	A	A	A	A	C	A	B	B	A	A	C	C	A	C	A	A	A
HP Envy Printer	A	A	A	C	C	C	A	A	A	C	C	C	A	C	C	C	A	A	A	C	C	A	C	A
LiFX lightbulb	A	A	A	A		C	A	A	A	A	C	C	C	A	B	A	A	C	B	A	A	A	A	A
Canary Camera	A	A	A	A	A	A	A	A	A	A	A	C	A	A	A	A	A	C	A	A	C	A	A	A
TPLink Switch	A		A	A		C	A	A	A	A	C	C	A	C	C	C	A	C	C	C	C	A	A	A
Amazon Echo	A	A	A	A	A	A	A	A	A	A	A	C	A	C	C	A	A	B	C	C	C	A	A	A
Samsung Smart Things	A	A	A	A	A	A	A	A	A	A	A	C	A	C	B	C	A	C	C	C	C	A	A	A
Pixstar Photo Frame	A	A	A	A	A	A	A	A	A	A	A	C	A	A	C	A	A			A	C	A	A	A
TPLink Camera	A		A	C	C	A	A	A	A	C	A	C	A	C	C	C	C	C	B	C	C	A	A	A
Belkin Motion Sensor	A	A	A	C	C	C	A	A	A	C	A			C	C	A	A	C	B	C	C	C	A	A
Nest Smoke Alarm	A		A	A	A	A	A	A	A	A	A	C	A	B	C	A	A			A	C	A	A	A
Netamo Camera	A	A	A	B	C	A	A	A	A	A	A	C	A	C	C	C	A	C	B	C	C	A	A	A
Dlink Camera	C	C	C	A	A	A	A	A	A	A	A			C	C	C	C	C	B	C	C	C	A	A
Hello Barbie Companion	A	A	A	A	A	A	A	A	A	A	A	C	A	A	A	A	A	C	A	A	C	A	A	A
Whithings Sleep Monitor	A		A	A	A	A	A	A	A	A	A	C	A	C	C	C	A			C	C	A	A	A
Nest Drop Camera	A	A	A	A	A	A	A	A	A	A	A	C	A	A	B	A	A	C	A	A	C	A	A	A

In the article “IoT Security Challenges and Ways Forward”, the author Marcel Medwed discusses the fundamentals of the IoT computing industry as it begins impacting the world and how the world should consider preparing for this new wave in the industry of technology.

Currently, 40% of the world’s population is considered actively online. By 2020, at least 40 billion more “smart” devices will be launched into our society. These devices will impact our known society in monumental ways, contributing to some of the greatest breakthroughs of mankind. At the same time, however, these devices are at great risk of cyberattack since IoT is just beginning to emerge. Exploits of these devices are being steadily recorded and the estimated costs of cyberattacks on these devices will be 2 trillion dollars by 2020.

Sadly, security risk awareness is not present in today’s consumer and developer mindset. Once these risks become a focal point in our society, the next step is determining who is going to fund the research of the security protocols and the maintenance of said protocols once they are put into place.

Beyond conceptualizing the ideas of secure resolutions, the author states we also need to establish a baseline infrastructure that will provide secure software guidelines for all IoT devices. Furthermore, the debate between whether the answer to secure IoT devices lies within the aspect of hardware or software will need to be assessed. As it stands, an IoT device is readily susceptible to tampering or software security failures which poses great risk of cyberattack.

In conclusion, I highly support further research of IoT security before IoT devices become even more standardized in our society today. To increase security, I suggest research into the encryption of data traffic between IoT devices and their various connections to the Internet.

In the article “Big IoT Data Stream Analytics with Issues in Privacy and Security”, the author Latifur Khan describes the need for IoT data analysis and how to effectively research it while maintaining confidentiality and data integrity.

Because IoT devices are constantly monitoring systems that collect, process, and transmit data using the internet, the output of data generated by these devices will continue to grow exponentially. The result of this is a need for large scale processing systems that can evaluate and extract necessary information to continue IoT advancements in functionality and improve quality of life. This poses risk however, since a vast majority of the data that will be analyzed is highly private and confidential.

Dr. Khan recommends the development of secure and scalable architecture that can proficiently complete big data analytics, while providing a cryptographically secure mechanism for preserving data privacy and security. Using his experience in addressing privacy issues on Intel SGX, which is a cryptographically secure hardware device that provides confidentiality and data integrity, he and a team of others intend to employ the premise behind it to design a framework that will address data security concerns from IoT devices.

Intel SFX is a set of instructions that allow developers to securely compute within an execution environment because cryptographically secure keys encrypt and decrypt data depending on its location within or outside the execution environment. A poor implementation of the data analytics within this secure environment, however, is known to be subject to side-channel attacks. Therefore, it is the responsibility of the developer to preserve data privacy.

This is where the problem with this implementation method arises. I recommend researching a secure method that could automate the implementation method of the data analytics to preserve data integrity and thus absolving the possibility of human error.

My top 3 areas of interest in IoT security are:

- Privacy for Smart Devices
- Threat Models and Attack Strategies in IoT
- Usable Security of IoT