International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 2

Successive Security Challenges Implementation on Internet of Things

M. Ann Bency
Assistant Professor, Department of Computer Science
Prince Shri Venkateshwara Padmavathy Engineering College, Ponmar,Chennai, India

ABSTRACT

This Paper demonstrates *commonly* used communication scheme and information retrieval which are carried out via Internet using numerous types of smart devices, can turn the Internet into a very dangerous platform because of its built-in nature of making its users' identity easily traceable and discusses some countermeasures that can be used to prevent existing and projected security breaches. It initially provides some introductory information on technology advancement, penetration of the Internet to all aspects of our life and its associated conveniences. It then discusses vulnerability of internet services, presents some typical attack cases that are carried out via smart home appliances, and explains security implementation challenges on such devices from technical, social, and practical aspects. Finally, it proposes an appropriate security model, demonstrates relevant counter measures for numerous attack scenarios, and explains why and how numerous stake holders are needed to get together for its commercial implementation.

Keyword: *Internet of Things, IoT, Smart, Social Cybernetics, Social Networking, Facebook, Online Advertising, Security, Privacy, Network Tracing Tools*

I. INTRODUCTION

The 21st century has been regarded by many as the information era and penetration of Internet into all aspects of our life is a new dimension along which technologies continue to grow. The advancement in technology has been changing the way of our life and digital information has now become a social infrastructure. We are surrounded by technologies and there are computer technologies in our cars, phones, watches, entertainment systems, and home appliances. The idea is to make use of existing electronics in the devices and, in conjunction with some specialized software, create an intelligent network with access to the Internet.

Since the expansion of the Internet in 1990s, network infrastructure has become an indispensable part of social life and industrial activity for mankind. The idea of using existing electronics in smart home appliances and connecting them to the Internet is a new dimension along which technologies.

Continue to grow, and in recent years mankind has witnessed an upsurge of usage of devices such as smart phone, smart television, home health-care device, etc. Their build-in internet-controlled function has made them quite attractive to many segments of consumers and smart phone has become a common gadget for social networking. Commercial advertising has also greatly benefitted from Internet services and social networking is also being used for online advertising and business transaction.

With 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]. Just to mention a few examples, we use Internet for various sorts of communication like VoIP and email, multimedia services like Online Music and Online Movie, business transaction like e-Banking and e-

Business, administrative work like e-Governance and e-Administration, networking activities such as Online Advertising and Social Networking. Furthermore, along with the development of Internet, e-Commerce has become an efficient marketing tool for many companies and Social Networking with Facebook is an emerging market which has recently become the most visited website in the world [2][3].

Traditionally social networking was done in person and in places like schools, communities, neighborhoods, workplaces etc. and hence limited in size. Although the use of social networking for business and advertisement is not something new, its traditional approach had limited size as it required face-to-face or mouth-to-mouth interactions. Since the expansion of the Internet, however, social networking has grown exponentially and according to Statista [4], Facebook's registered accounts have surpassed one billion users as of March 2015. According to the same source, approximately 347 million people are active on LinkedIn, 300 million uses Google+ and another 288 million use twitter. There are of course many other social networking sites, but none of them even existed at the beginning of the 21st century. In fact, when Facebook was launched in 2004, many people considered it as a place for kids to share their pictures and emotions. Today, however, businesses and marketers love social media and indeed, 90 percent of marketers are using social media for business [5]. Seventy percent have used Facebook to successfully gain new customers and 34 percent have used Twitter to successfully generate leads [6].

In Japan, many audio visual equipment can already be connected to the Internet, enabling 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. Network connectivity is likely to be equipped in all AV equipment in the near future. Such developments have been leading mankind to a new era of technology, the era of the "Internet of Things" (hereafter: IoT), where all the appliances are getting tiny and controllable via the Internet, thus enabling people to enjoy network based services like Video on Demand (VOD), Music on Demand (MOD), remote update, e-Commerce, remote control, and other similar services.

Furthermore, researchers around the world have come up with an abundance of resourceful ideas on how to effectively use microprocessors and Internet in other everyday household appliances. 'Smart' is the new buzzword that we can hear these days; for example, in 'smart' homes, 'smart' kitchens, 'smart' ovens, 'smart' refrigerators, etc. [7]. Table 1 indicates functional classification of smart home appliances [8][9]. There is also a tremendous business potential for them because of foreseen future demand by elderly people, where the number of people over the age of 65 is expected to double to 70 million by 2030 [10]. 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 in 2020 [11]. Those "things" will be nothing special but daily used appliances ranging from watch, light bulb to smart television, refrigerator and so on.

TABLE I FUNCTIONAL CLASSIFICATION OF SMART HOME APPLIANCES

No	Function	Example of Product or Usage
1	Content Retrieval	Broadband TV, Microwave Oven, HDD Recorder (for TV program, etc.)
2	Content Storage/Usage	HDD Recorder (for TV program, etc.), MP3 Player
3	Communication/Messaging	VoIP , IP-TV Phone, All kinds of Emails System, Healthcare System
4	Remote Surveillance	Security Camera, Gas/Fire Sensors, Refrigerator, Lighting Fixture, Door Lock
5	Remote Control	Air Conditioner, Lighting Fixture, TV, TV Program Recording
6	Remote Maintenance	Firmware Update, Trouble Report
7	Instrument Linkage	Networked AV Equipment
8	Networked Game	Family Type Game Machine

Commercial advertising has also greatly benefitted from Internet services and online advertising can even be considered as the foundation of web economy. However, the system of online advertising is quite unique. Unlike conventional forms of advertising, the system of online advertising allows its target to receive something in return in exchange for viewing the advertisement. Besides getting information from the advertisement itself, the target of online advertising is usually allowed to use the advertisement host website's service. For example, as shown in Figure 1, video2mp3.net, a website that offers free file conversion from YouTube video to mp3 format, has numerous advertisements displayed on its page [12]. It even goes as far as setting a hidden advertisement that will only appear when the user clicks the "High quality" option. Nevertheless, the users are not required to pay for the service. They are instead offered a premium service where they can get exclusive access to the website without advertisements popping up along the way. In this way, online advertising has defined a new term of "free service", where four parties – the advertisers, the ad network, the ad hosts, and the users - are involved within it [13].

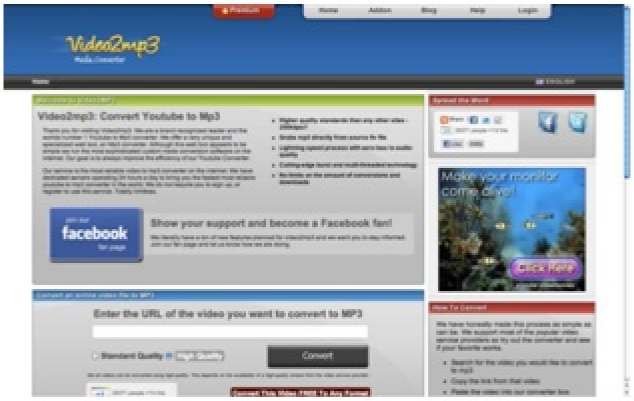

Premium
Home
Addon
Blog
Help
Login
Video2mp3
Media Converter
Video2mp3: Convert Youtube to Mp3
facebook
Show your support and become a Facebook fan!
Make your monitor come alive!
Click Here
Enter the URL of the video you want to convert to MP3
Standard Quality
Convert

Fig 1: A view of Video2mp3.net. On the right side is one of its many advertisements.

In other words, today's business activities depend highly on information systems and every enterprise has its own information for its business. In an industrialized country like Japan, most enterprises use information technology to establish their management governance. This helps them improve their efficiency and cost performance. As it is called 'IT governance', information systems have significant impact on the operations. Information assets have thus become valuable commodities for business and information systems are the key factors to ensure the growths of enterprises. Hence, it is essential to control the design process, development cycle and effective utilization of information systems. Nonetheless, as information and its value continue to increase, so does the management complexity, vulnerability and attractiveness to malicious attacks. Security threats can come in the form of unauthorized accesses, computer viruses, or cyber-attacks.

II. VULNERABILITY OF INTERNET SERVICES

For various reasons, however, today's networks are vulnerable to numerous risks, such as information leakage, privacy infringement and data corruption. One of the main underlying factors is operating nature of the communication protocol used in the Internet domain and availability of many free software that can carry out most of these attacks. The Internet protocol suite which is commonly known as TCP/IP (Transmission Control Protocol and Internet Protocol), is used for most Internet applications. IP serving as its primary component carries out the task of delivering packets from source host to destination host solely based on the IP addresses contained in the packet headers. In order to achieve proper operation of such transaction worldwide, this requires source and destination to have unique IP address and includes it in the packet headers of their information packets. Since every IP address is associated with a unique entity, identity of IP address holders can be traced using their IP addresses contained in the packet headers. This section briefly discusses vulnerabilities of some Internet services.

A. Vulnerabilities of e-Commerce

It is a known fact that privacy is implicated in e-Commerce because of the risk involved in disclosing personal information such as email addresses or credit card information, which is required for most electronic transactions. Specific privacy concerns in this realm include use of customers' information by companies for electronic surveillance (e.g., 'cookies'), email solicitation (e.g., 'spam'), or data transfer (e.g., when customer database information is sold to third parties or stolen) resulting in identity or credit card theft [12][13]. Online advertisement which is a major component of e-Commerce uses cookies as a mean to identify users and deliver targeted advertising by tracking their movements in the website. Such cookies are called tracking cookies and an ad network company like Google uses this type of cookies for delivering ads that are relevant to the user's interests, controlling the number of times the user sees a given ad, and "measure the effectiveness of ad campaigns" (Google Policies & Principles, 2012).

The problem with tracking cookies is that when the user visits multiple websites with the same ad provider, the same cookies from the ad provider will be used. This means that the ad provider will be able to track the user's activity in numerous sites just by compiling the information via tracking the cookies without the user's knowledge. The result of this action means the loss of anonymity to the users, which is a blatant breach of information security as well as privacy. Although the ad network are obliged to comply with privacy act and use the information only for marketing strategy, users cannot be sure if it is not used for other purposes. In fact, personal information is being freely traded without the consent of their owners for money making purposes. Personal information related to interest and habit of prospect customers are an essential component for delivering online advertising and can be considered as the lifeline of many websites.

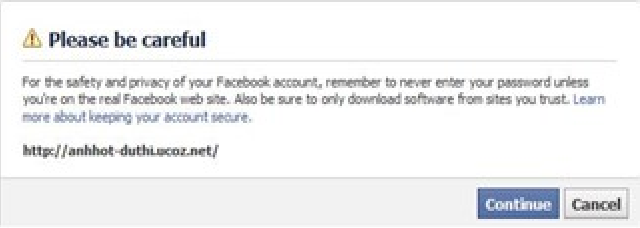
It is only recently that people and governments started to pay attention to this previously un-scrutinized golden goose. The Wall Street Journal's investigation in 2010 revealed an array of cookies and surveillance technologies, with real time function and deactivation resistance, are being used to monitor the users' personal information. The investigation also found out that online tracking is not a small business. The top 50 websites kept close tabs on their users by installing, on the average, 64 different pieces of surveillance technology

[14]. As such approaches could unconsciously victimize both technical and non-technical users, anonymous communication is becoming more and more important on Internet environment since it can protect people's right to online privacy and reduce the possibility of getting recognized and thus victimized.

B. Vulnerabilities of Social Networking

In recent years, because of dramatic increase in the use of social networking platforms by many non-technical people, social-engineering technique is also being widely exploited to victimize users. Phishing is a good example of social engineering intrusion technique in which a hacker just needs to tempt the innocent users to fill in only their Facebook ID and password. The aftermaths of releasing such information are detrimental since huge amount of private information such as user's address, birthday, job, education history, hobbies, friends, relationship and a bunch of other sensitive information could be accessed from the Facebook account.

Although Facebook filters all URLs which link its users to an external website and warns them of fraudulent websites, the approach does not always work. For example, after clicking to the link: http://anhhot-duthi.ucoz.net/, which is a fraudulent website created by a Vietnamese hacker [2][3], Facebook will warn the user about the vulnerability of the site through a dialog box shown in Figure 2. This, however, does not always happen since hackers keep on creating new fraudulent web pages in order to penetrate through loopholes of Facebook's security. Furthermore, oftentimes, non-technical people may unconsciously press the "Continue" button instead of the "Cancel" button.



⚠ Please be careful

For the safety and privacy of your Facebook account, remember to never enter your password unless you're on the real Facebook web site. Also be sure to only download software from sites you trust. Learn more about keeping your account secure.

http://anhhot-duthi.ucoz.net/

Fig 2: Vulnerability warning of Facebook

Now let us see what happens when either Facebook's security does not detect the above mentioned fraudulent website or a user clicks the "Continue" button. As shown in Figure 3, the control would transfer to a phishing site that has the appearance of Yahoo Vietnam website, containing Facebook Logo and a login form which resembles that of the official website. Although a technical user could easily display HyperText Markup Language (HTML) view of the page to determine where the information would be sent, some innocents users may just fill up the form and press the submit button. As indicated in the highlighted section of Figure 3, information content of the form would simply be sent to http://allforms. mailjol.net/, a site which provides free Form-to-Mail service. In other words, filling out the form and pressing "submit" button, will transfer ID and password of Facebook user directly to the email address of the attacker [2][3].

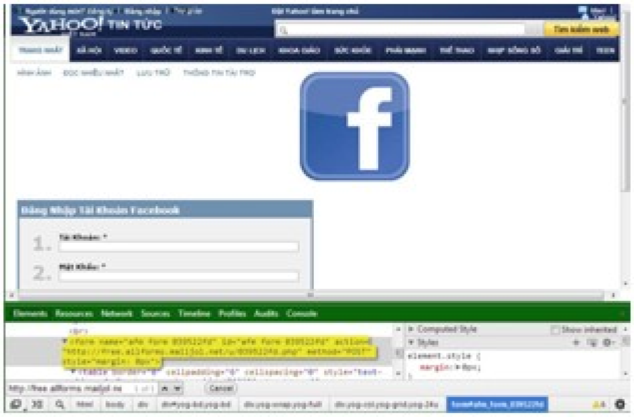


Fig 3: An example of a phishing website http://anhhot-duthi.ucoz.net/.

After obtaining the first victim's Facebook account, the attacker can easily exploit more users in a targeted manner by taking advantage of the victim's personal information and Facebook's internal working mechanism. Facebook has a built-in feature called "important friends" the function of which is to internally keep track of people with whom a Facebook user communicates frequently and shares some commonality (e.g., same high school, hometown, fan page, etc.). In a targeted phishing Facebook, since the phishing link is being sent from Facebook account of an important friend, i.e., trustable and authentic source, attacker may easily persuade the recipient friend to click the link and supply the requested information. The chain reaction of such approach will enable the attacker to easily victimize many Facebook users in a short period of time.

According to the 2013 Data Breach Investigations Report [15], cyber threat derived from social-engineering technique is increasing dramatically as shown in Figure 4. Although its percentage is still low compared to "Malware" and "Hacking", threat caused by social-engineering intrusion has increased by more than 4 times within one year. Considering the rapid development of social networks, it can be foreseen that social engineering intrusion will continue to increase in the coming years, thus necessitating appropriate countermeasures.

C. *Vulnerabilities of Smart Home Appliances*

Connecting smart home appliances to the Internet can also makes us vulnerable to malicious attacks. An intruder can steal private information such as contact info, shopping or eating preferences, lifestyle and relaxation habits, or credit card information used to pay for such services. With the rapid growth of online content in the last decade, advertisers became more aware that demographic information would allow more targeted approach in the advertisement. As database-mining techniques become more and more sophisticated, advertisers find more effective strategies, e.g. contextual targeting, in order to attract the attention of more targeted audiences as opposed to the basic targeting techniques such as time, frequency, demography, etc. [14]. They can also use smart appliances as launching pads to carry out malicious attacks into other systems. Table 2 shows a list of common attacks that can be carried out through smart home appliance and the next section discusses some specific attack cases[8][9].

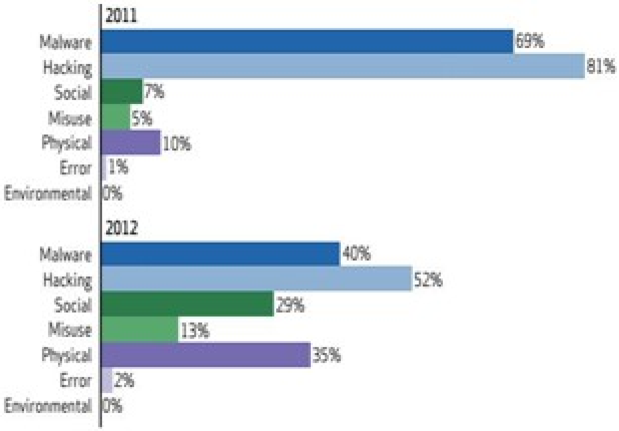


Fig. 4 Threat action categories in 2011 and 2012 (Verizon Enterprise, 2013)

TABLE II: A LIST OF COMMON ATTACKS

No	Common Threat	Example of an Attack
1	User Impersonation	Impersonation using password
2	Device Impersonation	Impersonation of a device using its faulty certificate
3	Service Interruption	Distributed Denial of Service (DDOS)
4	Data Alteration	Data alteration of transmitted or stored data
5	Worm/Virus Infection	Infiltration and/or damaging of a computer system
6	Phishing/Pharming	Impersonation of users' destination
7	Data Wiretapping	Information leakage through wiretapping
8	Firmware Alteration	Replacing of firmware at will
9	OS/Software Vulnerability	Launching of worms and attacks using such vulnerabilities

III. TYPICAL ATTACK CASES

The author has previously shown how the nature of Internet Protocol could accidentally put its user's identity into high risk of being revealed due to the existence of private information behind the IP address in the packet header, which can be easily extracted and observed by various IP tracer and deep packet inspection tools [2][3]. In addition, the use of sniffing tools such as Wireshark or other network monitoring applications, though not new, turn out to be very efficient for attacking IoT networks too. Table 3 shows threat likelihood level of a given smart home appliance type for a particular attack based on past and present security-related incidents, where H, M and L indicate high, medium, and low level threat likelihood, respectively and '-' entries implies no supporting data available. The rest of the section briefly discusses certain classical techniques that have recently been employed to carry some of these attacks on the smart home appliance system not only to steal personal information but also abuse the devices and make them serve cyber criminals' numerous illegal purposes.

TABLE III: THREAT LIKELIHOOD LEVEL OF A GIVEN SMART HOME APPLIANCE

	Common	1	2	3	4	5	6	7	8	9
No	**Threat Function**	User Impersonatio	Device Impersonatio	Service Interruptio	Data Alteration	Worm/Virus Infection	Phishing Pharming	Data Wiretapping	Firmware Alteration	OS/Software Vulnerabilit
1	Content Retrieval	H	H	M	L	M	L	L	-	L
2	Content Storage/Usage	-	-	L	L	M	-	L	-	L
3	Communicati /Messaging	H	H	M	L	M	M	L	-	L
4	Remote Surveillance	H	H	L	L	L	L	L	-	L
5	Remote Control	H	H	H	H	L	L	L	-	L
6	Remote Maintenance	H	H	H	M	L	L	L	L	L

7	Instrument Linkage	M	M	M	L	L	L	L	-	L
8	Networked Game	H	H	H	M	M	L	L	-	L

A. Man-In-The-Middle Attack

In March 2014, a Vulnerability Research Firm named ReVuln, published a video which describes how to employ man-in-the-middle attack to penetrate into the Philips Smart Television through the wireless network that the device connects to. Consequently, the cybercriminal could steal the cookies from the built-in web browser of the television and generate a session hijacking attack to gain access to victim's personal pages [16].

After observing the attack video, one can easily say that TV's configuration for connecting to wireless network through a default hard-coded password is not appropriate. Though it may be convenient for the users, it is quite dangerous if the cybercriminal is also within the range of wireless router. It could even cause more serious aftermath since remote control TV application can easily be downloaded from the Internet. Through such application the hacker could obtain the TV's configuration files and control the TV if he knew the IP address of the television.

B. Denial-of-Service (DOS) Attack

DOS attack is not a new technique and the main attacking mechanism is that a huge amount of packets are generated and sent simultaneously to a targeted appliance. As a consequence, the appliance is either brought down causing permanent crash, or reset to factory setting automatically and making it lose its configuration, stored data and applications.

This kind of attack has recently been reported [17]. A hacker named, Hemanth Joseph, shared on his blog a very simple way to carry a DOS attack on a Pebble Smart Watch. The attacker just needs to know the victim's phone number, Facebook ID, or any other way to interact with the Watch's IP address. Considering that the watch has a function of showing messages received from Facebook, tablet or phone on its screen without character limitation, the attacker can keep on sending many lengthy messages so as to cause a DOS attack on the watch. As a consequence, the Smart Watch could be brought down, reset to factory setting, and lose all of its data as shown in Figure 5.

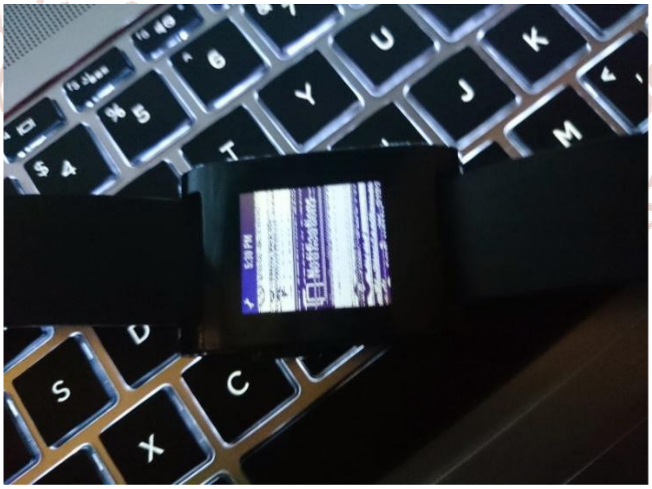


Fig. 5 After DOS attack, the Watch's screen is full of white straight lines, all data and applications are erased because of reset to factory setting (Hemanth Joseph, August 2014)

In addition to the IoT network of home appliances, cyber criminals can also easily penetrate into internet-based-control public appliances. A study published in August 2014 by security researchers from the University of Michigan demonstrates how a series of vital security vulnerabilities in traffic light systems in the US could allow adversaries to quite easily take control of the whole network of at least 100 traffic signals from a single point of access [18].

By carefully examining the above cases, one can easily trace the main reason behind such vulnerability to the fact that those appliances make use of unencrypted wireless radio signals thus can be monitored and compromised by cybercriminals.

C. Thingbot

Thingbot is an abbreviation similar to the word botnet, which itself is a combination of the words “robot” and “network”. In a similar manner, thingbot is comprised of the words “thing” and “robot”.

In order to create a huge botnet network, many computers are compromised and abused by malware to launch cyber-attacks without awareness of internet users. In a very similar manner, thingbot composed of smart home appliances and other devices in IoT network, can be infected and easily turned into slaves by the attackers because of lack of proper security. After knowing the real IP addresses of such compromised devices, it becomes easy for the hacker to generate cyber-attacks such as spamming, or executing Distributed Denial of Service (DDOS) by manipulating them via standards-based network protocols such as Internet Relay Chat (IRC) and Hypertext Transfer Protocol (HTTP), [19].

Although no serious DDOS attack originating from IoT network has yet been reported, it is predictable that DDOS attack scheme from IoT will be on its upward trend in a near future as mentioned in a warning press from Kaspersky blog

[20]. Just to do a small calculation as a reference, let us assume that only 0.01% of the IoT network is compromised by 2020. This will make 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 DDOS attack will be severe enough and should have no difficulty in bringing down a server, or any single host. Moreover, unlike DOS attack which is generated in a pinpointed manner from a single computer or server to flood a target, DDOS attack has an integrated effect of a huge number of compromised devices. Once it occurs, blocking becomes extremely difficult since each compromised element has its own unique IP address.

D. Some Specific Attack Cases in Japan

A DVD/HDD video recorder in Japan, which implemented a proxy server and was acessible without authentication under its default configuration, was used as an open proxy server base for spamming [21], as shown in Figure 6.

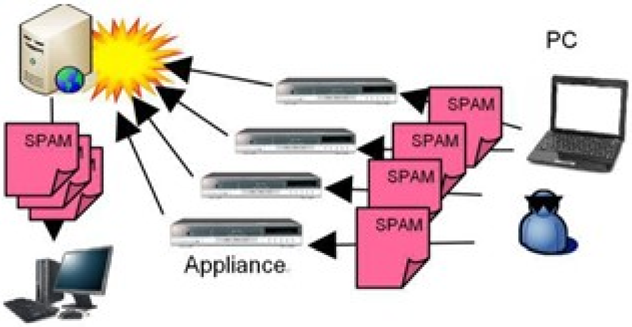


Fig. 6 A spamming incident

In another incident, a music player, which was infected with a virus in the factory, corrupted its user’s computer upon connection [22], as depicted in Figure 7.

In an example of privacy violation, a poorly implemented ‘referrer’ feature in a cellular phone constantly transmitted previously accessed page information even when the page was reached via direct addressing (i.e., non-hyperlink access). The browser flaw caused private information, which may had been required to access a previous page (e.g., user name, password), to be revealed to the next link. It also revealed the user’s favorite sites by transmitting information on a previously accessed page [23]. A Japanese researcher has also successfully exploited buffer overflow vulnerabilities in embedded home routers and managed to remotely gain complete access to peripheral devices [24].

IV. SECURITY IMPLEMENTATION CHALLENGES

Considering the above mentioned attacks aimed at smart appliances, it is apparent that the attack techniques are not new. However, what have been changed are the attack targets, which are the smart home appliances and devices in IoT network. In most cases, the attackers make complete use of the nature of Internet Protocol to have the access to those appliances; and oftentimes, the devices do not have full-functional display or screen so it is really hard for the victims to even detect that they are being attacked and abused internally. Furthermore, different from human-controlled computers, most of smart appliances (such as LED light bulbs smart system, smart refrigerators and smart meters) can easily be accessed due to their 24 hours around-the-clock availability on the Internet. Last but not least, because each appliance is designed to serve only a specific purpose, marketability factors such as low cost, portability, tinier size, etc. make built-in full cryptography capability infeasible in most of such appliances.

Therefore, implementing security on these devices presents more challenges than traditional computer security due to the limited resources (e.g., toy CPUs that cannot handle computationally expensive cryptographic computations and battery power that prohibits long-lasting or high-peak computations). Moreover, because security of a network depends on its weakest link, security of networked smart home appliances would rely on the security of its most primitive home appliance e.g., a coffee maker or a toaster. The problem is further aggravated by the fact that home appliance users cannot be considered as “skilled” administrators, but are instead technology-unaware people in many cases.

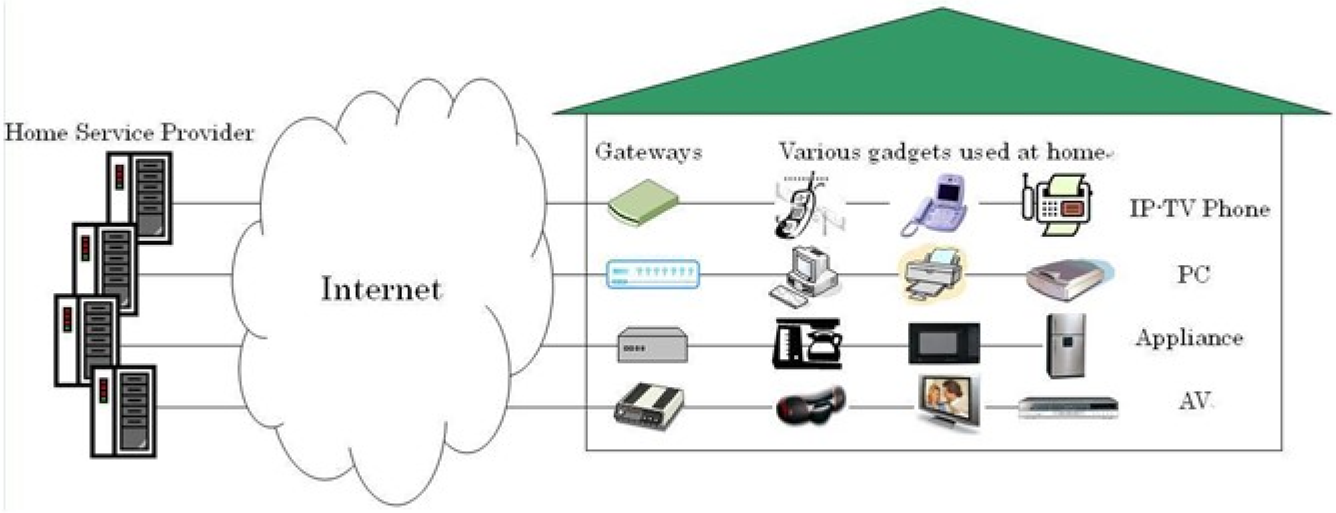


Fig 7: A heterogeneous home network and its service Providers

As such, continuous growth of diverse smart home appliances and development of numerous networking technologies make management of home network security and their associated services complex to both users and service providers, as can be seen from Figure 8.

V. APPROPRIATE SECURITY MODEL

Though it is essential to make the smart home appliance system more secure from aforementioned cyber-attacks, it is obvious that equipping each of them with its own built-in security function against cyber-attacks in the same manner that has been done on personal computers and web servers is not the right approach. In a previous work, the author together with Mr. Hoang proposed implementation of TOR-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 [2][3]. Although such approach can be effective, particularly for technology-aware and expert users, in this paper the author would like to emphasize the concept of universal home gateways and involvement of network operators in their security challenges [8][9] so as to effectively protect technology-unaware people who are the main users of such devices.

In order to come up with a model that can deal with the security requirements of smart appliances, a functionally categorized list of which shown in Table 1 along with a list of common attacks in Table 2 and likelihood of the attacks in Table 3, this section examines a proposed countermeasures shown in Table 4 in a conventional manner for each of the common attack and demonstrates how to tailor them for smart appliances via universal home gateways.

TABLE IV: SUMMARY OF PROPOSED COUNTERMEASURES

No	Common Threat	Proposed Countermeasure
1	User Impersonation	Introduce a certificate mechanism through memory card like devices.
2	Device Impersonation	
3	Service Interruption	Control through network and access mechanism to outside world.
4	Data Alteration	Introduce access control and certificate mechanism.
5	Worm/Virus Infection	Use virus protection software and prepare to handle new vulnerabilities.
6	Phishing/Pharming	Consider using SSL to assure genuineness of displayed sites.
7	Data Wiretapping	Protect communication via IPSEC, SSL/TLS.
8	Firmware Alteration	Use physical access control for update procedure.
9	OS/Software Vulnerability	Educate R&D people on security and conduct product test.

A. Counter Measures

This subsection examines in some details the countermeasures for common attacks listed in Table 4 and recommends how to tailor them for smart appliances.

1) **User/Device Impersonation**: In this scenario, a malicious attacker tries to make an unauthorized access to the appliance and possibly perform some configuration changes on the system. Since the risk level of such an attack is high for smart appliances, a certification mechanism based on standard and public-key infrastructures (PKI) must be used among the entities involved as shown in Figure 9.

Following is a list of required certification mechanisms:

- A standard certification mechanism between user and server.
- An easy-to-use certification mechanism (e.g., through a memory card like device, a built-in speech recognizer, or biometrics recognition method) between the following entities:
    - ○ Appliance ⇔ User o Appliance ⇔ PC o Appliance ⇔ Server
    - ○ Appliance ⇔ Appliance
- An SSL server certificate between the appliance and server

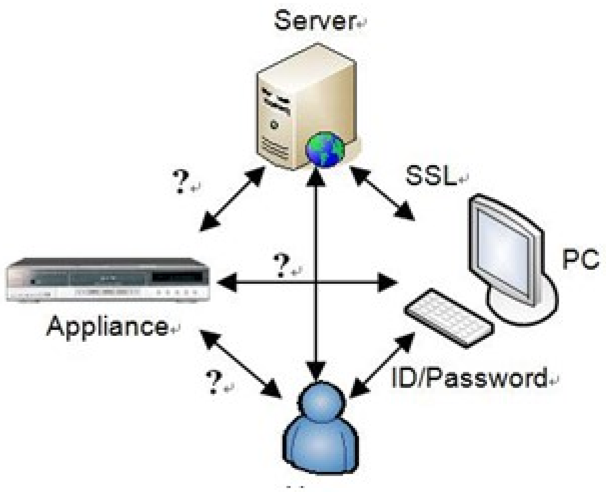


Fig. 8.Use of Certification Mechanism

2) ***Service Interruption:*** Smart home appliance can also be used as a launching pad for a distributed denial of service (DDOS) attack. The risk posed by this threat is medium to high across the various types of appliances and the following methods are recommended as countermeasures:

- Provide a suitable access control for external accesses based on an authentication mechanism.
- The appliance should neither implement redirection nor allow internet access via user input. It should also thoroughly examine the input.
- To prevent attack against a currently accessed site, the appliance should not hard code access address and should make it easily changeable.
- Redundancy and other usual prevention methods against service interruption should be implemented.

3) ***Data Alteration:*** This threat involves misuse of the link between the appliance and PC to alter data or system configuration in an unauthorized manner. The risk posed by this threat is high for remote controlled appliances, medium for networked games and remotely maintained appliances, and low for the remaining items. We can cope with these threats by:

- Implementing certification mechanisms for all appliances.
- Implementing access control based on the authentication method.

Presently most of the network media players that are available in the market do not have an authentication and access control system.

4) ***Infection by Worm or Virus:*** Worm/virus infected appliances can become a secondary source of damage for external access and poses a low to medium risk. We can employ the following methods to safeguard against these infections:

- Virus protection software, which is practical even from resource and operational points of view.
- Use of firewall or intrusion detections system (IDS) to deter infection.

Use of distributed patch programs for established vulnerability information.

5) ***Phishing/Pharming:*** In this scenario, a malicious entity tries to guide the appliance user into a different server for either marketing purposes or try to deceive the user to steal his/her personal information. Except for the

Communication/Messaging appliance, the risk of such an attack is relatively low. Nonetheless an SSL certificate mechanism can be used to prevent its occurrence. For server certificate verification, however, a mechanism wherein the user could clearly verify would be necessary. Furthermore, a design which prevents user information from being sent to the server is required.

6) ***Data Wiretapping*:** Wiretapping is a covert means of monitoring communication, the risk of which is quite low for smart appliances. The following methods can be considered as countermeasures:

- Use IPSEC, TLS or SSL for the communication.
- Use server certification mechanism from access points to the appliance. Or, facilitate the router's VPN or NAPT settings.

7) ***Overwriting Firmware:*** This involves unauthorized external access to the appliance and overwriting of its firmware. Appliances which are remotely maintained are susceptible to this attack. In order to prevent the risk of such attack, the appliance should require some form of direct user operation for its firmware update.

8) ***OS/Software Vulnerabilities;*** In this attack, a malicious user takes advantage of OS/software vulnerabilities and freely executes any code externally. The attacker can also misuse back doors that are left open for R&D and maintenance purposes for their malicious purpose. Although the risk of such an attack is relatively low for the smart appliances, the following methods can be employed to counteract the threat:

- Educate system designers and R&D people on secure development system.
- Familiarize R&D people on the vulnerabilities of back doors that are left open.

- Conduct an exhaustive test on projected vulnerable components during test phase of the product.

B. Discussion

As can be observed from the above, security requirements of smart appliances depend on their functions. To address such functionally dependent security requirements, one has to consider whether a given smart appliance is to be utilized on a stand-alone basis, or several of them are to be used in an interconnected manner in a family area network (FAN) environment. Although it is simpler to meet the security requirements of a single appliance, in reality however, several appliances will be used in an interconnected manner. Therefore, security of the FAN and its underlying technologies, e.g., dedicated wiring, existing power or phone wiring, or wireless, must also be considered. Similarly, while it is ideal to address security requirements of smart appliances by local means and without any need for a background online system, it is not clear what such a security infrastructure will look like at present. Hence, it becomes essential to also employ PKI in this field. Furthermore, because appliance users are technology-unaware people, network operators appear to be in an excellent position to offer the required security services. They handle various network technologies, have experience with PKI and direct access to the users, and are capable of managing large-scale infrastructures *Implementation Guidelines*

It seems that no single vendor/manufacturer may be able to solve the problems faced. Nevertheless, the best way to proceed is to develop the security model around smart home appliances and network components that conform to certain standards. There are standards bodies which specify how to build these devices and meet their various requirements. It is essential to conform to these standards when building, managing and providing services for smart home appliances 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 following subsections briefly explain some of the existing standards that define how to build and manage universally deployable smart home appliances. It also specifies implementation guidelines to set up a prototype system using an open architecture and a modular development scheme.

*1) **Association of Home Appliance Manufacturers**:* The Association of Home Appliance Manufacturers (AHAM) has completed an ANSI standard for generic object models for all of the major white goods in the home, including refrigerators, washing machines, dryers, dishwashers, microwave ovens, room air conditioners and ranges [25]. The AHAM Standard for Connected Home Appliances-Object Modeling (CHA-1) was also created to provide interoperability with higher-level protocols such as Universal Plug and Play (UPnP), Versatile Home Network (VHN) and others. It enables both appliance manufacturers and third-party developers to create new value-added services and features that will allow remote operation and monitoring of appliances from anywhere in the home or even when you are away from home.

*2) **ECHONET Consortium:*** ECHONET develops specifications of home network for networked household appliances, facilities and sensors. ECHONET Consortium has formulated the ECHONET Specification, which can be used to centrally monitor and control smart home appliances that are connected through an ECHONET compatible network interface and a controller [26]. The ECHONET specifications can ensure interoperability between devices of different vendors and realize easy home network at low cost. Also, ECHONET promotes the development of attractive service and application systems using the ECHONET ™ specifications.

ECHONET routers have conversion functions to accommodate home appliances that use different transmission media. The ECHONET, which had previously only supported transmission media such as power lines, low-power radio frequency, and infrared radiation, has come to support other transmission media such as Bluetooth and Ethernet since the release of its version 3.00. Therefore, when there are multiple transmission media in the same domain, the installation of an ECHONET router specified by the ECHONET Specification will allow seamless connection between different types of transmission media.

The ECHONET consortium has over 100 members and its major sponsors are "Hitachi, Ltd.," "Matsushita Electric Industrial Co., Ltd.," "Mitsubishi Electric Corporation," "Sharp Corporation," "Tokyo Electric Power Company, Inc.," and "Toshiba

Corporation." Smart home appliances built by major Japanese companies are ECHONET compliant.

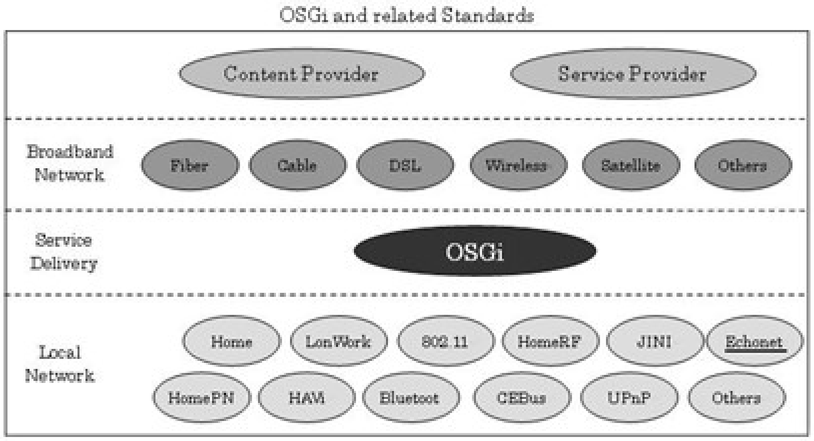


Fig 10: ***OSGi and other Standardized Technologies***

3) Open Services Gateway Initiative Alliance: The OSGi Alliance is an open forum. Their mission is to specify, create, advance, and promote an open service platform for the delivery and management of multiple applications and services to many types of networked devices. Their specifications were initially targeted at residential gateways for the connection of home devices to an external network or for interconnections between the different protocols that are used in devices at homes but have recently been extended to accommodate vehicle, mobile and other environments [28].

About half of its members are based in North America, a third are based in Europe, and the rest are based in the Asia/Pacific region. A number of products developed by member companies are based on the OSGi Service Platform specification [29].

The OSGi specification is not a new protocol technology that replaces existing ones; but rather assumes that multiple protocols could be used within the target device. Its relationship to other standards is schematically shown in Figure 10, where OSGi maps existing local network standards to broadband networks and provides portal services.

Figure 11 shows OSGi architecture which consists of OSGi Framework and a set of bundles [28].

The OSGi Framework provides the basic functionality for executing OSGi bundles which are software components that contain algorithms and protocols for controlling a device. When a bundle is required, it can be downloaded from a server on the network and then executed. This feature makes it possible to download and use the latest and most optimal bundles and allows customization of gateway functions for each user. Since only the bundles that are needed are downloaded and stored, little memory space is required.

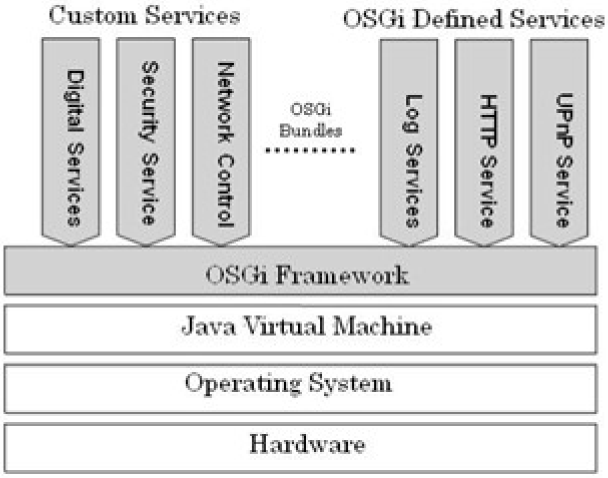


Fig 11:***Structure of OSGi Gateway***

4) Next Generation Gateways: Even with the existence of standardized smart home appliances and standard specifications on how to network them together, a major challenge still falls on capabilities of gateways that connect all of these devices to the network, control the devices, and provide portal capability for using services offered by the external networks, including the Internet. The OSGi specification can be used to implement such gateway capabilities through software component technologies that use the Java language.

There are vendors like ProSyst [30] Bosch Group that use OSGi specification in their modular and open service platform. Companies like Motorola integrate ProSyst's Service Gateway software in their advanced residential products and there are forums like Home Gateway Initiative [31] which define the next generation of residential gateway. There are also forums like UPnP [32] which provides architectural framework for self-configuring, self-describing devices.

The next logical step is to develop an experimental, secured service application for a home network consisting of open standard compliant home appliances and network components that are manufactured by different vendors. Although when using off-the-shelf products, one may need to employ several gateways and a computer as a service gateway, the above described OSGi specification maybe used to answer such problems. The next generation gateway should enable adoption of a uniform approach regardless of underlying technology and manufacturer.

D. A New Security Architecture

Considering the abovementioned security requirements and the various associated challenges, the most effective way to address security issues of the smart appliances are to:

➢ Engage a network operator to build dedicated but nonproprietary home gateways and become the preferred trusted third party.

➢ Motivate internet-enabled smart appliance manufacturers to develop device drivers and application software that can run on such universal home gateways to control and operate the appliances.

This idea is schematically shown in Figure 12, where a universal home gateway, managed by a network operator, functions as an entry point to the networked appliances. In this architecture, all transactions with the smart appliances, whether local or remote, are done via universal home gateways.

1) ***Basic Usage Scenarios:*** There are three basic usage scenarios here; one is access of local services by a user from

within a FAN (e.g., watch a movie using a video recorder located in another room), the other is downloading remote services, and the third one is control of smart appliances interconnected in a FAN environment, by a remote user (e.g., turn on air conditioner from the office).

From within the FAN, users can be authenticated through a common-password-based, log-on approach. Each user's access control information (e.g., no adult movies for kids below 17, or no movies for school-going children after 11 p.m. etc.), which is stored in the universal home gateway, can be used for access granting. To access a remote service site from within the FAN, the universal home gateway authenticates the user through an authentication server, establishes the user's access control privilege, and initiates a secure communication between the remote service provider and the user for the transfer of the requested service. Remotely accessing home appliances is the counterpart of remote service access where the universal home gateway checks and validates a remote user's access control privileges and allows secure communication for legitimate data transfer.

2) ***Desired Features of the Universal Home Gateway****:* In general, universal home gateways, in addition to having the general functions of supporting the underlying FAN technology, and acting as a gateway between a telecom operator's network and the FAN and as an access point to the smart appliances for digital service providers and remote users, are envisioned to have the following security functions:

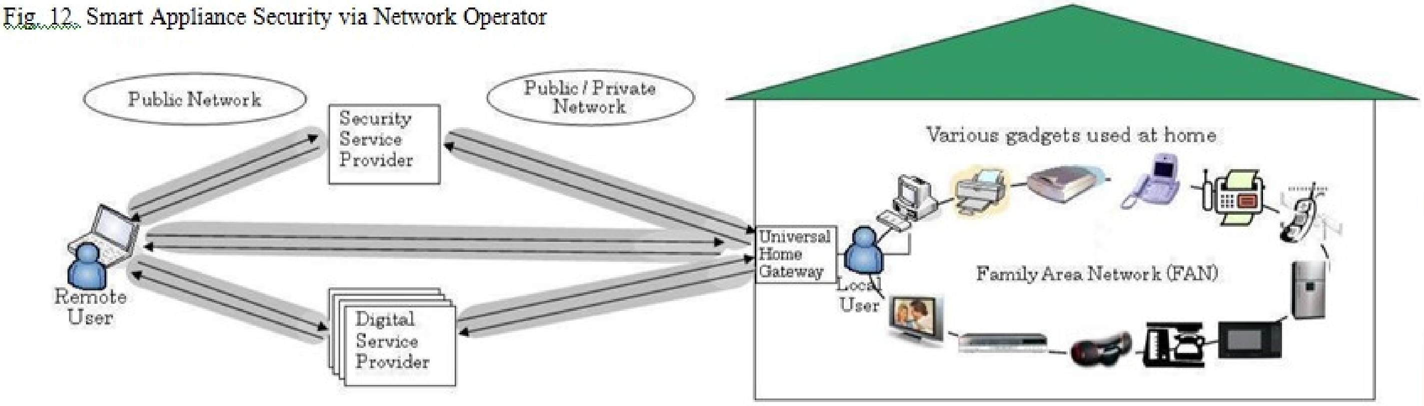
➢ Authenticate a user from within FAN through either a common-password-based log-on approach or by the plugging of a memory card like device, containing user's access control information, into the system. A more user-friendly approach would require a built-in speech recognizer or biometrics recognition method.

➢ Act as a security server and maintain each user's access control information (security attributes and the basic key for communication with remote services).

➢ Provide secure communication and deal with security issues on behalf of the appliance users. Enable remotemanagement services through providers, intermediaries, and network operators. Allow network operators to use universal home gateways to authenticate their users, or bill them on behalf of a third party e.g., service providers.

- ➢ Detect connection of a new appliance to the FAN and prompt users to insert its manufacturer supplied driver/application software. Such a plug and play type auto configuration mode, however, should be manually selectable (i.e., be enabled when needed) in order to provide an added security for wireless FAN and prevent arbitrary connection from the neighborhood.

Fig. 12. Smart Appliance Security via Network Operator



- ➢ Automatically disable, via software selectable functions, an appliance when it is detached from the FAN and auto configure when a previously detached appliance is re-connected.

- ➢ Be equipped with firewall and virus protection software Such functionalities could meet security measures which were discussed earlier. Moreover, because security requirements are handled via central universal home gateways, it could offset resource limitations of individual smart appliances.

3) Existing and Envisioned Technologies: Although at present there are some vendors who market their own brand of smart appliances, which are equipped with a central controller that links the appliances together in a FAN environment and offer limited security and exclusive digital services [33][34], history shows that such propriety approaches are prone to fail. Similarly, while some researchers, e.g., those at the University of Illinois [35], have done ingenious work in coming up with protocols and schemes that could provide security for smart home appliances, a universally deployable, user-friendly system, which is acceptable to a wide range of users, is the key issue.

V. CONCLUSION

This paper demonstrated how commonly used communication scheme and information retrieval which are carried out via Internet using numerous types of smart devices, can turn the Internet into a very dangerous platform. After providing some introductory information and necessary background knowledge, it examined a number of security incidents that are carried out via smart devices, identified existing challenges and showed that the security requirements of smart appliances depend on their functions. The security requirements of the appliances, categorized based on their functions, were then identified and appropriate solution for each category was proposed. PKI was identified as an essential security component and easy-to-use authentication mechanisms were recommended. It considered compliance with existing standards and liaise with appropriate for a to downstream new requirements important when trying to address security requirements of smart home appliances. It argued that successive security implementation involves cooperation of manufacturers, network operators and service providers. An architecture wherein security issues are managed through universal home gateways by network operators in a product based fashion is proposed and manufacturers and service providers are recommended to adapt the technology, in order to offset resource limitations of individual smart appliances and make their security issues straightforward to ordinary users.

REFERENCES

1. Chris Drake (2013). *FireHost Detects Surge in SQL Injection for Q3 2013 and Cross-Site Scripting is Rising.* Retrieved October 22, 2013, from

2. Hoang Nguyen Phong, Davar Pishva (2014). Anonymous communication and its importance in

social networking. In *Proceeding of the 16th International Conference on Advanced Communication Technology* (vol. 1, pp. 34-39).

3. Hoang Nguyen Phong, Davar Pishva (2014). A TOR-Based Anonymous Communication Approach to Secure Smart Home Appliances. *ICACT Transactions on Advanced Communications Technology (TACT),* 3(5), 517-525.

4. Statista (2015). *Leading social networks worldwide as of March 2015, ranked by number of active users (in millions)*. Retrieved June 18, 2015, from http://www.statista.com/statistics/272014/global-social-networks-ran_ked-by-number-of-users/.

5. Kimberlee Morrison (2015). *The Growth of Social Media: From Passing Trend to International Obsession*. Retrieved June 18, 2015, from http://www.adweek.com/socialtimes/the-growth-of-social-media-from________-trend-to-obsession-infographic/142323.

6. Jeffbullas (2014). *22 Social Media Facts and Statistics You Should Know in 2014*. Retrieved June 18, 2015, from http://www.jeffbullas.com/2014/01/17/20-social-media-facts-and-stat___istics-you-should-know-in-2014/.

7. Herper, Matthew (2003, Febuary). *Emerging Technologies: 'Smart' Kitchens A Long Way Off*. Paper presented at Forbes.

8. D. Pishva, K. Takeda (2006). 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).

9. D. Pishva, K. Takeda (2008). A Product Based Security Model for Smart Home Appliances, *IEEE Aerospace and Electronics System Magazine,* 23(10), 32-41.

10. Staff (2003). *Wired News: Caregiver Tech Slowly Evolves*, Associated Press, September 2003.

11. Carrie MacGillivray, Vernon Turner, Denise Lund (2014). *Worldwide Internet of Things (IoT) 2013–2020 Forecast: Billions of Things, Trillions of Dollars.* Retrieved January 2014, from International Data Corporation: http://www.idc.com/getdoc.jsp?containerId=243661.

12. Angelia, D. Pishva (2013). Online Advertising and its Security and Privacy Concerns. In *Proceeding of the 15th International Conference on Advanced Communication Technology* (vol. 1, pp. 372-377).

13. Metzger, Miriam J. (2007). Communication Privacy Management in Electronic Commerce. *Journal of Computer-Mediated Communication*, 12(2), 335–361. Retrieved June 18, 2015, from http://dx.doi.org/10.1111/j.1083-6101.2007.00328.x.

14. Schwartz, M. J. (2011, March 31). *Schwartz On Security: Online Privacy Battles Advertising Profits*. Retrieved June 7, 2015, from

15. Information Week: http://www.informationweek.com/news/security/privacy/229400615.

16. Revuln (2014). *Having fun via WIFI with Philips Smart TV*. Retrieved July 8, 2015, from http://vimeo.com/90138302.

17. Hemanth Joseph (2014). *Dosing Pebble Smart Watch And Thus Deleting All Data Remotely*. Retrieved August 2014, from http://www.whitehatpages.com/2014/08/dosing-pebble-smartwatch-a_nd-thus.html.

18. Ghena, B., Beyer, W., Hillaker, A. Pevarnek, J., & Halderman, J. A. (2014). Green lights forever: analyzing the security of traffic infrastructure. In *Proceedings of the 8th USENIX conference on Offensive Technologies* (vol. 1, pp. 7-7). USENIX Association.

19. Ramneek Puri (2003, August). *Bots &; Botnet: An Overview*. Retrieved July 8, 2015, from SANS Institute InfoSec Reading Room: http://www.sans.org/reading-room/whitepapers/malicious/bots-botnet________-overview-1299.

20. Brian Donohue, Beware (2014). *The Thingbot!* Retrieved January 2014, from Kaspersky Lab: https://blog.kaspersky.com/beware-the-thingbot/.

21. Katagi, Kizu (2004). *Vulnerability of Toshiba's RD Series HDD-DVD Recorder 'Stepping-stone' for Danger*, Retrieved (in Japanese) June 18, 2015, from Internet Watch: http://internet.watch.impress.co.jp/cda/news/2004/10/06/4882.html.

22. Creative (2004). *A Report to Customers on the Issue of 'Creative Zen Neeon' Digital Audio Player and its Response.* Press Release (in Japanese) retrieved June 18, 2015, from http://jp.creative.com/corporate/pressroom/releases/welcome.asp?pid_=12181.

23. AU Announcement (2005). *EZweb Browser's Home Page URL Transmittal on AU and TU-KA Mobile Phones.* Retrieved (in Japanese) December 2005, from KDDI News: http://www.au.kddi.com/news/topics/au_topics_index20051209.html.

24. OSGi Alliance (2015), *OSGi and the Internet of Things (IoT)*. Retrieved June 18, 2015, from http://www.osgi.org/Main/HomePage.

25. OSGi Service Platform Products (2015). *OSGi Markets and Solutions.* Retrieved July 8, 2015, from http://www.osgi.org/products/products.asp?section=3.

26. ProSyst Bosch Group (2015). *Internet of Things*. Retrieved July 8, 2015, from http://www.prosyst.com/startseite/.

27. HGI (2006). *Home Gateway Initiative.* Retrieved January 2006, from http://www.homegateway.org/aboutus/vision.html.

28. UPnP Forum (2008). *UPnP Product Scenarios.* Retrieved January 2008, from http://www.upnp.org/.

29. Kato Yoshimi (2005). *Addressing Security Requirements of Network Enabled Home Appliances, Next Generation IP Infrastructure Group Report (WG3-1),* Retrieved (in Japanese) December 2005, from Ministry of Internal Affairs and Communication (MIC): http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/jise_ip/pdf_/050217_1_s1.pdf.

30. Tezuka Satoru (2005, February). *Information Appliance System Authentication Technology, Next Generation IP Infrastructure Group Report (WG3-2).* Retrieved (in Japanese) January, 2006, from Ministry

31. of Internal Affairs and Communication (MIC): http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/jise_ip/pdf_/050217_1_s2.pdf.

32. J. Al-Muhtadi, M. Anand, M.D. Mickunas, R. Campbell (2000). Secure Smart Homes Using Jini and UIUC SESAME. In *Proceeding of 16th Annual Computer Security Applications Conference* (vol. 1, pp. 77).