International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

CURRENT THREATS IN SMART SYSTEMS

Tushar Patel
B.Sc. MPCS, Bhavan's Vivekananda College of Science, Humanities & Commerce,
Sainikpuri, Secunderabad - 500 094, India

Abstract: **Internet of things is no doubt making our lives easier, the question that the majority overlooks is how secure is this next-generation innovation. The objective of this paper is to make a comprehensive analysis on the current threats and countermeasures to the very real-world threat to the security of smart devices. We have used a methodology that is based on declassified intelligence reports and security audits conducted by cyber security auditing bodies. The major threats to the ever-expanding internet of things are ransomware, weak encryption protocols and hidden backdoors meant for the intelligence community falling into the wrong hands. The lack of awareness of these security threats compounds it further. The key countermeasures would be the reduction of resource intensiveness of security protocols, firewalls for embedded systems and stable, comprehensive security patches. Additionally, we will delve in the future of cyber security and automation technology.**

Keywords: **Cyber security; Backdoors; Embedded systems; Intelligence; Ransomware;**

I. INTRODUCTION

Internet of things (IoT) is the Interlinking of hardware devices to the web. The concept of IoT was envisioned in 1982, the term "Internet of things" was only coined in 1999 by Kevin Aston during his work on RFID (Radio frequency identification) at Auto-ID Labs.

In layman's terms, IoT is defined as everyday objects with computing devices embedded in them that have the ability to transfer data over the internet. This is one of the primary focus of today's world, where computerization is a necessity and no longer a luxury.

Security on internet-connected devices hasn't evolved enough to meet the expected demand of20.4 billion IoT devices globally by 2020 [1]. Gadget designers tend to make IoT devices as simple as possible, which can often mean sacrificing security.

The purpose of this study is to give a concise roundup on the threats and countermeasures of these security issues. The methodology used was the collection of data and statistics from various sources and analyzing their relevance to our current situation.

II. CHALLENGES

The following are what we consider major security concerns and the possible countermeasures that are being examined by various organizations and security professionals:

1. Inadequate Hardware Specifications

The biggest challenge to IoT devices is posed due to their weak hardware. To make the manufacture of these devices economical the companies have to cut costs in terms of hardware, as the smart features of these devices are not as significant as the primary functions of these devices. In most cases, internet connectivity is considered an add-on feature of these devices. Hence not much concern is put into the security and computing power. The inability of conventional security measures to run on such low-end hardware has significantly increased the susceptibility to attack. This is because the manufacturers have little choice but to make devices with little or no security measures in place.

The NSA has come up with a very ingenious defense in terms of very lightweight cryptographic algorithms. They are very efficient requiring very little power and computational space. This allows devices that were too weak to run conventional encryption to be able to encrypt their data. The NSA officially released these two encryption algorithms to the public by the names 'Simon' and 'speck' in the summer of 2013 [2]. Since then these algorithms have drawn the attention of IoT chip manufacturers as a cost-effective deterrent against cyber threats.

Floodgate is a firewall product designed by Icon Labs to meet the specific requirements of embedded applications [3]. It provides static filtering, threshold-based filtering, and Stateful Packet Inspection to protect embedded devices from Internet-based threats. Floodgate has a small footprint, low CPU processing impact, and is easily integrated with any embedded IP stack.

2. Exploitation of Backdoors

Backdoors are access points that are built into most devices for remote maintenance of product software. These are also used for monitoring of data for reasons that pertain to national or international security. However, these backdoors can be exploited by unauthorized parties for malicious purposes. Using back doors, one can gain remote access to the insecure system or network. Thus, enabling them to gain sensitive information and violating the privacy of the user.

AEGIS is a Lightweight Firewall for Wireless Sensor Networks [4]. This uses IPV6 and 6LoWPAN that are ideal for embedded systems. AEGIS is based on a simple yet rich rule-based language. It is highly efficient in operation and is easy to maintain. With the help of this robust and effective firewall, there is a possibility that IoT devices will become more secure in the near future.

3. Software Updates

IoT devices just like any other devices are generally riddled with errors, which cannot be detected until real world usage on a massive scale is performed. These errors may be loopholes in security or errors that impede the general operation of these devices. IoT devices due to their low storage capacities and processing power are unable to process significant updates to their code. Moreover, the lines through which these updates are deployed are not encrypted. Hence, the update can be intercepted and tampered with.

One of the Major problems with many IoT devices is that they are not patchable. Hence, new vulnerabilities cannot be made secure. The IoT is growing on a path that is quickly leading to the pervasive deployment of unmonitored devices throughout our surroundings. Ensuring that these devices are capable of being updated would be a first step as manufacturers neglect security, and do not consider security patches as a necessity. Moreover, the IoT devices should be capable of verifying the integrity of the security patches before they are applied. This is done in Computers and other devices that have more processing power with the help of hashes and checksums. The innovation of newer integrity checking methods that can run on lower end hardware would greatly boost the safety of the updates that are being installed.

4. Hardware Vulnerabilities

These are the vulnerabilities that creep into the defenses of the IoT; they are problems that can't be solved by applying a patch. This is due to the fundamental architecture of the embedded device that gives away information on the operating protocols of these embedded systems. Designs need to ensure that overbuilding or cloning of the design is not possible. This can be seen in differential power analysis (DPA) attacks can extract keys and vital device information. The bootup process of the system has to be secured not only from

network-based attacks but also in a scenario where the attacker has physical access to the device.

If the hardware can be physically reached due to insufficient protection, it is possible to obtain sensitive data directly from an external programmable read-only memory (PROM) or external RAM chip, or by probing the connecting bus. It is safe and relatively easy, to encrypt all static data for example firmware stored the ROM. The absence of memory encryption in a smart electric meter design was the biggest that led to an estimated $400 million annual loss by a power company.

5. Miscellaneous Vulnerabilities:

The original device manufacturers (ODMs) who often don't get their brand name on the finished product. Hence, they do not have the incentive to improve security further. The brand-name company on the box may add a user interface, and maybe some new features which makes sure everything works, and that is the end of the manufacturing process.

The problem with this method is that no single entity has any incentive, expertise, or even ability to patch the software once it is shipped. The chip manufacturer is busy shipping the next version of the chip. The maintenance of the older chips and products is not a priority.

This loophole in the process of manufacturing of a product is a problem that will be difficult to address as it has arisen due to the way of doing business rather than a device insecurity. The only practical way to resolve this issue would be the introduction of strict manufacturing standards by governing bodies.

Around 60 percent of Internet of Things device manufacturers do not properly tell customers how their private information is being used [5]. A recent study by 25 data protection regulators around the world studied devices like electricity meters, Internet-connected thermostats, and watches that monitor health. This study of how well companies communicate privacy matters to their customers highlighted the following facts:

i. Only 41 percent companies completely told users how their private information was collected, used and disclosed.
ii. The number of companies that informed customers how they could delete their information off the device was 72 percent.
iii. The companies that provided easily identifiable contact details if customers had privacy concerns was only 62 percent.
iv. Only 68 percent companies informed users how their data is stored.

This can be countered by endorsing and consuming products from manufacturers that are transparent about matters concerning data storage, usage, and sharing.

III. CONCLUSION

The main inference that we draw from this study is that there are ample solutions for most of the problems pertaining to IoT devices. IoT is growing at an astounding rate, but this growth is without proper emphasis on security. The liability falls on manufacturers who have an ethical responsibility to ensure that their clients are safe from exploitation. If the manufacturing companies fail to do so, it should be solved by putting in place more stringent regulatory norms by the government. However, the biggest means to solve this ever-intensifying problem would be to ensure awareness of the general public about the security concerns that they might face, thus making them better equipped to keep themselves safe in this digital universe.

IV. ACKNOWLEDGEMENT

I would like to thank Mr.Sagar Jinde for his help in critical reading of the manuscript, and Mrs KVB Saraswathi and Mr. G Mahesh Kumar for critical comments and encouragement.

V. BIBLIOGRAPHY

[1]. Hassan NA, Hijazi R. *"What's Next?."* InDigital Privacy and Security Using Windows 2017 (pp. 273-278). Apress.

[2]. Beaulieu R, Treatman-Clark S, Shors D, Weeks B, Smith J, Wingers L. "The SIMON and SPECK lightweight block ciphers." InDesign Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE 2015 Jun 8 (pp. 1-6).

[3]. Grau A. "Can you trust your fridge?." IEEE Spectrum. 2015 Mar;52(3):50-6.

[4]. Hossain M, Raghunathan V. "Aegis: A lightweight firewall for wireless sensor networks." Distributed Computing in Sensor Systems. 2010:258-72.

[5]. *"Privacy regulators study finds Internet of Things shortfalls"* [Internet]. ICO (Information Commissioner's Office). 2076 [cited 2017Aug5]. Available from: http://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/privacy-regulators-study-finds-internet-of-things-shortfalls.