International Journal of Smart Home
Vol. 9, No. 12, (2015), pp. 191-198
http://dx.doi.org/10.14257/ijsh.2015.9.12.20

# Threats Analysis, Requirements and Considerations for Secure Internet of Things

Yunjung Lee[1] and DoHyeun Kim[2*]

*[1] Dept. of Computer Science and Statistics, Jeju National University*
*690-756 Jeju-si, South Korea*
*[2] Dept. of Computer Engineering, Jeju National University*
*690-756 Jeju-si, South Korea*
*[1]rheeyj@jejunu.ac.kr, [2]kimdh@jejunu.ac.kr*

## *Abstract*

*For the Internet of Things security, it should be considered security risk environments such as various platforms and services including smart devices that can be mounted on household electric appliances, healthcare, car, and heterogeneous networks that are connected to the Internet, and cloud services mobile apps. In this paper, we provides analysis of new security threats, caused by open-platform of Internet of Things (IoT) and interconnectivities among various smart devices and sensors via the Internet, and requirements and scenarios for establishing standards and secure IoT service.*

***Keywords****: IoT Security, Things of Internet Network Security, Privacy, Smart devices, Sensor, Smart Home.*

## 1. Introduction

Internet of Things (IoT) is a technology that can connect to the Internet to all devices, including resource limited sensor as well as smart devices that operated by the user's control. Gartner would be expected that 26 billion or more devices by 2020 will be cross connected and a variety of innovations and business opportunities will be created [1].

Some reports showed that a new worm targeting embedded devices spread during the holiday season. The worm that targets various devices running on Linux has brought to light the numerous security vulnerabilities of IoT endpoints networks. Some Researchers discovered the worm and said that it appears to be engineered to target IoT. It works by leveraging a PHP vulnerability patched in May 2012, and attacks un-patched devices, such as Linux-based home routers, set-top boxes, security cameras etc. The worm generates IP addresses randomly, sends out HTTP POST requests and then spreads itself [2].

For the Internet of Things security, it should be considered security risk environments such as various platforms and services including smart devices that can be mounted on household electric appliances, healthcare, car, and heterogeneous networks that are connected to the Internet, and cloud services mobile apps. International standards organizations such as IETF, ITU-T, and ISO are actively in progress for IoT service platform and lightweight authentication / encryption technology standardization. The steps for discussion about IoT security requirements start [3].

As the platform or interoperability of services increased, security became indispensable as well standardization to the spread and success of IoT. If hacking happens, Injury to persons, as well as damage to economic and industrial life, could be caused because IoT can control the information in public infrastructure and industrial facilities. Invasion of

[*] Corresponding Author

ISSN: 1975-4094 IJSH

privacy such as personal information will be amplified with the degree that cannot compare with the current one.

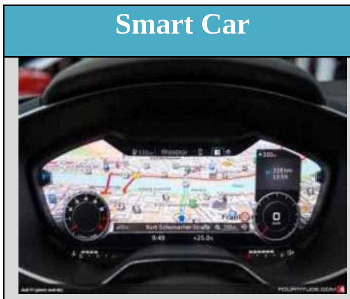
In this paper, we analyze of the main IoT security threats, such as smart cars, smart home, aircraft, and presents requirements to network standards for the IoT, and suggest future research consideration to receive a secure IoT Services.

## 2 Security Threats against IoT

In Black Hat 2014 conference, the fact, "Everything can be hacked." was reaffirmed, and hacking demonstration against main IoT was performed. The next shows presented vulnerabilities such as smart homes, smart cars and aircraft (Table 1) [4, 5].

- ✓ Smart Car : hacking by exploiting a vulnerability in the Remote Network such as Bluetooth and telematics in Car, in-vehicle phone applications
- ✓ Smart Home: monitoring and remote control of the main household equipment to bypass the security features of the Nest smart home devices and
- ✓ Aircraft: unauthorized access via a satellite communication system of the aircraft, by hacking aircraft navigation and security systems

**Table 1. Hacking Simulation**

| Smart Car | Smart Home | Aircraft |
|---|---|---|
|  | <br> | <br> black hat<br>USA 2014<br>Aircraft Data Networks Domain Model<br>SATCOM<br>IOActive |

It is difficult to enforce heavyweight security methods such as antivirus, encryption, and authentication, etc., due to using a low-end device. It is impossible that ZigBee, Wi-Fi, Bluetooth, etc. does not solve the security problem because it is operated via the interconnection between heterogeneous networks. In particular, the heterogeneous network interconnection is established via the Internet, so the security requirements should be consistent with the existing Internet environment.

### 2.1. Categorized IoT Security Threats

Categorized IoT Security Threats are as follow:

- Privacy Protection Encryption method: light-weight encryption and real-time encryption suitable to very simplified small devices in particular
- Device to Device authentication: person-excluded authentication method should be considered, because conventional KEY or certificate verification method using server aren't fit to IoT environment that all things are connected.
- Secure Booting: ways to verify device integrity or the authenticity and integrity of software running on a device or at booting
- VPN: way to use a public network like a private network between server and IoT with small devices
- Updates and Patches: way to security patches or update methods against to a waste of bandwidth on a number of devices operation, performance lowering, functional stability damaging
- Firewalling and IPS: DPI (Deep Packet Inspection) or packet filtering (Inbound / Outbound) measures to be applied in a particular industry and malicious violations

detection and prevention methods on the collective intelligence-based so that response over the entire IoT network system when malicious violations occur in a terminal.

- Big data Privacy Protection: privacy protection or anonymization of data collected from the IoT
- Reliability Management: ways of managing to trust or reject information, depending on confidence in IoT network of in-domain or between different domains
- Malicious traffic detection and countermeasures on IoT networks: detect malicious traffic to prevent denial of service attacks and corresponding network of IoT technologies
- Distributed Security: cryptographic methods and management technologies distributed among IoT
- Response against Cyber-physical fusion attack: defense, detection and restoration against various attacks considering the physical characteristics of devices and systems
- Access Control on IoT: Environment establishment that provide limited range of information and device control according to access level the user (device) entered the specific area
- Usable Security and Privacy: way to enforce security by making recognition for security and privacy to user

## 3 Existing Research

Enterprises can protect themselves by ensuring all of the devices accessing their network have up-to-date firmware and implement network security technologies, such as intrusion prevention systems (IPS), firewalls and VPNs, within an in-depth defense framework to minimize potential attack vectors. Although VPNs are commonly associated with securing communications with corporate networks and the Internet, they are often implemented on devices to safeguard machine-to-machine (M2M) communications and more innovative forms of connectivity. By leveraging a VPN, end devices communicate through a secure encrypted tunnel, which makes it much more difficult for an attacker to access an IoT device and breach a network. [2]

### 3.1. 6LoWPAN and CoAP

International standards organizations such as IETF, ITU-T and ISO are actively underway IoT-related technical standardization. The IETF conducted standardization engrafting IEEE 802.15.4 based sensor network to TCP/IP protocol stack, through the 6LoWPAN Working Group, as shown in Figure 1. However, it is inappropriate to IoT environment. [6]

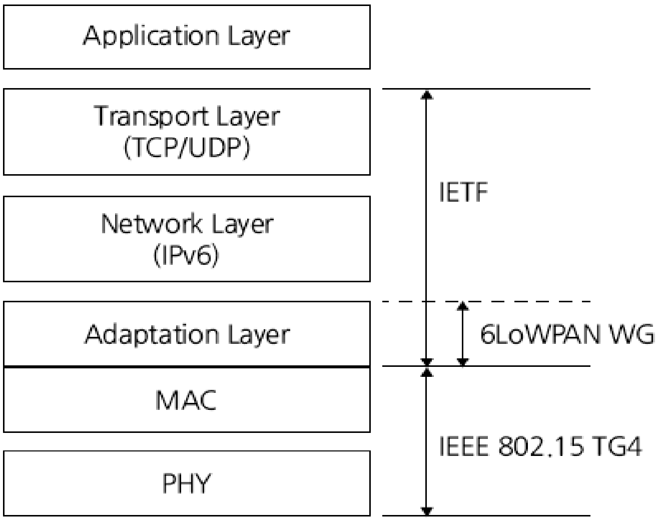


**Figure 1. 6LoWPAN Technical Range**

The Core Working Group of the IETF has developed CoAP (Constrained Application Protocol) as web-based application protocol that can be used in a network environment. As shown in Figure 2, CoAP adopts the UDP as a transport layer protocol, forward the event message with way of server/client system, and has an asynchronous transmission mode for sending and receiving. However, as using the protocols such as UDP datagram, the entire message should be sent again even if just a loss of packet. [7]

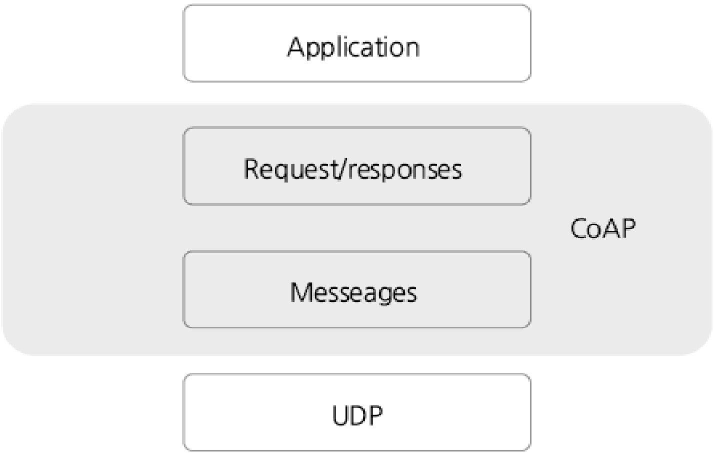


**Figure 2. CoAP Protocol Stack**

### 3.2. SSL VPN

For most applications of the Internet, Transport Layer Security is considered the gold standard for security. For a majority of users, a web site that runs over HTTPS is safe – and in the World Wide Web, it most likely is: there is direct interaction between a user (via a browser) and a server system. The user needs to implicitly trust the server, as it processes all data and operations displayed in the browser anyway. Even for basic IoT applications, this assumption is no longer sufficient. [8]

Some IoT security products include SSL VPN functionality that utilized advanced encryption technology and is configured by default to require two-factor authentication (certificate plus valid username/password). VPN security can be increased by using PKI x.509 certificates that are unique for each user. The vender persist that a powerful and highly scalable solution that offers advanced VPN capabilities with a simple web-based interface allows all  remote devices, networks and users to be able to communicate seamlessly. Industry standard encryption technology ensures data stays protected in transit for complete IoT security [9, 10]. Figure 3 shows IoT VPN concept, and Figure 4 shows SSL VPN Architecture.

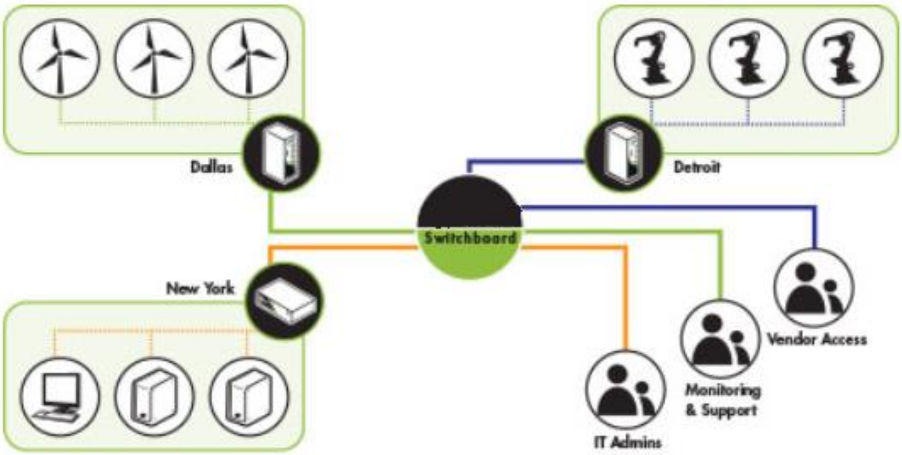


**Figure 3. IoT VPN Concept**

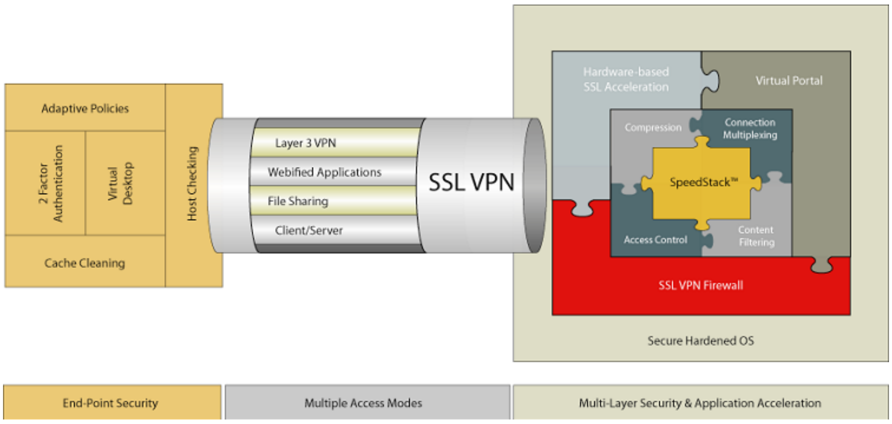


**Figure 4. SSL VPN Architecture**

VPN provides a space on the network that's securely isolated from all other traffic. However, within that space, all nodes are accessible by any participant. Think of an office building with one highly secure entry door. Only the holders of the key can get in. If once inside, they find the doors to every room on every floor unlocked. Thus, it becomes critically important to keep any keys to the building in the right hands.

Another consideration is multi-institution connections. For some people, the vision of the IoT includes connecting devices that belong to different companies. Maybe you want to give certain suppliers access to the latest data in your production system, or permit consultants to poll devices in the field. Or perhaps several companies need to work from a common data set. Few IT managers would be willing to provide all these participants access to a corporate VPN.

And finally, there are the sheer numbers. The vision for the IoT is for millions of devices to be connected. Although not every device will be linked to every other device, the scale still dwarfs most current implementations of VPN. Each additional device becomes one more security risk, and adds to the tasks of maintaining the system. The per-device resources needed to support a VPN are significant, as are the requirements on the server side to manage such a vast network. The costs and workload add up quickly. [11]

## 4 IoT Security Requirement and Scenarios

### 4.1. IoT Security Requirements

IoT network security requirements considering the pros and cons of the given standards and the IoT network environment are as follows:

- Security protocols development that meets the existing network stacks
  - Sensor network technologies between the sensors have been communication by configuring its own network that is not connected to the Internet. However, IoT connect all devices for operation by a user of the control Internet and connect all devices including smart devices and resource-limiting sensors.
  - Security protocol development is required to operate without any problem in existing IP-based network protocol stack
- Ensuring interoperability among heterogeneous networks
  - IoT is composed of sensors, smart devices, networks, platforms (hardware platform, open software platform, specific OS platforms, etc.), Web services, and data analysis / forecasting, Big-data processing, and security / privacy protection technologies.
  - Each of these factor technologies provide certain features, and are integrated with each other, also provides new features. However, linkage between securities technologies existed in each component might cause unknown problems.
  - Need for the development of security technology that can be applied in particular to the mutual connection of the common kind of device.

### 4.2. Scenarios of Security challenges

Applying these same practices or variants of them in the IoT world requires substantial reengineering to address device constraints. Blacklisting, for example, requires too much disk space to be practical for IoT applications. Embedded devices are designed for low power consumption, with a small silicon form factor, and often have limited connectivity. They typically have only as much processing capacity and memory as needed for their tasks. And they are often “headless”—that is, there isn’t a human being operating them who can input authentication credentials or decide whether an application should be trusted; they must make their own judgments and decisions about whether to accept a command or execute a task. There is the variety of IoT applications poses an equally wide variety of security challenges. For example: [12]

- ✓ In factory floor automation, deeply embedded programmable logic controllers (PLCs) that operate robotic systems are typically integrated with the enterprise IT infrastructure. How can those PLCs be shielded from human interference while at the same time protecting the investment in the IT infrastructure and leveraging the security controls available?

- ✓ Control systems for nuclear reactors are attached to infrastructure. How can they receive software updates or security patches in a timely manner without impairing functional safety or incurring significant recertification costs every time a patch is rolled out?
- ✓ A smart meter—one which is able to send energy usage data to the utility operator for dynamic billing or real-time power grid optimization—must be able to protect that information from unauthorized usage or disclosure. Information that power usage has dropped could indicate that a home is empty, making it an ideal target for a burglary or worse.

It needs to study more detail examples of threats that may occur in a variety of environments IoT by collecting a variety of its scenarios.

## 5 Conclusion

Accelerating the pace of development of smart devices as times goes on, IoT is expected to be more widely used in a variety of areas. But we can expect that a variety of security threats against IoT appears Through IoT is platform opening, and the interconnectivity among various heterogeneous smart devices and sensor via Internet.

Recent international standards organizations have been to build IoT over the technology that can connect the devices having various physical constraints to the Internet. However, It is difficult to meet the new requirements related to IoT connecting countless devices to internet and processing large amount of data he Internet.

This paper provides analysis of new security threats, caused by open-platform of Internet of Things (IoT) and interconnectivities among various smart devices and sensors via the Internet, and requirements and scenarios for establishing standards and secure IoT service.

In the future, we will proceed with the research for security protocol applied data compression technology on the basis of the proposed consideration.

## Acknowledgments

This work was supported by the Convergence R&D program of MSIP/NST. [Convergence Research-14-2-ETRI, Development of Internet of Things (IoT)-based Urban Underground Utility Monitoring and Management System]. Corresponding author; DoHyeun Kim (e-mail: kimdh@jejunu.ac.kr).

## References

[1] Gartner, “Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020”, (http://www.gartner.com/newsroom/id/2636073), **(2012)**.

[2] VPN Haus, "The Internet of Vulnerable Things: Why Remote Access Security is Critical", **(2014)**.

[3] “Information Security Load-Map for IoT”, Ministry of Science, ICT and Future Planning of Korea, **(2014)**.

[4] https://www.blackhat.com/us-14/.

[5] Y. J. Park and Y. J. Lee, “A Study on Security Threats and Countermeasures for Internet of Things”, Summer KICS Conference Proceedings, **(2015)**.

[6] http://www.ietf.org/wg/concluded/6lowpan.html/.

[7] K. Hartke, "Observing Resources in CoAP”, IETF Internet Draft, **(2014)**.

[8] C. Heger, "SSL isn’t enough for Internet of Things", http://blog.zuehlke.com/en/ssl-isnt-enough-for-internet-of-things/, **(2014)**.

[9] http://www.endian.com/products/connect/, **(2015)**.

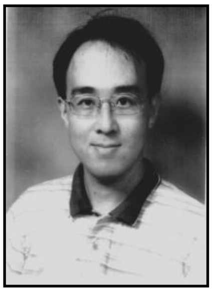
[10] T. H. Kim, “SSL VPN is the Solution for Ubiquitous Workplace”.

[11] B. McIlvride, “A VPN may not be the right tool for IoT security”, http://embedded-computing.com/guest-blogs/a-vpn-isnt-the-right-tool-for-iot-security/, **(2015)**.

[12] W. River, “Security in the Internet of Things”, **(2015)**.

## Authors

**Yunjung Lee,** She did her Ph.D. in the Department of Computer Science from Korea University, Seoul, South Korea in 2002. Professor, Dept. of Computer Science and Statistics of Jeju National University, South Korea



**Do-Hyeun Kim**, He received the B.S., M.S. and P.D degrees in Electronics Engineering from Kyungpook National University, Taegu, Korea, in 1988 and 1990, 2000 respectively. He joined the Agency of Defense Development (ADD), Korea, in 1990. Since 2004, he is currently a professor at the Department of Computer Engineering at Jeju National University, Korea. His research interests include sensor web, optimization algorithm and context prediction.