ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 3, 1211-1217 (2017)

www.astesj.com

Special Issue on Recent Advances in Engineering Systems

ASTESJ

ISSN: 2415-6698

IoT: Their Conveniences, Security Challenges and Possible Solutions

Davar Pishva*

Ritsumeikan Asia Pacific University, Faculty of Asia Pacific Studies, 874-8577, Japan

ARTICLE INFO

Article history:
Received: 16 May, 2017
Accepted: 17 July, 2017
Online: 21 July, 2017

Keywords:
Internet of Things
IoT
Collaborative Internet of Things
C-IoT
Mirai IoT botnet
DDoS-for-hire
Thingbot
Security
Privacy
UHG

ABSTRACT

The build-in internet-controlled functions of smart devices such as smart phone, smart television, home healthcare gadget, etc., have made them quite attractive to many segments of consumers. In recent years mankind has witnessed an upsurge usage of such devices for numerous purposes. In this paper, the author is going to show how previously forecasted security challenges of these devices are becoming realities in the present day life. The paper initially provides some introductory information about the topic, mostly by means of survey and citations of previous work. It then highlights the devastating effects of October 21, 2016 DDoS attack which mainly utilized IoT devices. It emphasizes the danger of recently revealed Mirai IoT botnet which serves as the basis for the DDoS-for-hire 'booter'/ 'stresser' service. In terms of counter measures, after highlighting IoT security implementation challenges, numerous approaches are presented. As a long-term solution, an architecture wherein security issues are managed through universal home gateway by network operators in a product based fashion is emphasized. The author shows its technical feasibility and demonstrates its partial materialization in proprietary manners. It then explains why and how numerous stake holders are needed to get together for its wide range commercial implementation. Some immediate necessary safeguard actions and intermediate schemes which include soft infrastructures are also presented for the purpose of risk reduction.

1. Introduction

Advancement in technology has been changing our way of life and digital information has become a social infrastructure. Since the expansion of the Internet in 1990s, network infrastructure has become an indispensable part of social life and industrial activity for mankind.

We are now surrounded by Internet enabled smart devices and there are computer technologies in our cars, phones, watches, entertainment systems, and home appliances. The idea of making use of their existing electronics devices and connecting them to the Internet in conjunction with some specialized software have been leading mankind to a new era of technology known as the "Internet of Things" and commonly referred to as IoT. Their build-in internet-controlled function has made them quite attractive to many segments of consumers. Adoptions of cloud computing, mobile applications and virtualized enterprise architectures have led to a tremendous expansion of applications that are connected to internet resources [1].

Japanese audio visual equipment has been Internet enabled for over a decade now. This has enabled people to enjoy network based services, such as Video on Demand (VOD), Music on Demand (MOD), remote update, e-commerce, remote control, and other similar services. Samsung's 'Family Hub' fridge can order food, play films, and even let you see inside of it remotely [2]. Researchers around the world have come up with an abundance of resourceful ideas on how to effectively use microprocessors and the Internet in other everyday household appliances. According to a study conducted by International Data Corporation, 212 billion "things" will be installed based on IoT with an estimated market value of $8.9 trillion by 2020 [3]. Those "things" will be nothing special but daily used appliances ranging from watch, light bulb to smart television, refrigerator and so on.

Commercial advertising has also greatly benefitted from Internet services and online advertising can even be considered as the foundation of web economy. Unlike conventional forms of advertising, the system of online advertising even allows its target to receive something in return for viewing the advertisement [4]. In other words, our daily life, social activity, industrial and

*Corresponding Author: Davar Pishva, Address: APU, 1-1 Jumonjibaru, Beppu, Oita 874-8577 Japan, Tel: +81-977-78-1261, Email: dpishva@apu.ac.jp

business governance highly depend on information systems. In an industrialized country like Japan, most enterprises use information technology to establish their management governance and every enterprise has its own information for its business. 'IT governance' enables them to improve their efficiency and cost performance. The impacts of information systems on their operations are quite significant. It can be said that information assets have become valuable commodities for business and information systems are the key factors to ensure the growths of enterprises.

The Internet has created new markets around the globe by means of breaking physical barriers and connecting people and organizations of similar interests together. We are now progressing towards collaborative intelligence, something which will impact our connected life and business. The era of Collaborative Internet of Things (C-IoT) is approaching wherein improvement of life quality will have a direct impact on business efficiency enhancement. Furthermore, the process of sensors generating data, data producing knowledge and knowledge driving actions is creating a new direction. The introduction of smart phones has generated wide acceptance and adaption by business, consumer and general population. This is mainly because of their conveniences and many added values like navigation, location based services, etc. Today, we see higher growth in mobile traffic than landline. Introduction of tablets and growth of ecosystem for mobile applications will cause gradual decline in the growth of PCs and rapid end of desktop equipment. People are now equipped with remote access and control capabilities to manage their home environment (energy, safety and security). They can have access to gadgets that help track their physical condition and wellbeing and generate necessary proactive course of action. For instance, there are devices that can monitor driving behaviors, children's actions and elderly people's routine life and generate multiple alerts when deemed necessary.

In other words, smart connected digital life which is composed of smart homes, offices, factories, hospitals, transports, etc., will contribute to better quality of life, generate business efficiency and additional source of significant revenues. Through cyber-physical and social data, we can better understand events and changes in our surrounding environment. Such information can enable us to monitor and control buildings, homes and city infrastructures. They can also provide better healthcare and elderly care services among many other things. However, in order to make effective use of cyber-physical and social data, integration and processing are necessary since their data come from various sources. IoT includes every device that is connected to the Internet, ranging from home automation products like smart thermostats, security cameras, refrigerators, microwaves, to home entertainment devices such as TVs and game machines, to smart retail shelves that know when they need replenishment, to industrial machinery and many more.

Nonetheless, as the value of connectivity and information continue to increase, so does the management complexity, vulnerability and attractiveness to malicious attacks. Considering that traditional approach security mechanism does not work on IoT and consumers have little knowledge or incentive to make them more secured, cybercriminals can make use of IoT for their distributed attacks. It is therefore essential to consider security in their design process, development cycle and in the effective usage of their information systems [5]. This paper is a follow up of recently published work [5] and the author would like to highlight sequence of events which have happened since then. The aim is to emphasize the danger of devastating attacks via IoT devices and numerous challenges that exit in equipping them with appropriate security. It then underlines the importance of previously proposed universal home gateway based security approach and shows some progress in its implementation process. Finally it explains why and how numerous stake holders are needed to get together for its wide range commercial implementation and urges policy makers and big players to take the security issues of IoT devices more seriously.

The rest of the paper is organized as follows: Section 2 discusses vulnerability of Internet connectivity, including those due to the operating nature of Internet Protocol (IP) and the ones originating from various Internet services. Section 3 presents some details on IoT, their vulnerability, including devastating effects of October 21, 2016 DDoS attack which mainly utilized IoT devices, and the danger of recently revealed Mirai IoT botnet. Section 4 explains why traditional security approaches do not work on IoT and highlights the main causes that make IoT attractive weapon for professional attackers. Section 5 presents a comprehensive long-term security implementation strategy, an immediate necessary and implementable safeguard action, and some intermediate schemes. Finally, summary conclusion and practical recommendation are highlighted in section 6.

2. Vulnerability of Internet Connectivity

For various reasons, today's networks are vulnerable to numerous risks, such as information leakage, privacy infringement and data corruption. Operating nature of communication protocol used in the Internet domain, availability of many free software that can carry out numerous attacks and users' unawareness about such issues are some of the main contributing factors.

2.1. Operating Nature of Internet Protocol

Internet protocol suite which is commonly known as TCP/IP (Transmission Control Protocol and Internet Protocol), is used for most Internet applications. Its IP serves as the primary component for carrying out the task of delivering packets from a source to a destination using the IP addresses contained in the packet header. Proper operation of such transaction worldwide requires source and destination to have unique IP address and included in the packet header of their information packets. The fact that each IP address gets associated with a unique entity, enables attackers to trace IP address of each holder through the packet headers.

What makes security implementation more challenging is the fact that Internet has 256 protocols and TCP is just one of them. Other commonly known Internet protocols are UCP (Universal Computer Protocol), and ICMP (Internet Control Message Protocol). Most experts who try to prevent attacks just consider these three protocols in their implementations. Many skilled attackers, however, use less known protocols in their attacks to bypass system security and such trends have been increasing during the past decade. In most cases, their attacks initially succeed until the defenders could figure out what was going on. What makes it worse is the fact that skilled attackers experiment with their new attack methodologies for years before they weaponize them via automation in order to create high volume impacts.

2.2. Vulnerability of Various Internet Services

As mentioned earlier, Internet services have their associated risks and a few them are intentionally created by service providers. Although at superficial level, they are supposed to be for better

service purposes, but are often abused for the sake of business expansion at the expense of their users' victimization. The rest are carried out by attackers, the purpose of whom may range from adventurism at individual level to financial gain at individual/group/corporate level, all the way to socio-political competition at much wider scale. This section will highlight vulnerability of some services which are used by a wide public, most of whom being technology-unaware people.

As we all know, most Internet services, e.g., web browsing, email, social networking, navigation and location services, etc., are provided for free. But most of such service providers are private companies and for their source of income, they mainly rely on online advertisement. Under the pretext of better service, most of these service providers use what is called tracking cookies, to keep track of their users' activities. For example, if they know your location, they can show you what are available in your surroundings. If they know your eating habit, they can guide you to pertinent restaurants. If they know your shopping habit, they can show you similar products, etc. When a user visits multiple websites with the same ad provider, since the same cookies are employed, the ad provider can track the user's activity in numerous sites just by compiling the information via tracking the cookies without the user's knowledge. The bottom line is to identify users, deliver targeted advertisement and persuade them do things which they may not have done under normal condition. Furthermore, since payments of most online advertisement is established on per click basis, just persuading the user to click the ad, automatically generates income for its host.

Other Internet service vulnerability can include e-commerce and social networking. We all know the convenience of online shopping and social networking. The fact that we can buy anything from any part of the world without leaving our home or connect to our networks and anyone in the world free of charge from our pc/tablet/smart phone etc., is a good evidence of such realities. Today, nations are using social networking for their election campaigns and super powers are using it to influence elections or create revolutions, etc.

It is, however, a well-known fact that privacy is implicated in e-Commerce because it requires us to disclose our personal information, such as email address, credit card information, etc., to complete the transactions. After the transaction, the retailer can use the info for their next targeted advertisement and bombard us with spam emails. What is more dangerous is the scenario of data transfer (e.g., when customer database information is sold to third parties or stolen) since it results in identity or credit card theft [6]. Furthermore, when such transactions are done via less secured networks, professional attackers can use numerous techniques to steal our credit card information and use it up to its maximum limit before we realize it. During the past decade, this approach has also penetrated to e-banking and huge amount of money have been stolen from peoples' accounts. [7-8].

At a bigger scale, security experts claim that North Korean cyber attackers have targeted banks in 18 countries for the purpose of Pyongyang using the money to boost its nuclear program [9-10]. Using cyber-attacks on nuclear power plant is even more concerning. On October 10, 2016, Reuters reported that according to Yukiya Amano, the International Atomic Energy Agency director, a nuclear power plant had been disrupted by a cyber-attack in the past two or three years [11]. Although additional details, including where the incident took place were not provided, Amano had said: "This issue of cyber-attacks on nuclear-related facilities or activities should be taken very seriously. We never know if we know everything or if it's the tip of the iceberg."

Vulnerability of social networking services is another example that the author would like to mention in this paper since it is mostly used by non-technical people. It is a scenario similar to IoT and combined utilization of different social networking services has dramatically increased, surpassing nine billion users as of April 2017 [12]. As can be guessed, this has lead cyber threats originating from social-engineering technique to also significantly increase. A study conducted by Verizon Enterprise in 2013 showed that it increased by 4 folds within the single year that they carried out the investigation [13]. Considering its rapid development, its adoption for online advertising and marketing, and its utilization by big powers even in political games, it can be foreseen that intrusions through social networking services will continue to increase in the coming years.

3. IoT and their Vulnerability

As mentioned in the introduction section, IoT includes every device that is connected to the Internet, including those ranging from home automation products like smart thermostats, security cameras, refrigerators, microwaves, to home entertainment devices such as TVs and game machines, smart retail shelves that know when they need replenishment, to industrial machinery and many more.

3.1. Some Elaborations on IoT

The term IoT was invented by a British entrepreneur Kevin Ashton in 1999 and was initially used to refer to a global network of Radio-frequency identification (RFID) connected devices [14]. Although the usage of the term IoT in its present context is less than a decade old, most of the present day IoT devices have existed for decades but they were called under different names such as smart devices, smart systems, smart home appliances, etc. Smart has been a common keyword for such devices before the invention of the term IoT.

Recent rapid expansion of IoT has been due to miniaturization of integrated circuit (IC) chips, tremendous increase in their processing/storage capabilities and huge drop in their production cost. Readily available fast, reliable and free/cheap Internet connection around the globe can be considered another major factor in the rapid expansion. Such developments have made it possible to embed various devices with electronics, software, sensors, and network connectivity and enable them to collect and exchange data. The process of sensors generating data, data producing knowledge and knowledge driving actions has enabled automation, remote sensing and remote control in many areas.

3.2. Vulnerability of IoT

As mentioned earlier, convenience of connecting to the Internet has its associated risks and IoT are no exception in this context. However, threat likelihood level of IoT for a particular type of attack would depend on its function. For example, a healthcare monitor device will be less vulnerable to data alteration attack than a security camera device.

On the other hand, huge number of IoT combined with their weak/no security, make them quite attractive for distributed denial of service (DDoS) attack, regardless of their specific functionality. Although no serious DDoS attack originating from IoT network had been reported until recently, the next section will highlight some devastating recent attacks. Nonetheless, its possibility and

upward trend had been predicted based on simple calculation and projection many years ago. If we assume that only 0.01% of the IoT network gets compromised by 2020, this could lead around 20 million appliances vulnerable to cyber-attacks. Even granting that most of the IoT will only transmit relatively small amounts of data, considering their enormous size, the attack can easily bring down a domain name system (DNS) server, or any another host. This is mainly because DDoS attack uses an integrated effect of its compromised devices. Furthermore, because each compromised element has its own unique IP address, blocking a DDoS attack becomes extremely difficult after it takes place.

3.3. Emergence of Thingbot

Traditional DDoS attack took place via a huge network of compromised PCs. Each PC in the network is transformed into a slave by means of malware. Such network is called botnet which is an abbreviation for words "ro**bot**" and "**net**work". This type of attacks occur without awareness of Internet users. Thingbot is an abbreviation similar to the word botnet, but comprised of the words "**thing**" and "ro**bot**". It indicates a huge network of compromised IoT for launching cyber-attacks. The first large scale thingbot based attack was discovered by security researchers from Proofpoint in early 2014. It consisted of more than 750,000 phishing and spam emails which were launched from thingbot. The network contained more than 100,000 hacked IoT devices, ranging from smart TVs, refrigerators and other smart household appliances [15].

Presence of huge vulnerable IoT devices and introduction of DDoS-for-hire 'booter'/'stresser' service have significantly changed and increased the risk. It enables attackers to launch DDoS attacks against target(s) of their choices in exchange for monetary compensation which usually comes in form of Bitcoin. On October 21, 2016 a DDoS attack utilized at least 150,000 hacked IoT devices and created devastating effects. It resulted in a 1 Tbps traffic, 40 to 50 times higher than normal, and brought down much of the America's internet for few hours [16]. The compromised IoT consisted of digital video recorders (DVRs), surveillance cameras and other smart devices that had weak default passwords. The created huge amount of bogus traffic targeted a major DNS service provider (Dyn) and others. This is the largest of its kind in the history as of today and its origin is traced to Mirai-based thingbot from where a significant volume of the attack traffic was originated.

The Mirai IoT botnet which was revealed in August 2016 has been launching multiple high-profile, high-impact DDoS attacks against numerous Internet properties and services worldwide. Even 2016 Rio Olympics and their associated organization were targeted by sustained and large-scale DDoS attacks, but due to their advance preparedness, they were able to minimize the impact. The botnet serves as the basis for the so called 'booter'/'stresser' service and its nodes are scattered around the world. Their concentrations are, however, higher in Spain, Brazil, Indonesia, Thailand, South Korea, Taiwan, Macau, Hong Kong, and China [17-18]. The botnet has been expanding by incorporating vulnerable IoT devices through automated continuous scanning using well-known, hardcoded administrative credentials that are present in the IoT devices.

4. IoT Security Implementation Challenges

Like other Internet enabled devices, IoT are also prone to numerous risks. Although threat likelihood level of IoT for a particular type of attack depends on its functionality, none of such threats are new. There are established security measures for most of them. However, peculiar characteristics of IoT make implementation of such security measures in a traditional way quite challenging and this section highlights some of its major causes.

4.1. Limited Resources

Unlike traditional computers, IoT are designed to serve only a specific purpose and marketability factors such as low cost, portability, tinier size, etc., prevent them from having powerful processing capabilities. It does not make sense to incorporate several hundred dollars' worth of security and processing capability in IoT devices like smart watch, smart LED, smart toaster, etc., the sale value of which are few tens of dollars. As such, most IoT end up having toy CPUs that cannot handle computationally expensive cryptographic computations and with battery power that prohibits long-lasting or high-peak computations. Hence, built-in full cryptography capability which is common for most computers becomes infeasible for most IoT devices.

4.2. Technology-Unaware Users

Even in those IoT devices, such as smart TV, smart refrigerator, healthcare monitor, etc., into which incorporation of powerful processing capabilities are feasible (cost wise, size wise, etc.), such incorporation does not produce positive results in most cases. This is mainly because most of their users are technology-unaware people, unable to take advantage of such functionality, consider their usage and requirements user unfriendly and additional burden both in terms of their cost and utilization. Hence, our competitive market makes vulnerable IoT devices more attractive in terms of their low cost and user friendliness. It also discourages makers to build secured devices in the production stage.

4.3. Around-the-clock Availability

Traditional computer users, in addition to being more technology aware people in comparison with typical IoT users, turn off their computer after they accomplished their tasks. Furthermore, they stay at their computer most of the time while it is on. In other words, Internet connectivity of traditional computers is enabled while their users actively use them and are disabled when they finish their tasks. In contrast to human-controlled computers, most IoT e.g., smart refrigerators, security cameras, gas/fire sensors, etc., are connected to the Internet 24 hours. Hence, their around-the-clock availability on the Internet, weak/no security make them quite attractive for attackers to continuously experiment their attack techniques. As mentioned earlier, skilled attackers experiment with their new attack techniques for years before they employ them at large scale via automation for high impact achievement.

5. Possible IoT Security Solutions

As we can see, despite the necessity and high importance of equipping IoT with appropriate security measures, its achievement is not that easy. The author originally got involved with investigation of security of smart home appliances over a decade ago and has recently extended it to the broader field of IoT. In this section, the author would like to share his findings in form of a comprehensive long-term security implementation strategy, an immediate necessary and implementable safeguard action, and some intermediate schemes.

Considering the existence of theoretical security measures for most threats against IoT, impracticability of incorporating such measures within each individual IoT inform of powerful security processing capability, the author would like to emphasize the importance of securing the local area network to which they are connected. The fact that most IoT rely on locally available Internet in their vicinity, e.g., home, office, etc., existence of more than one IoT in every home or office and stationary nature of most IoT, the approach can be considered as the most practical one.

5.1. Appropriate Security Model

A decade ago, the author after thoroughly investigating vulnerability of smart home appliances and existence of numerous challenges in equipping individual appliance with appropriate security, came up with the idea of "universal home gateway" (UHG) approach. The idea was to connect all Internet enabled gadgets of a house through a single gateway, build the necessary security processing capability into the gateway and let network operators and service providers to remotely manage the required security via the gateway [19-20]. The purpose was to avoid built-in security features for each gadget and embed all the security related processing capability into the gateway instead. The operation involved channeling of all local and remote access to a family area network (FAN) via the gateway by means some user-friendly authentication schemes. Its required security management was envisioned to be carried out remotely by service related third party experts in exchange for a reasonable overhead cost. The logic was, since vulnerability comes from the Internet connection, if we channel all of our devices' Internet access through a single gateway and secure the gateway, everything gets secured without requiring any of our devices to have its own built-in security related processing capability or us to perform technical security management tasks. This approach will definitely work for IoT devices like smart thermostats, security cameras, refrigerators, microwaves, etc. which are used at a fixed location. However, a different security scheme will still be needed for non-stationary IoT like smart watch, smart phone, tablet, etc. when they utilize Internet from outside the FAN.

The problem was that existing gateways were not compatible with all smart home appliances since they required different wireless technologies and protocols. The author, however, gave detailed functional requirements of such UHG, how to initiate its construction, as well as pertinent responsibilities and commitments of its numerous stakeholders. The proposed idea may have sounded like a far reachable dream and some people even wondered about the viability of being able to control many different devices by means of a single gateway. Nonetheless, even at that time, there were some vendors whose products were marketed with a central controller that could link their smart home appliances together in a FAN environment and offered some limited security and exclusive digital services [21-22]. History has shown that propriety approaches are prone to fail and the author was hopeful that in the near future, a universal controller could control various smart gadgets that are manufactured by many different companies.

5.2. Current State of the Envisioned Security Model

At present, commonly used communication methods for IoT devices include Z-Wave, Zigbee, Powerline, Bluetooth 4.0 and other radio frequency (RF) protocols. Among these, Z-Wave, Zigbee and Powerline are the most common ones for home automation devices. Z-Wave protocol seems to also have better backwards and forwards compatibility, widely adopted as it is easier to find Z-Wave compatible devices from different manufacturers. Figure 1 shows a commercial product of Z-Wave which is compatible with 1,500 products that are produced by 375 companies [23].

Figure 1 Z-Wave Wireless Technology (Z-Wave Alliance, May 2017).

5.3. Long Term Security Strategy

For a comprehensive long-term security implementation strategy, the author would still recommend the originally proposed UHG approach since no other scheme can handle the numerous challenges that exit in equipping IoT with appropriate security measures in a better way. The fact that in less than a decade, compatibility from a few single company based products has grown to 1,500 products that are produced by 375 different companies, shows that it is not a far reachable dream and we are indeed moving in that direction. Unfortunately, however, Z-Wave protocol is still a proprietary standard.

The remaining gaps are to get rid of proprietary standards, involve cooperation of manufacturers, network operators and service providers more widely, arrive at a consensus on minimum security requirements among main stakeholders and involve policy makers on the legal implementation. The size and impact of October 21, 2016 shows the urgency of the matter and an unsuccessful 2016 Rio Olympics attack should not be allowed to turn into a perfect success in a foreseen 2020 Tokyo Olympics attack. The most effective way to achieve this is to:

- Engage a network operator to build dedicated but nonproprietary universal home gateways and become the preferred trusted third party.
- Motivate IoT manufacturers to develop device drivers and application software that can run on such UHG for their control and operation.

This will, however, require support for security-driven business models and involvement of policy makers on the legal aspects of utilizing IoT. It is worth mentioning that thingbots are used against third parties rather than their IoT owners. Furthermore, consensus on minimum security requirements among main stakeholders (e.g., IoT manufacturers, third-party developers, service and solution providers and electronic communications providers) will be essential.

Therefore, design and development of an open system and involvement of big and experienced players like network operators

are vital to the successful adoption of the technologies. This way, their users can enjoy security without having to be aware of the underlying mechanisms. UHG may even be provided free of charge, like the way that cell phone sets and broadband modems are being given away by their respective service providers in Japan. Security pricing may also be implemented on a product (functional group) based scheme.

There are standards bodies which specify how to build these devices and meet their various requirements, e.g., OSGi Alliance [24-25]. It is essential to conform to these standards when building, managing and providing services for IoT in the future. Such an approach will encourage more vendors/manufacturers to conform to these standards, and the standards themselves will evolve as needs arise. The best way to proceed is to develop the security model around IoT and network components that conform to certain standards.

5.4. Immediate Necessary Safeguard Actions

Considering our globalization trends and increase in competition, the levels of bureaucracy that exist in many governments when making new policies, and their difficulties when trying to implement created policies, immediate implementation of the proposed security scheme may be difficult. Nonetheless, through some immediate safeguard actions, one can at least reduce vulnerabilities of IoT for their involvement in possible attacks. The following such actions are therefore recommended to be carried by IoT owners, their sellers or service providers:

- Change their default passwords since attackers usually penetrate through such settings.
- Disable their Universal Plug-and-Play features since they create security loopholes and are enabled by default.
- Disable their Telnet based remote management as Telnet can be used to control them remotely.
- Keep their software up-to-date so as to protect them against the known attacks.

5.5. Some Intermediate Schemes

Let us not forget that achievement of ultimate security goal requires both hard and soft infrastructures. The author has so far mainly focused on the hard infrastructure but soft infrastructures inform of appropriate education, training, guidelines, policies and governance systems are equally important. The fact that thingbot adversely affects third parties rather than their respective IoT owners, implies moral, social and "hopefully in the near future" legal obligation for their possessors. Now that the Internet is an indispensable part of our social life and business activity, security awareness and pertinent education for the common people is also quite important. Furthermore, no security will work when a user does not properly select/protect his/her passwords for various Internet services or does not know what Phishing/Pharming is, clicks such links and provide the requested information. In some collaborative work, the author has explained some relevant incidents which have taken place in online advertising and social networking services [4, 26]. Unfortunately, even in a highly industrialized country like Japan, information security awareness is not part of general education even at university level!

Considering slow progress in the UHG approach and dramatic increase in the use of social networking platforms by many non-technical people, its adoption for online advertising and marketing and victimization of many users, the author also investigated the employment of anonymous communication and its adoption to IoT network. Implementation of TOR (the Onion Router)-based anonymous communication into the IoT network as an effective alternative way to help smart home appliance users protect their privacy and make the smart home appliance system more secure from aforementioned cyber-attacks was the main objective of the work [27]. Such approach can also be effective, particularly for technology-aware users and could even be utilized for non-stationary IoT devices.

6. Conclusion

This paper explained numerous conveniences of IoT and its projected huge market in the near future. It also showed that like other Internet enabled devices, IoT are also prone to numerous risks but there exist theoretical security measures for most of them. Nonetheless, peculiar characteristics of IoT make implementation of such security measures in a traditional way quite challenging and their huge number make them quite attractive for DDoS attack. It highlighted the devastating effects of October 21, 2016 DDoS attack and emphasized the danger of Mirai IoT botnet which serves as the basis for the DDoS-for-hire 'booter'/'stresser' service and enables attackers to carry out DDoS attacks against targets of their choice in exchange for monetary compensation that usually comes in the form of Bitcoin payments. An architecture wherein security issues are managed through universal home gateway by network operators in a product based fashion was cited. It emphasized support for security-driven business models, consensus on minimum security requirements among main stakeholders and involvement of policy makers on the legal aspects of IoT environments. Some immediate necessary safeguard actions and intermediate schemes which included soft infrastructures were also recommended for the purpose of risk reduction. It is hoped that policy makers and big players take the security issues of IoT devices quite seriously and maintain the October 21, 2016 DDoS attack as the largest of its kind in the history forever.

Conflict of Interest

The author declare no conflict of interest.

References

[1] C. Drake, "FireHost detects surge in SQL injection for Q3 2013 and cross-site scripting is rising", retrieved from http://www.firehost.com/company/-newsroom/press-releases/firehost-detectssurge-in-sql-injection-for-q3-2013-with-cross-site-scripting-also-rising/, October 2013

[2] Samsung Group, "Home has a new hub", retrieved from http://www.samsung.com/us/explore/family-hub-refrigerator/, July 2016.

[3] ZDNet, "Internet of Things: $8.9 trillion market in 2020, 212 billion connected things", retrieved from http://www.zdnet.com/ article/internet-of-things-8-9-trillion-market-in-2020-212-billion-connected-things/, May 2017.

[4] Angelia, D. Pishva, "Online advertising and its security and privacy concerns" in proceeding of the 15th International Conference on Advanced Communication Technology (vol. 1, pp. 372-377), Seoul Korea, 2013.

[5] D. Pishva, "Internet of Things: security and privacy issues and possible solution" ICACT Transactions on Advanced Communications Technology (TACT), **5**(2), 797-808, 2016.

[6] M.J. Metzger, "Communication privacy management in electronic commerce" Journal of Computer-Mediated Communication, **12**(2), 335–361, January 2007.

[7] Mybroadband, "How criminals steal money from your online bank account", retrieved from https://mybroadband.co.za/news/banking/125652 -how-criminals-steal-money-from-your-online-bank-account.html, May 2017.

[8] N. Kaur, "A survey on online banking system attacks and its countermeasures" International Journal of Computer Science and Network Security (IJCSNS), **15**(3), 57-61, 2015.

[9] MailOnline, "Researchers say group linked to North Korea is attacking banks around the world", retrieved from http://www.dailymail.co.uk/news/article-4379248/North-Korea-hackers-target-banks-18-countries.html, May 2017.

[10] Reuters, "North Korean hacking group behind recent attacks on banks: Symantec", retrieved from http://www.reuters.com/article/us-cyber-northkorea-symantec-idUSKBN16M37J, May 2017.

[11] Wired, "International Atomic Energy Agency director says nuclear power plant was impacted by malicious hack", retrieved from https://www.wired.com/2016/10/security-news-week-hackers-hit-nuclear-plant/, May 2017.

[12] Statista, "Most famous social network sites worldwide as of April 2017, ranked by number of active users (in millions)", retrieved from http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/, May 2017.

[13] Verizon Enterprise, "The 2013 Data Breach Investigations Report", retrieved from http://www.verizonenterprise.com/DBIR/2013, 2013.

[14] Wikipedia, "Internet of things", retrieved from https://en.wikipedia.org/wiki/Internet_of_things, May 2017.

[15] Cyber Defense Magazine, "Proofpoint discovered more than 750,000 phishing and spam emails launched from thingbots including televisions, fridge", retrieved from http://www.cyberdefensemagazine.com/ iot-discovered-first-internet-of-things-cyberattack-on-large-scale/, May 2017.

[16] P. Paganini, "150,000 IoT devices behind the 1Tbps DDoS attack on OVH", retrieved from http://securityaffairs.co/wordpress/51726/ cyber-crime/ovh-hit-botnet-iot.html, November 2016.

[17] Arbor Networks, "DDoS attacks from IoT botnets don't have to mean game over", retrieved from https://www.arbornetworks.com/ blog/asert/rio-olympics-take-gold-40gbsec-sustained-ddos-attacks/, November 2016.

[18] Arbor Networks, "The lizard brain of lizard stressor", retrieved from https://www.arbornetworks.com/blog/asert/lizard-brain-lizardstresser/, November 2016.

[19] D. Pishva, K. Takeda, "A product based security model for smart home appliances" in proceeding of 40th Annual IEEE International Carnahan Conferences on Security Technology (vol. 1, pp. 234-242), Lexington USA, 2006.

[20] D. Pishva, K. Takeda, "A product based security model for smart home appliances" IEEE Aerospace and Electronics System Magazine, **23**(10), 32-41, 2008.

[21] K. Yoshimi, "Addressing security requirements of network enabled home appliances, next generation IP infrastructure group report (WG3-1)", retrieved (in Japanese) from Ministry of Internal Affairs and Communication (MIC):http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/jise_ip/pdf/050217_1_s1.pdf, December 2005.

[22] T. Satoru, "Information appliance system authentication technology, next generation IP infrastructure group report (WG3-2)", retrieved (in Japanese) from Ministry of Internal Affairs and Communication (MIC): http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/jise_ip/pdf/050217_1_s2.pdf, January, 2006.

[23] Z-Wave Alliance, "The Internet of Things is powered by Z-Wave", retrieved from: http://z-wavealliance.org/z-wave_for_consumers/, May 2017.

[24] OSGi Alliance, "Internet of Things", retrieved from https://www.osgi.org/business/markets-and-solutions/markets-and-solutions%E2%80%8Einternet-of-things/, May 2017.

[25] OSGi Service Platform Products, "OSGi Markets and Solutions", retrieved from http://www.osgi.org/products/products.asp?section=3, July 2015.

[26] N.P. Hoang, D. Pishva, "Anonymous communication and its importance in social networking" in proceeding of the 16th International Conference on Advanced Communication Technology (vol. 1, pp. 34-39), Seoul Korea, 2014.

[27] N.P. Hoang, D. Pishva, "A TOR-based anonymous communication approach to secure smart home appliances" ICACT Transactions on Advanced Communications Technology (TACT), **3**(5), 517-525, 2014.