A TOR-Based Anonymous Communication Approach to Secure Smart Home Appliances

Nguyen Phong HOANG, Davar PISHVA

Institute of Information & Communications Technology, APU

(Ritsumeikan Asia Pacific University), Japan

hoang.phong.37e@st.kyoto-u.ac.jp, dpishva@apu.ac.jp, **Fax: +81 977 78 1001, Tel: +81 977 78 1000**

***Abstract*— Digital information has become a social infrastructure and with the expansion of the Internet, 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, smart LED light bulbs system, 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. There are, however, serious challenges which need to be addressed as these tiny devices are designed for specific functions and lack processing capacity required for most security software. This research explores how these internet-enabled smart devices can be turned into very dangerous spots for distributed attacks purposes by cybercriminals for various ill intensions in a pinpointed manner. It then introduces a new approach to deal with such problems by taking advantage of the anonymous communication of the Onion Router (hereafter: TOR). It compares pros and cons of using anonymous communication scheme and justifies it be an efficient countermeasure to most attack scenarios.**

***Keyword*—Smart Appliances, the Internet of Things, Security, Anonymous Communication, the Onion Router (TOR)**

I. INTRODUCTION

NOWADAYS, thanks to the impressive achievement of material science especially in semiconductor materials and nanomaterials, all the electronic devices are getting smaller in size, and microprocessors can be found in most appliances. 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, such as 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' has become the new buzzword that we have kept on hearing in recent years, for example, in 'smart' homes, 'smart' kitchens, 'smart' ovens, 'smart' refrigerators, etc. [1]. Table 1 indicates functional classification of smart home appliances. 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 [2]. 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 [3]. 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 Equipments
8	Networked Game	Family Type Game Machine

Connecting smart home appliances to the Internet, however, 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. 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.

TABLE II
A LIST OF COMMON ATTACKS

No	Common Threat	Example of an Attack
1	User Impersonation	Impersonation using password
2	Device	Impersonation of a device using its faulty

Manuscript received on September 9, 2014. This work is a follow up of a presentation done at the 16th International Conference on Advanced Communication Technology which received Outstanding Paper Award.

Nguyen Phong HOANG is a graduate student at the Graduate School of Informatics at Kyoto University Japan (hoang.phong.37e@ st.kyoto-u.ac.jp).

Davar Pishva is a professor in ICT at Ritsumeikan Asia Pacific University (APU) Japan (corresponding author: +81-977-78-1000, fax: +81-977-78-1001, e-mail:dpishva@apu.ac.jp).

ISBN 978-89-968650-5-6

	Impersonation	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

II. Typical Attack Cases On Smart Appliances

In a previous research, the authors showed 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 [4]. 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 and the rest of the section briefly discusses some of the 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

No.	Common Threat / Function	1. User Impersonation	2. Device Impersonation	3. Service Interruption	4. Data Alteration	5. Worm/Virus Infection	6. Phishing/Pharming	7. Data Wiretapping	8. Firmware Alteration	9. OS/Software Vulnerability
1.	Content Retrieval	H	H	M	L	M	L	L	-	L
2.	Content Storage/Usage	-	-	L	L	M	-	L	-	L
3.	Communication /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 cyber criminal 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 [5].

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 cyber criminal 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 (August 2014) [6]. 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 Fig. 1:

Fig. 1. 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 [6].

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 [7].

By carefully examining the above cases, the authors found that the main reason behind such vulnerability was because those appliances make use of unencrypted wireless radio signals thus simply monitored and compromised by cybercriminals.

C. Thingbot

Thingbot is derived from 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, botnet composed of smart home appliances and

ISBN 978-89-968650-5-6

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) [8].

Although no serious DDOS attack originating from IoT network has been reported as of this moment, 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 [9]. 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 is 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 accessible without authentication under its default configuration, was used as an open proxy server base for spamming [10], as shown in Fig. 2. In another incident, a music player, which was infected with a virus in the factory, corrupted its user's computer upon connection [11]. In an example of privacy violation, a poorly implemented 'referer' 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 [12].

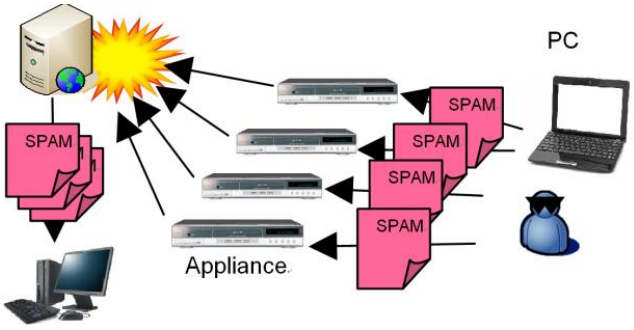

Fig. 2. A spamming incident

III. Security Implementation Challenges

Continuous growth of diverse smart home appliances and development of numerous networking technologies make management of home network security and their associated

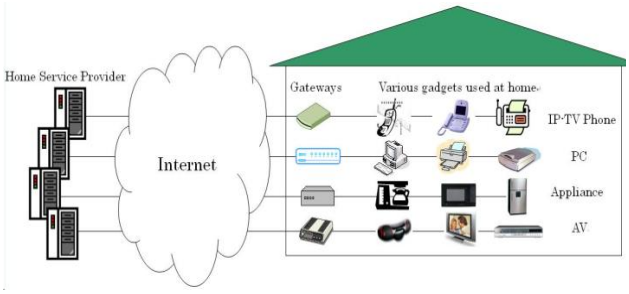

Fig. 3. A heterogeneous home network and its service Providers

services complex to both users and service providers, as can be seen from Fig. 3.

Implementing security on these devices also 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). Furthermore, 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.

In order to cope up with such security challenges, the corresponding author in a previous work proposed the idea of handling them through network operator. The recommendation was to engage a network operator to build dedicated but nonproprietary home gateways and become the preferred trusted third party and 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 Fig. 4, 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. [13][14].

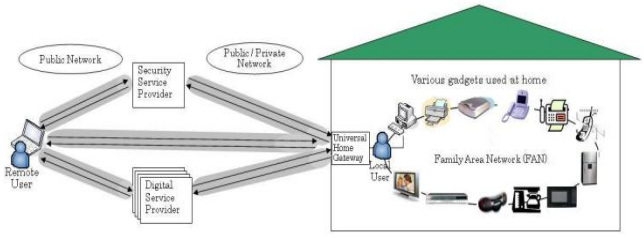

Fig. 4. Smart home appliance security via network operator

Unfortunately, however, as of today no such universal home gateway has yet been manufactured, without which it becomes impossible for a network operator to take the role of trusted third party.

IV. Motivation Behind The Study

In a recent previous work on anonymous communication and its application to social networking, the authors conducted some experiments to test the confidentiality level and anonymity level of several anonymous tools such as

ISBN 978-89-968650-5-6

Incognito Mode in Chrome browser, proxy server, virtual private network (VPN), and TOR. In conclusion, the study was able to point out some significant pros and cons in each particular anonymity tool. Additionally, the authors recognized that TOR is indeed the strongest anonymous tool compared with other tools [4]. This is mainly because "Tor Browser Bundle" operates as an internet browser which anonymizes all internet surfing activities that pass through and sends them to the TOR network. After concluding that TOR is a powerful tool for protecting internet user's privacy from being compromised by most contemporary attack techniques and learning about a new-style of attack; reported by Proofpoint, an innovative security-as-a-service vendor, in January 2014, the authors realized that smart appliances' security have not yet been realized via network operator and TOR may play an effective role in this endeavor.

The Proofpoint's report was about cyber attack involving commonly used smart home appliances and in its press release, the company stated: "The attack that Proofpoint observed and profiled occurred between December 23, 2013 and January 6, 2014, and featured waves of malicious email, typically sent in bursts of 100,000, three times per day, targeting Enterprises and individuals worldwide. More than 25 percent of the volume was sent by things that were not conventional laptops, desktop computers or mobile devices; instead, the emails were sent by daily consumer gadgets such as compromised home-networking routers, connected multi-media centers, televisions and at least one refrigerator. No more than 10 emails were initiated from any single IP address, making the attack difficult to block based on location" [15]. Thus, this study is motivated by the aforementioned scenario and our relevant previous work. In this paper, the authors will demonstrate how TOR can help remedy the recent security problems in smart home appliance system.

V. TOR – A New Approach To Secure Smart Home Appliances

Taking into consideration all of the aforementioned cyber attack cases 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.

While the previously proposed concept of universal home gateways and involvement of network operators in security challenges of such appliances is not achieved, it is going to be difficult for producers to produce economically feasible, safe and tiny smart appliances. This is because for instance, an LED in smart light bulb systems would become unaffordable to buy if cryptography process and sufficient memory for encrypting information were built into each single bulb. Hence, it is certainly not the right approach to equip all smart appliances with built-in security function against cyber attacks in the same manner that has been done on personal computers and web servers.

An intermediate solution, which is proposed in this paper, is to make use of TOR and this section will demonstrate how to utilize TOR to make the IoT network more robust and secure against most of the contemporary cyber attacks.

A. Some Important Properties of TOR

Before moving into detailed technical demonstrations, it is necessary to briefly introduce some important properties of TOR. In the previous research we already described its internal working mechanism and showed that it is indeed an ideal anonymous communication tool which employs asymmetric cryptography, takes advantage of public-key encryption and transmits data from a source to a destination through a randomly selected route of multiple nodes [4]. Raw data having its destination IP address encrypted and re-encrypted with public key of the selected nodes, something which resembles an onion ring where in each layer is a re-encrypted version of an encrypted data by the public key of the node. In the transmission process, each node decrypts a layer of the encryption to extract the next layer's IP address, an operation resembling an onion-peeling-off process. The final node decrypts the last layer of the encryption and sends the original data to its real destination without revealing or even knowing its original sender [16].

In this paper, we would like to expand the research into a deeper level of TOR and employ its subproject, The Amnesic Incognito Live System (Hereafter: Tails); a live operating system, Debian-based Linux distribution which can run on almost any CPU based gadget like DVD, USB stick, or SD card [17].

Usually ordinary internet users often use TOR as an internet browser and the Tor Browser Bundle is one of its most well-known subprojects. While the Tor Browser Bundle operates as an anonymous browser where only those surfing activities done within the browser are anonymized, Tails acts as a complete stand-alone operating system causing not only net surfing activities in the browser but also all of the networking activities running within other applications and operating system be anonymized by forcing them to pass through TOR network before going out to the public internet environment. Through this mechanism, the data transmission process gets firmly secured because of the multilayer asymmetric cryptography feature of TOR. As the process also encrypts the destination IP address, real IP address of the device also gets hidden from the adversaries. Thus we have taken advantage of these two features of Tails operating system and investigated its potential for addressing the security problems of the IoT network.

B. Test Platform Configuration and Monitoring Process

In this section we describe how to configure TOR to secure smart home appliance system. The main idea is to set up Tails to be the central control gateway thus forcing all the transmitted data packets of smart home appliances to pass

ISBN 978-89-968650-5-6

through before going out to the public internet environment. Since no universal home gateway has yet been produced, we made use of existing devices and software to create a new system and used it to conduct the experiment as illustrated in Fig. 5:

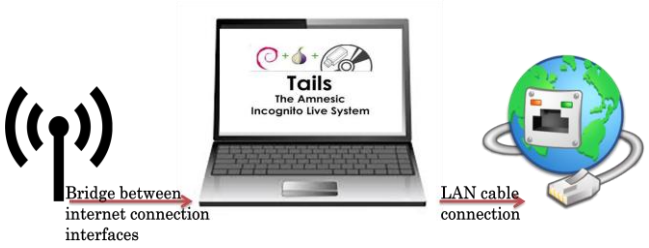

Fig. 5. Setting up a TOR network for smart home appliances

Our experimental system consisted of a laptop with WiFi internet connection interface, local area network (LAN) cable connection interface and a Tails-contained storage device (such as DVD, USB stick, or SD card). Initially we loaded Tails into the laptop, configured the LAN cable to be its main interface to the Internet and reserved WiFi interface as an Access Point for smart home appliances. The LAN and WiFi interfaces were then bridged to each other so that the Internet connection from LAN cable is shared with WiFi interface to form the Access Point. All the smart home appliances were then configured to connect through this Access Point instead of directly connecting to the Internet.

This way, because of the built-in anonymity feature of Tails, all the networking activities passing via laptop's WiFi Access Point are anonymized and multilayer-encrypted by public-key cryptography before being sent through the TOR nodes network to their real destinations. Fig. 6 shows the operating mechanism of this process.

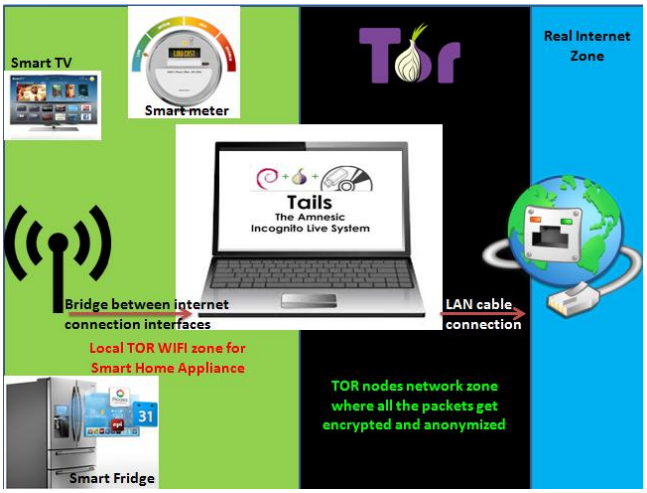

Fig. 6. The overview of TOR WiFi network for smart home appliances

Once the Internet connection is available, Tails immediately send a request to TOR directory server node to obtain the list of other nodes in TOR network and establish a sufficient amount of circuits for routing data through the TOR network anonymously. It is easy to monitor how Tails forms the available TOR nodes to create circuits by means of a built-in tool called *TOR network map*. Fig. 7 shows a series of random routing paths that Tails forms to transmit data through the TOR network.

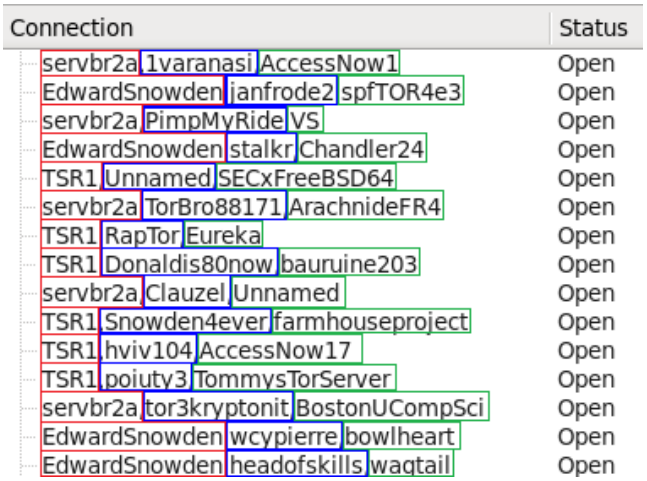

Fig. 7. A list of TOR circuits obtained from TOR network map tool

The data transmission process is done anonymously through distributed TOR nodes system operated by a huge number of volunteers around the world. As indicated in Fig. 7, each circuit has 3 nodes called entry, intermediate and exit which are highlighted in red, blue and green respectively. The entry nodes (in this case: *servbr2a, EdwardSnowden, TSR1*) are rarely changed. Tails sometimes reuses the same set of entry nodes in a working session, while the intermediate and exit nodes keep changing from circuit to circuit. This is because the entry node is the first node where the connection gets into the TOR network. As it is vital to make the connection steady and robust as much as possible, TOR directory nodes often have longer uptime than other voluntary nodes (in this case: the directory node *servbr2a* has 118-day uptime). In order to provide more thorough details, we collected information about all the nodes shown in Fig. 7, the results of which are indicated in Fig. 8.

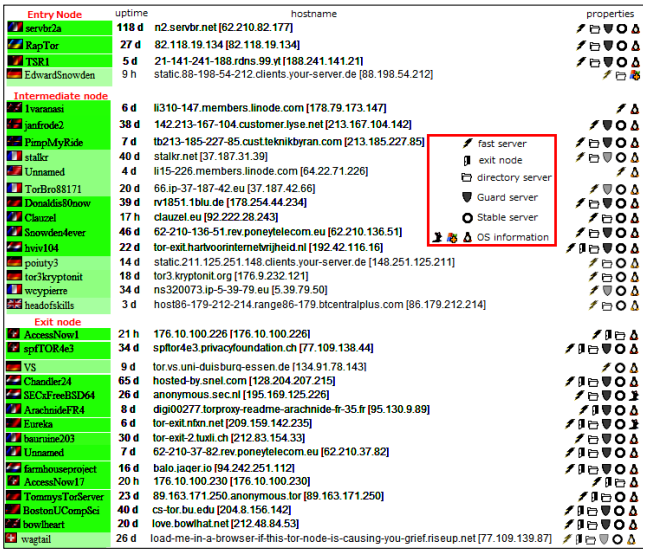

Fig. 8. List of TOR nodes in a random working session of Tails with their detailed information (country, uptime, IP address, sever type and Operating System information)

TOR nodes of Fig. 8 are obtained from the TOR-network monitoring website named http://www.torstatus.blutmagie.de, which contains detailed information of the available TOR nodes. In a similar manner, Tails user can check through which node the data packets will be transmitted and decide to either let the data pass through a

ISBN 978-89-968650-5-6

particular route or not. For instance, by examining the uptime and properties of the entry node *EdwardSnowden,* an experienced Tails user may not want his/her data pass through that node. This is because its uptime is not long; it is not a Guard and Stable node, hence, vulnerable to compromise because the data could be dropped during transmission process and result in leaking the identity information of Tails users. To prevent data transmission through such an unwanted circuit, the user just needs to right click on it from *connection window*, choose *Delete circuit*, and then Tails will remove it from the list.

Another noteworthy feature of this Tails is that all data are sent and received in a distributed manner, a particular case of which is shown in Fig. 9.

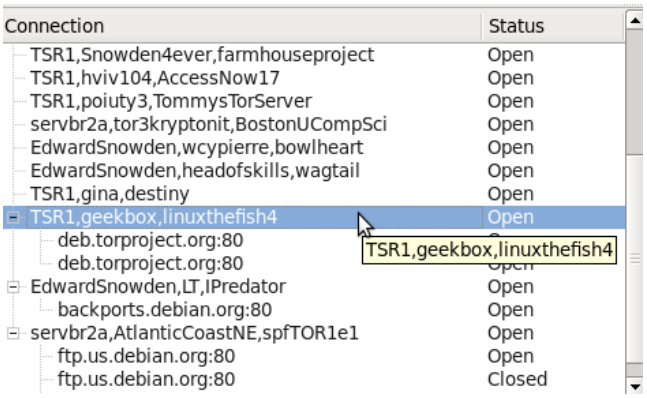

Fig. 9. Data Transmission is done in distributed manner by means of dispersed voluntary TOR nodes around the world

For example, in the same working session of Tails, we executed *sudo apt-get update* in *root terminal* to run an update task for the Debian operating system. Although it is a single task in which the system communicates with Debian database servers to update newest functions for Tails, the task gets divided into many subtasks and communicates with Debian servers through separate streams as described technically in Tor proposal 171 [18]. The update task shown on Fig. 9 is done in distributed manner through the following 3 separate circuits:

1. *TSR1, geekbox, linuxthefish*
2. *EdwardSnowden, LT, IPredator*
3. *servbr2a, Atlantic CoastNE, spfTOR1e1*

As a result, there is no way for any single node in the circuits, including the LAN admin or Debian servers' admin nodes to have all the information about transmission route, original IP address of TOR user, and the raw data. This means that each component in the system can only know a part of the whole transmission process. Thanks to this unique working mechanism of Tails, altering transmission route frequently in about every 10 minutes and providing maximal anonymity for Tails user. Therefore, if functionality of the system shown in Fig. 5 is constructed as a Tails-embedded router, it is certainly going to be a promising solution for securing smart home appliance system.

Last but not least, *MAC address spoofing* feature is also an indispensable feature of Tails. Although MAC address is not sent over the Internet and only used within the local network, there is a risk of an internal attack from an adversary who is also in the same network. Tails also fakes MAC address of the system, laptop in our example, so as to protect the system from internal attack and prevent local network admin or other users in the same LAN to monitor Tails-installed device from within.

To verify the *MAC address spoofing* feature, we used a network tool called Fing [19] and monitored the LAN to where Tails-based laptop was connected. As shown in Fig. 10, devices without Tails-installed operating system could be easily traced thus revealing their names, real interfaces and MAC addresses; while Tails-installed laptop changed its MAC address every time the machine got connected again to the local network and did not leak its name, thus made monitoring hard as indicated in the highlighted red section of Fig 10.

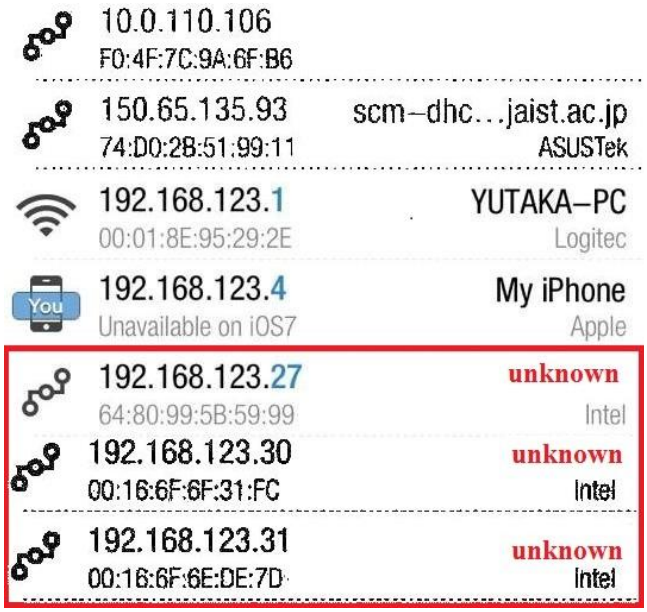

Fig. 10. MAC address spoofing feature of Tails

C. Testing with Multimedia Transmission

In this section we demonstrates feasibility of transmitting multimedia data over the TOR-based network using Sony BRAVIA smart television (hereafter: the smart TV) as a typical testing object, shown in Fig. 11:

Fig. 11. Testing object - Smart Sony BRAVIA television

The smart TV was intentionally selected for the experiment since it is integrated with many applications and can be considered as a typical representative of other smart appliances as well. Apart from the function of a traditional television, the smart TV has also many other multimedia applications and internet-based services such as high

ISBN 978-89-968650-5-6

definition (hereafter: HD) movies from the Internet, online music, net surfing, social networking and so on as shown in Fig. 11.

Considering that TOR only supports the Transmission Control Protocol (hereafter: TCP), as stated in TOR project documentation [16], we had to first examine which protocol is mainly used in the smart TV to communicate with the Internet and ensure proper rerouting of its data stream through the TOR network. To monitor the data transmission process of the smart TV, we used a network monitoring tool, called Microsoft Network Monitor, to tap to the connection channel between the smart TV and the Internet. We then run all the essential applications, ranging from Youtube, Sony online HD movies service to gaming applications, at the TV side and Fig. 12 shows captured result at the network monitoring tool side.

Source	Destination	Protocol	Description
r5.sn-xgmnpoxuopp-ogue.googlevideo.com	192.168.123.28	TCP	TCP:[Continuation to #15198]Flags=.....
r5.sn-xgmnpoxuopp-ogue.googlevideo.com	192.168.123.28	TCP	TCP:[Continuation to #15198]Flags=.....
192.168.123.28	r5.sn-xgmnpoxuopp-ogue.googlevideo.com	TCP	TCP:Flags=...A...., SrcPort=40156, Ds...
192.168.123.28	r5.sn-xgmnpoxuopp-ogue.googlevideo.com	TCP	TCP:Flags=...A...., SrcPort=40156, Ds...
192.168.123.28	bivl.np.ac.playstation.net	TCP	TCP:Flags=.....S., SrcPort=43382, Ds...
ssm1.internet.sony.tv	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTPS(443...
192.168.123.28	ssm1.internet.sony.tv	TCP	TCP:Flags=...A...., SrcPort=47781, Ds...
ssm1.internet.sony.tv	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTPS(443...
bivl.np.ac.playstation.net	192.168.123.28	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443...
192.168.123.28	bivl.np.ac.playstation.net	TCP	TCP:Flags=...A...., SrcPort=43382, Ds...
23.32.241.24	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTP(80),...
tv.app.bs.sony.jp	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTP(80),...
23.32.241.24	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTP(80),...
tv.app.bs.sony.jp	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTP(80),...
23.32.241.24	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTP(80),...
applicast.jp.sonystyle.com	192.168.123.28	TCP	TCP:Flags=...A...F, SrcPort=HTTP(80),...
192.168.123.28	23.32.241.24	TCP	TCP:Flags=...A...., SrcPort=40495, Ds...
192.168.123.28	23.32.241.24	TCP	TCP:Flags=...A...., SrcPort=40496, Ds...
192.168.123.28	23.32.241.24	TCP	TCP:Flags=...A...., SrcPort=40497, Ds...
192.168.123.28	tv.app.bs.sony.jp	TCP	TCP:Flags=...A...., SrcPort=59071, Ds...
192.168.123.28	23.32.241.24	TCP	TCP:Flags=...A...., SrcPort=40498, Ds...
192.168.123.28	tv.app.bs.sony.jp	TCP	TCP:Flags=...A...., SrcPort=59072, Ds...
192.168.123.28	23.32.241.24	TCP	TCP:Flags=...A...., SrcPort=40499, Ds...
192.168.123.28	applicast.jp.sonystyle.com	TCP	TCP:Flags=...A...., SrcPort=58565, Ds...

Fig. 12. Data stream between Sony BRAVIA smart television and multimedia resources

As can be seen in the captured result, most of applications communicate with the Internet via TCP. In this particular case, Youtube communicates with *r5.sn-xgmnpoxuopp-ogue.googlevideo.com* to load videos via TCP; or other Sony-based services like online HD movies, gaming applications communicate with Sony's service-providing servers such as *bivl.np.ac.playstation.net, ssm1.internet.sony.tv, applicast.jp.sonystyle.jp,* and *tv.app.bs.sony.jp* using TCP. It is evident that such TCP-based data streams can be routed through the TOR network in order to make the connection more secure. Though the Internet connection speed may theoretically get slower and adversely affect quality of the services when routed through the TOR network since it has to pass through 3 TOR nodes before reaching the final destination, the experiment showed that all the above mentioned applications and Sony-based services still works smoothly over the TOR network. Despite the fact that buffering speed of HD movies and videos from Youtube was not as fast as the normal and direct connection environment, the videos from Youtube server still loaded with an acceptable speed and caused no interruption in between.

D. Testing with Voice-over-Internet Protocol Applications

This section examines potential of using the TOR-based network for voice over IP application like Skype. Unlike Youtube videos and HD movies which are TCP-based applications, Skype which is a voice over IP service and instant messaging client software developed by Microsoft, operates based on The User Datagram Protocol (hereafter: UDP). It is one of the vital applications in the application suite of the smart TV, but has to operate in a real-time manner. In other words, the transmitted data packets have really short time-to-live and need to hit their final destination before the time-to-live is over. Hence, applications like Skype, LINE and Viber conventionally operate based on the UDP.

Our initial attempt to launch Skype via TOR network in the same manner as other TCP-based applications over the Internet having a regular speed failed mainly because of the short time-to-live duration of UDP packets. In order to prove that TOR-based network could also work with voice over IP application, we conducted the next phase of our experiment at Japan Advanced Institute of Science and Technology (hereafter: JAIST) where the Internet connection speed is 10 Gbit/s, one of the highest in Japan [20]. Fig. 13 shows the setup of our experiment where at one side, we connected the smart TV to the Internet via the Tails-installed laptop and at the other side; a regular Windows equipped with Skype was connected to JAIST network. At both side, Microsoft Network Monitor was used to tap to the transmission channels.

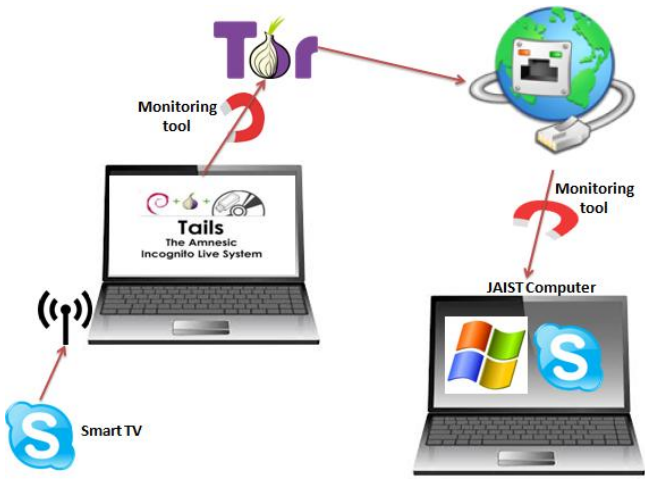

Fig. 13. Testing VoIP over TOR network

We then made a call from the Skype account in the smart TV to the Skype account in the JAIST computer while monitoring the transmission process at both sides by two separate network monitoring tools. This time, the Tails-installed laptop instead of dropping out the UDP connection, encrypted and encapsulated all the UPD packets of Skype into TCP packets and sent them through the TOR network as shown in the captured screen of its monitoring tool in Fig. 14, where *192.168.123.27* is the local IP address of the Tails-installed laptop, and *62.210.137.27*, *188.138.1.229* and *94.23.105.27* are the IP addresses of the entry TOR nodes at that time.

Source	Destination	Protocol	Description	Time Date Local Adjusted
62.210.137.230	192.168.123.27	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
192.168.123.27	62.210.137.230	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
62.210.137.230	192.168.123.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
192.168.123.27	62.210.137.230	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
188.138.1.229	192.168.123.27	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
192.168.123.27	188.138.1.229	TCP	TCP:[Continuation to #...	1:26:04 PM 8/27/2014
188.138.1.229	192.168.123.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
188.138.1.229	192.168.123.27	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
94.23.105.27	192.168.123.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
192.168.123.27	94.23.105.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
62.210.137.230	192.168.123.27	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
192.168.123.27	188.138.1.229	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
192.168.123.27	62.210.137.230	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
62.210.137.230	192.168.123.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:04 PM 8/27/2014
192.168.123.27	62.210.137.230	TCP	TCP:Flags=...A...., SrcP...	1:26:04 PM 8/27/2014
188.138.1.229	192.168.123.27	TCP	TCP:Flags=...A...., SrcP...	1:26:05 PM 8/27/2014
192.168.123.27	188.138.1.229	TLS	TLS:TLS Rec Layer-1 SS...	1:26:05 PM 8/27/2014
94.23.105.27	192.168.123.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:05 PM 8/27/2014
192.168.123.27	94.23.105.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:05 PM 8/27/2014
188.138.1.229	192.168.123.27	TLS	TLS:TLS Rec Layer-1 SS...	1:26:05 PM 8/27/2014

Fig. 14. Tails-installed PC encapsulates UPD packet inside TCP packet

ISBN 978-89-968650-5-6

At the exit node of the TOR, the TCP packets got decrypted thus disclosing the original UDP packets and sending them to the final destination. Consequently, at JAIST computer side the incoming Skype UDP packets created a ring sound of the incoming call and established a channel for voice conversation as shown in the captured screen of its monitoring tool in Fig. 15.

Source	Destination	Protocol ...	Description	Time Date Local Adjusted
JAIST	46.9.176.21	UDP	UDP:SrcPort = 33276, DstPort = 39283...	1:26:05 PM 8/27/2014
46.9.176.21	JAIST	UDP	UDP:SrcPort = 39283, DstPort = 33276...	1:26:05 PM 8/27/2014
JAIST	46.9.176.21	UDP	UDP:SrcPort = 33276, DstPort = 39283...	1:26:13 PM 8/27/2014
46.9.176.21	JAIST	UDP	UDP:SrcPort = 39283, DstPort = 33276...	1:26:13 PM 8/27/2014

Fig. 15. Incoming UDP Skype packets after being decrypted and dispatched from TOR exit node (in this case, TOR exit node IP address is 46.9.176.21).

However, by the time the Skype account at the JAIST computer side clicked *answer*, the channel only survived for a few seconds and without being able to transmit any voice it got dropped. By analyzing the monitoring results of both sides, it is not difficult to show the cause of the drop out shortly after the ring. As shown in Fig. 14, the TCP packets are sent out at the time the call was made (from 1:26:04). However, at the JAIST computer, the UDP packets were received interruptedly at 1:26:5 and at 1:26:13. It is therefore clear that connection delay and short time-to-live duration of UDP packets is the main cause, something which could be eventually offset by the expected increase in the Internet connection speed in the next coming years through the evolution of optical fiber technology.

To further investigate the potential of TOR-based network for with voice over IP applications, we also tested it with other voice over IP applications like LINE and Viber and observed the same phenomenon and have no doubt that UDP-based smart home appliances could also operate smoothly in TOR environment in the near future.

VI. Conclusion

Since the Internet of Things is still at the early stage of its development, smart home appliance producers need more time and effort in order to produce cost-effective and safe products. Until then, however, being aware of cyber attacks aimed at smart home appliances and its numerous risks, having an alternate solution to remedy the potential problems is quite important.

In this paper we first showed numerous vulnerabilities that smart home appliance users are facing and how networking monitoring tool and regular DDOS attack technique can easily be used to attack the IoT network and simultaneously abuse them for illicit purposes. We then proposed the 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. Our results show that Tails having many security features such as multilayer encryption, data transmission in distributed manner over a huge amount of voluntary nodes around the world, and MAC address spoofing, is indeed a suitable approach to solve recent security problems in TCP-based smart home appliances.

Future work along this research which is already being carried out by the authors is to utilize the TinyOS programming language and simplify The Amnesic Incognito Live System so as to create a Tails-embedded router that can act as the central control gateway to support and secure the smart home appliance system. The idea is to come up with a practical version of the universal home gateway while waiting for the development of its ideal version and involvement of network operators in the security challenges of smart home appliances. Practical realization of "*VoIP over TOR*" is another area which needs further investigation while waiting for further increase in the Internet connection speed through the evolution of optical fiber technology.

Acknowledgment

Firstly, Nguyen Phong HOANG would like to sincerely thank his supervisor, Professor Davar PISHVA (Dean of College of Asia Pacific Studies at APU), for his dedicated help and support during the last 2 years. Without such help and academic advice this research could not have been accomplished. Next, we would like express our deepest gratitude to Professor Atsuko Miyaji from the School of Information Science, Japan Advanced Institute of Science and Technology (JAIST). Through an Academic Exchange Program which exists between APU and JAIST, Mr. Nguyen Phong HOANG was able to enjoy her state-of-the-art scientific laboratory and precious advice while conducting some experiments for this work.

References

[1] Herper, Matthew. *Emerging Technologies: 'Smart' Kitchens A Long Way Off*, Forbes, Feb. 2003.

[2] Staff. *Wired News: Caregiver Tech Slowly Evolves*, Associated Press, September 2003.

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

[4] Hoang Nguyen Phong, and Davar Pishva. "Anonymous communication and its importance in social networking." *the 16th International Conference on Advanced Communication Technology (ICACT 2014)*, pp. 34-39 (February 2014)

[5] *Having fun via WIFI with Philips Smart TV. Revuln, 2014. Available: http://vimeo.com/*90138302

[6] Hemanth Joseph, *Dosing Pebble Smart Watch And Thus Deleting All Data Remotely*, August 2014 [Online]. Available: http://www.whitehatpages.com/2014/08/dosing-pebble-smartwatch-and-thus.html

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

[8] Ramneek Puri, *SANS Institute InfoSec Reading Room*. SANS Institute, August 2003. Available: http://www.sans.org/reading-room/whitepapers/malicious/bots-botnet-overview-1299

[9] Brian Donohue, *Beware The Thingbot!* Kaspersky Lab, January 2014. Available: https://blog.kaspersky.com/beware-the-thingbot/

[10] Katagi, Kizu. *Vulnerability of Toshiba's RD Series HDD-DVD Recorder 'Stepping-stone' for Danger*, Internet Watch, October 2004 (In Japanese) http://internet.watch.impress.co.jp/cda/news/2004/10/06/4882.html.

[11] Press Release, *A Report to Customers on the Issue of 'Creative Zen Neeon' Digital Audio Player and its Response*, Creative, September 2004 (In Japanese) Available: http://jp.creative.com/corporate/pressroom/releases/welcome.asp?pid=12181.

ISBN 978-89-968650-5-6

[12] AU Announcement, *EZweb Browser's Home Page URL Transmittal on AU and TU-KA Mobile Phones*, KDDI News, December 2005 (In Japanese) Available: http://www.au.kddi.com/news/topics/au_topics_index20051209.html.
[13] D. Pishva, K. Takeda, *A Product Based Security Model for Smart Home Appliances*, 40th Annual IEEE International Carnahan Conferences on Security Technology, pp. 234-242 (2006).
[14] D. Pishva, K. Takeda, *A Product Based Security Model for Smart Home Appliances*, IEEE Aerospace and Electronics System Magazine, Vol.23, No.10, pp. 32-41 (October, 2008).
[15] *Proofpoint Uncovers Internet of Things (IoT) Cyberattack*. Proofpoint Inc., Sunnyvale California, 2014.
[16] "*The solution: a distributed, anonymous network*", Tor: Overview. TOR project. Available: https://www.torproject.org/about/overview.html.en#thesolution
[17] Koen Vervloesem, *the Amnesic Incognito Live System: A live CD for anonymity*. Linux Info from the Source, April 2011. Available: https://lwn.net/Articles/440279/
[18] Robert Hogan, Jacob Appelbaum, Damon McCoy, Nick Mathewson, *Separate streams across circuits by connection metadata*. The Tor Project, October 2008. Available: https://gitweb.torproject.org/torspec.git/blob/HEAD:/proposals/171-separate-streams.txt
[19] *Fing, the ultimate network toolkit*. Overlook Soft. Available: http://www.overlooksoft.com/features
[20] *Information Environment, Information Environment (Information Society Research Center) - Campus Network*. Japan Advanced Institute of Science and Technology. Available: http://www.jaist.ac.jp/is/keyword/research/info.html

Nguyen Phong HOANG was born in Tien Giang Province, Vietnam in 1992. He received his undergraduate degree in Business Administration majoring in Information & Communications technology (ICT) from Ritsumeikan Asia Pacific University (APU), Japan. He is presently pursuing his graduate studies at the Graduate School of Informatics at Kyoto University in Japan. He has received numerous scholarship and awards; APU Tuition Reduction Scholarship from 2010-2014, JASSO (Japan Student Services Organization) Scholarship from 2011-2012, and TOYOTA Tsusho Scholarship from 2013-2014. His research interests include information security, privacy and anonymous communication. He hopes to advance his research on TOR (The Onion Router), one of the most robust anonymous tools, during his graduate studies. He participated in the 16th International Conference on Advanced Communication Technology and received Outstanding Paper Award from the Conference. He has been an IEEE member since 2013.

Davar Pishva is a professor in ICT at the College of Asia Pacific Studies, Ritsumeikan Asia Pacific University (APU) Japan and presently serves as the Dean of both College and Graduate School of Asia Pacific Studies. In teaching, he has been focusing on information security, technology management, VBA for modelers, structured decision making and carries out his lectures in an applied manner. In research, his current interests include biometrics; e-learning, environmentally sound and ICT enhanced technologies. Dr. Pishva received his PhD degree in System Engineering from Mie University, Japan. He is Secretary General of IAAPS (International Association for Asia Pacific Studies), Senior Member of IEEE, and a member of IEICE (Institute of Electronics Information & Communication Engineers), IAAPS and University & College Management Association.

ISBN 978-89-968650-5-6