Survey on the Insecurity of the Internet of Things

Elizabeth LaGreca
Department of Computer Science
Hampton University
elizabeth.lagreca@my.hamptonu.edu

Chutima Boonthum-Denecke
Department of Computer Science
Hampton University
chutima.boonthum@hamptonu.edu

ABSTRACT

Even the most casual observers of the latest cyber security threats are aware of how susceptible internet-connected devices such as cameras, home monitoring systems and cable boxes are to being taken over by an attacker. This paper surveys the weak (and often times non-existent) security measures deployed within devices in one of the fast growing sectors of information technology – the Internet of Things (IoT). It exemplifies these flaws using independent research as well as the 2016 Mirai attacks. It then proposes the institution of government regulations within the IoT sphere in order to ensure that manufactures' of IoT devices do not continue to produce and sell devices that are inherently insecure.

CCS CONCEPTS

• **Security and privacy** → **Systems security** → Distributed systems security; Vulnerability management • **Security and privacy** → **Software and application security** → Domain-specific security and privacy architectures

KEYWORDS

Internet of Things, Telnet, Universal Plug and Play, Mirai

ACM Reference format:
E. LaGreca, C. Boonthum-Denecke. 2017. Survey on the Insecurity of the Internet of Things. In *Proceedings of 2017 ADMI Symposium*, Virginia Beach, Virginia USA, March 23-26, 2017.

1 INTRODUCTION

As technology has advanced, so has our ability to take any electrically-powered object and connect it to the Internet. This connection between physical objects with sensors, actuators, and controllers and the Internet is referred to as the **Internet of Things (IoT)**. The IoT has the capability to be transformative across all sectors, changing the ways in which we live and work. The application of IoT has numerous benefits including:

- Smart cities – financial savings realized through improved operational efficiency and city management, environmental sustainability and infrastructure resilience [1]
- Smart homes – increased energy efficiency, home automation and security
- Smart manufacturing and business – improved inventory management, customer and business metrics, reduced cost in production, energy and equipment maintenance

However, along with all of the promise and innovation that can be realized through IoT integration, come significant security concerns. It is estimated that 8.4 billion IoT devices will be in use in 2017 [2]. Most of these devices will be connected online all of the time and many are built with few or no security measures implemented. This represents a serious threat to life and property and must be addressed [3].

Figure 1: Graphical representation of the IoT.

The inherent insecurity of IoT devices was dramatically exposed by the malware Mirai in late 2016. Mirai contained code that resulted in hundreds of thousands of IoT devices becoming part of a botnet that performed several high profile distributed denial of service (DDoS) attacks.

While the result of the 2016 Mirai attacks was primarily inconvenience, they illustrated the catastrophic risks created by the proliferation of billions of insecure devices [3]. The source code for Mirai has been publicly released and is used within this paper, which also contains additional independent research to expose how the deficiencies of IoT devices have created one of the greatest threats to cyber security today.

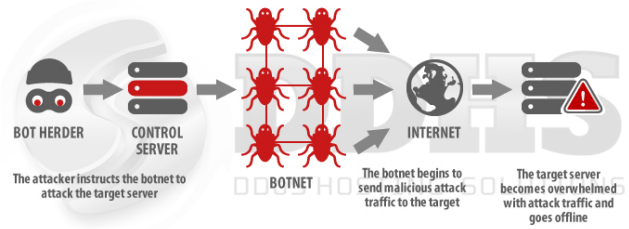

BOT HERDER
CONTROL SERVER
The attacker instructs the botnet to attack the target server
BOTNET
INTERNET
The botnet begins to send malicious attack traffic to the target
The target server becomes overwhelmed with attack traffic and goes offline

Figure 2: Creation of a botnet to perform DDoS attacks.

2 EXPERIMENTAL AND COMPUTATIONAL DETAILS

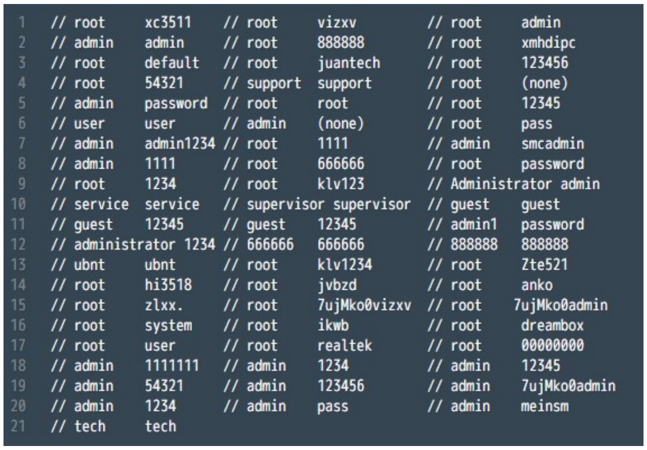
2.1 Characteristics of a Flawed IoT device

2.1.1 Weak Authentication Mechanisms. Authentication is used between an IoT device and an application or server to verify their identities when they interact. IoT devices have two main flaws in this area – the use of default passwords and the lack of a mechanism to assure that when a device is connecting to a server or to an application, it is one to which the device should be connecting.

The first flaw concerns the use of default passwords on devices. Authentication is typically performed on IoT devices using a username and password combination. Usernames and passwords are set by the manufactures of the devices at the factory. After a customer purchases the device, there is often no requirement to change the default for the entire life of the device. Some devices do not even allow the default to be changed, as the username and password are hard-coded into the firmware of the device. The Mirai malware took advantage of the use of unchanged default usernames and passwords. Fig. 3 displays the default usernames and passwords used within Mirai for a variety of IoT devices.

Researchers have demonstrated a second major flaw in the authentication mechanism - a device not knowing with 100% certainty to what it is connecting. In one experiment, a wireless router was placed on a network that had the same SSID (network name) as one an IoT device had previously connected [5]. Simply because the router had the same service set identifier (SSID), it automatically connected to the rogue access point with no password required.

2.1.2 Unencrypted Data Transfer. Nineteen percent of IoT devices do not encrypt the data exchanged between the device and its application or server [6]. Therefore, based on the Gartner, Inc. forecast of 8.4 billion IoT devices in use in 2017, roughly 1.6 billion of devices will be using unencrypted data transfers [2]. Unencrypted data transfer is a great risk to privacy as it allows man-in-the-middle attacks that can intercept data such as login credentials and personal information.



```
// root     xc3511   // root     vizxv       // root     admin
// admin    admin    // root     888888      // root     xmhdipc
// root     default  // root     juantech    // root     123456
// root     54321    // support  support     // root     (none)
// admin    password // root     root        // root     12345
// user     user     // admin    (none)      // root     pass
// admin    admin1234 // root    1111        // admin    smcadmin
// admin    1111     // root     666666      // root     password
// root     1234     // root     klv123      // Administrator admin
// service  service  // supervisor supervisor // guest   guest
// guest    12345    // guest    12345       // admin1   password
// administrator 1234 // 666666  666666      // 888888   888888
// ubnt     ubnt     // root     klv1234     // root     Zte521
// root     hi3518   // root     jvbzd       // root     anko
// root     zlxx.    // root     7ujMko0vizxv // root   7ujMko0admin
// root     system   // root     ikwb        // root     dreambox
// root     user     // root     realtek     // root     00000000
// admin    1111111  // admin    1234        // admin    12345
// admin    54321    // admin    123456      // admin    7ujMko0admin
// admin    1234     // admin    pass        // admin    meinsm
// tech     tech
```

Figure 3: Default usernames and passwords used in Mirai attack [4].

2.1.3 Insecure Protocol Use. Many IoT devices use Telnet and Universal Plug and Play (UPnP) networking protocols. These protocols that allow interaction between devices and an application or server.

Introduced in 1969, Telnet was created to allow remote administration of equipment. A 2014 study found that 70% of IoT devices still used Telnet [7]. Insecurities of Telnet include susceptibility to denial of service (DDoS) attacks and lack of brute force protection. Mirai took advantage of this lack of brute force protection to cycle through default usernames and passwords in order to gain access to IoT devices.

Universal Plug and Play (UPnP) is another networking protocol used in IoT devices. Like Telnet, it allows communication between devices and other applications or servers. Enabled by default on many Internet-connected devices, during installation a port is opened up on the user’s Internet router. This open port can then be exploited by attackers looking to gain access to the internal network [8].

2.1.4 Embedded Firmware. Firmware is software embedded within hardware, including IoT devices. Like an operating system or software installed on a computer or phone, firmware must be regularly updated to protect the devices against known vulnerabilities and likelihood of attack. However, many IoT devices do not have the extra processing power needed to support a specialized upgrade process, others simply do not have the capability [9]. Accordingly, many IoT devices will run the same version of software installed at the factory throughout their lifespan.

2.2 Implement Regulations

Vulnerabilities within the IoT have been disclosed by researchers, reporters, hackers and attackers. Nonetheless, many companies continue to sell quick-to-market, cheap-to-manufacturer, no-emphasis-on-security devices. While government agencies such as the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) have released guidance concerning security for IoT devices, as of now, there are no minimum technical standards that manufacturers are required to meet before releasing their product to market [10]. Due to this lack of self-policing and to help diminish the rapidly growing security threat, I am recommending instituting government regulation within the IoT sphere. The initial focus of this regulation should include:

- Ensuring manufacturers take a security-by-design approach throughout the development process, including the use of secure protocols for connection, data encryption, providing a method for patch management and no longer using default passwords
- Recalling devices that do not meet security thresholds
- Providing incentives for companies to replace devices already in homes or businesses

3 RESULTS AND DISCUSSION

Through our evaluation, we have identified inherent insecurities within IoT devices. Table 1 identifies proposed technical solutions to each risk.

Table 1: Improvements that can be made within the IoT sphere as a result of regulation.

Current Insecure Method	Proposed Secure Method
Use of Telnet	Implement Secure Shell (SSH)
Use of Universal Plug and Play (UPnP)	Disable all use of UPnP
Use of default passwords	All devices should enforce mandatory password changes
Inability to upgrade firmware	Build devices that are able to be updated, including over-the-air updates
Unencrypted data transfer	Use a combination of Transportation Layer Security (TLS) and AES Encryption for full end-to-end encryption
Lack of proper authentication between devices	Use of a token-based access control that authorizes device access and manages which devices can speak and listen on the network based on the tokens the network distributes [11].

Our survey has identified and described several fundamental security defects in millions of IoT devices currently in use. It has also proposed secure methods that can be used in place of each. Since we have identified a model for a secure device, we can now focus on the IoT ecosystem as a whole. Future research will focus on the potential for vastly enhanced IoT device security through use of a decentralized Blockchain approach (the technology use for Bitcoin security) in place of the current traditional server/client model.

4 CONCLUSIONS

The Internet of Things has the promise to transform our cities, homes, manufacturing and business. However, we will never realize these benefits if security is not implemented during the development process. Current security flaws in weak authentication mechanisms, unencrypted data transfer, insecure protocol use and embedded firmware that cannot be upgraded are all issues that must be addressed, and addressed now. There is little evidence that manufactures’ of IoT devices are willing to expend the cost and time it would take to properly implement security. For that reason, government regulations are needed within the industry to guide the IoT into a more secure future.

Acknowledgement

This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program under grant no. DGE-1303409 (PI/co-PI: Dr. Chutima Boonthum-Denecke, Dr. Jean Muhammad).

REFERENCES

[1] Andrew Meola. 2016. How smart cities & IoT will change our communities. (December 2016). Retrieved February 8, 2017 from http://www.businessinsider.com/internet-of-things-smart-cities-2016-10

[2] Anon. 2017. Gartner Says 8.4 Billion Connected Will Be in Use in 2017, Up 31 Percent From 2016. (February 2017). Retrieved February 8, 2017 from http://www.gartner.com/newsroom/id/3598917

[3] Mike Orcutt. 2016. Security Experts Warn Congress That the Internet of Things Could Kill People. (December 2016). Retrieved February 8, 2017 from https://www.technologyreview.com/s/603015/security-experts-warn-congress-that-the-internet-of-things-could-kill-people/

[4] Jgamblin. 2016. jgamblin/Mirai-Source-Code. (October 2016). Retrieved February 8, 2017 from https://github.com/jgamblin/Mirai-Source-Code/blob/6a5941be681b839eeff8ece1de8b245bcd5ffb02/mirai/bot/scanner.c

[5] Eric Lai. 2016. BlackBerry Security Summit 2016 Recap: Customer Wins, Giuliani Keynote, Hacking via Tea Kettle, & More [Video, Pics]. (July 2016). Retrieved February 8, 2017 from http://blogs.blackberry.com/2016/07/blackberry-security-summit-2016-recap-customer-wins-giuliani-keynote-hacking-by-coffee-pots-and-more-video-pics.

[6] Mario Ballano Barcena and Candid Wueest. 2015. *Insecurity in the Internet of Things*, Symantec.

[7] Anon. 2014. HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. (July 2014). Retrieved February 8, 2017 from http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WJssaxCPjlQ

[8] Anon. 2016. Alert (TA16-288A). (November 2016). Retrieved February 8, 2017 from https://www.us-cert.gov/ncas/alerts/TA16-288A

[9] Alan Grau. Security Requirements for Embedded Devices – What is Really Needed? Retrieved February 8, 2017 from http://www.iconlabs.com/prod/security-requirements-embedded-devices-%E2%80%93-what-really-needed

[10] Matt Hamblen. 2016. After DDOS attack, senator seeks industry-led security standards for IoT devices. (October 2016). Retrieved February 8, 2017 from http://www.computerworld.com/article/3136650/security/after-ddos-attack-senator-seeks-industry-led-security-standards-for-iot-devices.html

[11] Anon. *A New Approach to IoT Security*, PubNub