INVITED PAPER *Special Section on Information and Communication System Security*

An Overview of Security and Privacy Issues for Internet of Things

Heung Youl YOUM[†a)], ***Nonmember***

SUMMARY The Internet of Things (IoT) is defined as a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies by ITU-T. Data may be communicated in low-power and lossy environments, which causes complicated security issues. Furthermore, concerns are raised over access of personally identifiable information pertaining to IoT devices, network and platforms. Security and privacy concerns have been main barriers to implement IoT, which needs to be resolved appropriate security and privacy measures. This paper describes security threats and privacy concerns of IoT, surveys current studies related to IoT and identifies the various requirements and solutions to address these security threats and privacy concerns. In addition, this paper also focuses on major global standardization activities for security and privacy of Internet of Things. Furthermore, future directions and strategies of international standardization for the Internet of Thing's security and privacy issues will be given. This paper provides guidelines to assist in suggesting the development and standardization strategies forward to allow a massive deployment of IoT systems in real world.

key words: *security, privacy, threats, new work item, internet of things, IEEE 802.15, standardization direction*

1. Introduction

The internet of things (IoT) provides a feasible tool to facilitate the vision of future Internet, where physical devices, vehicles (such as "connected devices" and "smart devices"), buildings and other items are interworked, which are embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. The Gartner estimated that the market for Internet of Things (IoT) devices is exploded and nearly 21 billion devices will be connected to the Internet by 2020 [1]. With the increasing number of devices, security and privacy concerns are also going to increase significantly. A study by HP reveals that 70% of the most popular Internet of Things (IoT) devices contain serious vulnerabilities [2]. The 5 stages of IoT device lifecycle are identified in [3]: design and development, testing and debugging, deployment, management, and decommissioning of IoT devices, which need to be considered when security requirements are derived. Security and privacy should not be considered as an add-on to IoT devices later, but rather as an integral part to the IoT device's reliable functioning throughout IoT device lifecycle.

There have been several surveys and studies regarding the security issues for IoT during about past 5 years. Context aware computing research efforts are analyzed and evaluated to understand how the challenges in the field of context-aware computing have been tackled in desktop, web, mobile, sensor networks, and pervasive computing paradigms [4]. Capabilities are introduced to identify and connect worldwide physical objects into a unified system, and the security threats and privacy concerns of IoT are summarized [5]. Extensive analysis, as well as open research issues, on security protocols and mechanisms related to IoT is provided [6]. It also analyzes how existing approaches ensure fundamental security requirements and protect communications on the IoT, together with the open challenges and strategies for future research work in the area. Lifecycle of things and threats and their countermeasures are presented [7]. A survey of all the security issues existing in the Internet of Things (IoT) along with an analysis of the privacy issues are conducted [8]. A survey of the state-of-the-art in Intrusion Detection Systems (IDSs) that are proposed for Wireless Sensor Networks is provided [9].

Our paper differs from the previous surveys mentioned above in many ways. Our survey focuses on studies related to standardization activities and analyzing practical studies and works, including analyzing the existing security protocols stacks and security architecture. Our paper has considered all survey described above to address standardization aspects. There are several Standards Developing Organizations (SDOs) working for IoT security and privacy, such as ITU-T [10], ISO/IEC SC27 [11], IEEE SA [12] and IETF [13]. Major international standardization work has been extensively evaluated in order to propose future standardization directions to these organizations. Our paper also focuses on all related issues to propose future international standardization's directions.

The rest of the paper is organized as follows: In Sect. 2, we identify the definition of IoT, relationship between sensor network and IoT, security threats and requirements, privacy threats and security capabilities for IoT. In Sect. 3, existing protocols applicable to IoT communications and security characteristics of the protocols applicable to IoT are addressed and evaluated. In Sect. 4, we discuss new topic for IoT standardization as well as proposed future directions of international standardization activities related to IoT security. Finally, in Sect. 5, we conclude this paper with presenting the relationship between new research topics and new

Manuscript received December 19, 2016.
Manuscript revised January 27, 2017.
Manuscript publicized May 18, 2017.

[†]The author is with the Department of Information Security Engineering, Soonchunhyang University, Korea.
a) E-mail: hyyoum@sch.ac.kr

DOI: 10.1587/transinf.2016ICI0001

work items for standardization.

2. IoT Overview and Background

2.1 Application Areas of Internet of Things

The 10 most popular IoT applications are summarized by [14]: applications for smart home, wearables, smart city, smart grids, Industrial internet, connected car, connected health (digital health/telehealth/telemedicine), smart retail, smart supply chain and smart farming. Security and privacy issues should be addressed to operate these systems and platforms.

2.2 What is the Internet of Things?

IoT has gained significant attention in industries as well as academia during the past decade. The term 'Internet of Things' was firstly coined by Kevin Ashton [15] in 1998. He has mentioned "The Internet of Things has the potential to change the world, just as the Internet did".

Terms definition of Internet of thing varies between different contexts. Table 1 summarizes definitions of Internet of things by different relevant organizations. The definition provided by ITU-T Y.2060 [20] is accepted for this paper, because this definition is agreed by the De jure standardization development organization.

2.3 Security Architectures of Internet of Things

Figure 1 presents a generic IoT topology [28], which comprises sensor-equipped edge devices on a wired or wireless network sending data via a gateway to a public or private cloud. Aspects of the topology will vary broadly from application to application; for example, in some cases the gateway may be implemented as a part of the IoT device. Devices based on such topologies may be built from the ground up to leverage IoT or may be legacy devices that will have IoT capabilities added post-deployment.

2.4 Relationship between Sensor Network and IoT

In a sensor network, data is generated by either a low-end sensor nodes or high-end sensor nodes. Then, data is collected by mobile and static sink nodes. The sink nodes send the data to low-end computational devices. These devices perform a certain amount of processing on the sensor data. Then, the data is sent to high-end computational devices to be processed further. Finally, data reaches the cloud where it will be shared, stored, and processed significantly.

The Ubiquitous Sensor Network (USN) is defined as an intelligent information infrastructure of advanced e-Life society. It delivers user-oriented information and provides knowledge services to anyone anytime, anywhere and wherein information and knowledge are developed using context awareness by detecting, storing, processing, and integrating the situational and environmental information gathered from sensor tags and/or sensor nodes [29] affixed to anything described in Recommendation ITU-T X.1311 [30]. It describes the security threats to and security requirements of the ubiquitous sensor network. The sensor networks (SN), a part of USN, are the most essential components of the IoT. They include sensors and actuators. The sensors collect data which then is processed and decisions are made.

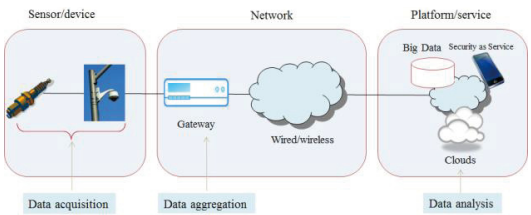

Fig. 1 Generic IoT topology [21]

Table 1 Definition of internet of things

	Definitions
Wikipedia [16]	Internetworking of physical devices, vehicles, buildings and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.
GSMA [17]	Coordination of multiple machines, devices and appliances connected to the Internet through multiple networks.
European Research Project [18]	The Internet of Things allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service.
European Commission [19]	The semantic origin of the expression is composed by two words and concepts: Internet and Thing, where Internet can be defined as the world-wide network of interconnected computer networks, based on a standard communication protocol, the Internet suite (TCP/IP), while Thing is an object not precisely identifiable. Therefore, semantically, Internet of Things means a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols.
ITU-T Y.2060 [20]	A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

Finally, actuators make the decided actions. Relationship between sensor networks and Internet of Things is presented as shown in Fig. 2 [4]. The comparison between sensor network and Internet of Things is described in Table 2.

2.5 ITU-T SG17's Activities of Internet of Things Security

Table 3 provides current standardization activities of ITU-T SG17 (Study Group 17) on security [31] and SG20 on IoT and its applications including smart cities and communities [32] in the area of security and privacy of Internet of things. It is noted that ITU-T SG17 addresses all security issues and ITU-T SG20 addresses all issues related to IoT. So, there is a need for coordinating work related to IoT between two SGs.

2.6 Worst Security Scenarios for IoT

Seven worst scenarios [33] are described in terms of security in typical applications, such as home office, snapchat service in the smartphone, healthcare, satellite communications, transport safety, connected car and printer firmware. For example, attackers exploit smartphone through applications, photos, videos, social media, and GPS. Thousands of photos and videos from the Snapchat service could be uploaded online, which allows people to access to the site and to store photos within seconds of being viewed as shown in Table 4.

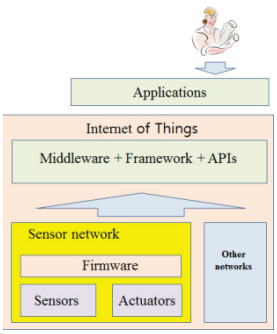

Fig. 2 Relationship between Sensor Network and IoT

The description of increasing challenges in privacy [8] is provided: In the IoT environment, IoT devices such as sensors are expected to collect more information about users (i.e. people) in all aspects. This includes both physical and conceptual data, such as location, preferences, calendar data, and medical information to name a few. As a result, utmost care needs to be taken when collecting, modelling, reasoning, and with persistent storage. Security and privacy need to be addressed at different levels in the IoT. At the lowest level, the hardware layer should ensure security and privacy during collecting and temporary storage within the device. Secure protocols need to ensure communication is well protected. Once the data is received, application level protection needs to be in placed to monitor and control whoever can see or use context and so on.

A survey presented in [34] identifies that only 22% of respondents agreed that the benefits of smart devices outweighed any privacy concerns. Furthermore, 83% of respondents were concerned about the idea of personal information being collected by smart devices and 87% are concerned about the type of personal information collected through smart devices.

2.7 Security Threats for IoT Things

As seen in Table 5, there are various threats that can exist through the lifecycle of a thing: manufacturing, installation/commissioning and operation, which are identified in [35] as follows:

- **Cloning of things**: During the manufacturing process of a thing, an untrusted manufacturer can easily clone the physical characteristics, firmware/software, or security configuration of the thing.
- **Malicious substitutions of things**: During the installation of a thing, a genuine thing may be substituted with a similar variant of lower quality without being detected.
- **Eavesdropping attack**: During the commissioning of a thing into a network, it may be possible to eavesdropping on keying materials, security parameters, or

Table 2 Comparison between sensor network and Internet of Things [4]

	Sensor network	Internet of Things
Components	▪ a part of the IoT. ▪ consist of the sensor hardware (sensors and actuators), firmware and a thin layer of software.	▪ comprise SN and include a thick layer of software such as middleware systems, frameworks, APIs and many software components, where the software layer is installed across computational IoT devices (both low and high-end) and the cloud.
Application	▪ is designed, developed, and used for specific application purposes.	▪ support many kinds of applications where it can be expanded as a general purpose sensor network.
Interoperability	▪ operate independently from the IoT.	▪ can exist together with the SN as the majority of hardware (e.g. sensing and communicating) infrastructure support, through providing access to sensors and actuators which are provided by SN.

Table 3 ITU-T standardization activities in the area of IoT

Recommendation Title		Content	Status
Recommendation ITU-T X.iotsec-1 (X.1362) [21]	Simple encryption procedure for Internet of things (IoT) environments	· provide an encryption procedure for the Internet of things (IoT) device security; · specify encryption mechanism with associated mask data (EAMD) for the IoT environments; · describe EAMD and how it provides a set of security services for traffic using it.	Under TAP (traditional approval procedure in accordance with ITU-T WTSA Resolution 1 [22])
Recommendation ITU-T X.iotsec-2 [23]	Security Framework for Internet of Things	· describe the security framework for Internet of Things; · analyse security threats and challenges in the Internet of Things environment; · describe security capabilities that could mitigate these threats and address security challenges; · focus on IoT security capabilities based on the Gateway model.	Under development
Recommendation ITU-T X.itssec-1 (X.1373) [24]	Secure software update capability for intelligent transportation system communication devices	· provide a procedure of secure software updating for ITS communication devices for the application layer; · include a basic model of software update, security controls for software update and a specification of abstract data format of update software module.	Under TAP
Recommendation ITU-T X.itssec-2 [25]	Security Guidelines for V2X Communication Systems	· provides security guidelines for V2X communication systems, where X denotes V, I and N; · includes analysis of threat and vulnerability for V2X communication systems; · provide security requirements for V2X (vehicle to X) communication, where X denotes V (vehicle), I (infrastructure) and N (nomadic).	Under development
Recommendation ITU-T Y.4100/Y.2066 [26]	Common requirements of the Internet of things	· provide the common requirements of the Internet of things (IoT), which are based on general use cases of the IoT and IoT actors.	Approved on June 2014
Recommendation ITU-T Y.4401/Y.2068 [27]	Functional framework and capabilities of the Internet of things	· provide a description of the basic capabilities of IoT, the implementation view and the deployment view of the IoT functional framework. · describe additional capabilities of the IoT for the integration of cloud computing and big data technologies with the IoT.	Approved on March 2015

configuration settings, if they are exchanged in the cleartext using a wireless medium. After obtaining the keying material, the attacker might be able to recover the secret keys established between the communicating entities, thereby compromising the authenticity and confidentiality of the communication channel, as well as the authenticity of commands and other traffic exchanged over this communication channel. When the network is in operation, communication between devices may be eavesdropped upon if the communication channel is not sufficiently protected or in the event of session key compromise due to a long period of usage without key renewal or updates.

- **Man-in-the-middle attack**: The commissioning phase may also be vulnerable to man-in-the-middle attacks, e.g., when keying material between communicating entities is exchanged in the cleartext and the security of the key establishment protocol depends on the tacit assumption that no third party is able to eavesdrop on or sit in between the two communicating entities during the execution of this protocol.
- **Firmware Replacement attack**: When a thing is in operation or maintenance phase, its firmware or software may be updated to allow for new functionality or new features. An attacker may be able to exploit such a firmware upgrade by replacing the things with malicious software, thereby influencing the operational behavior of the thing.
- **Extraction of security parameters**: A thing deployed in the ambient environment (such as sensors, actuators, etc.) is usually physically unprotected and could easily be captured by an attacker. Such an attacker may then attempt to extract security information such as keys (e.g., device's key, private-key, group key) from this

Table 4 7 scary security scenarios [33]

Applications	Security scenarios
Home office Hack	The printer can be updated with a Trojan for spying on printed documents or installed with malicious software on a network. It is necessary for Kaspersky Lab researcher to take less than 20 minutes to hack into his home office DSL router and network attached storage devices, where he found 14 vulnerabilities.
Ransomware to Thermostat	When you enter your house, the thermostat is set to 110 degrees, which you cannot control. An email arrives in poorly written English asking for $100 to return control of your home heating system.
Hacking of vehicle	Hackers can access the car's network by breaking into its wireless-enabled radio, for instance, and issuing commands to the automated steering, parking, braking, or driving mechanisms.
Hijacking smart applications	Hackers can utilize ways to exploit it through applications, photos, videos, social media, and GPS (global positioning system). Thousands of photos and videos from the Snapchat service can be disclosed online, which allow people to offer access to the site - and to store photos within seconds of being viewed.
Hacking transportation control system	A widely deployed carry-on baggage scanner could be easily manipulated by a malicious insider or outside attacker to sneak weapons or other banned items past TSA airport checkpoints.
Fake Satellite SOS	An attacker could compromise the satellite systems, run malware, install malicious firmware, and even send a phony SMS text to trick a ship to follow a certain path or to rescue another ship.
Pacemaker	A terrorist hacked into a pacemaker and assassinated a fictional victim.

Table 5 Security threats of IoT devices during lifecycle of things [35]

	Manufacturing	Installation/commissioning	Operation
Application layer			Firmware replacement
Transport layer		Eavesdropping & Man-in-the-middle	Eavesdropping, Man-in-the-middle
Network layer			DoS attack, Routing attack
Physical layer	Device cloning	Substitution	DoS attack, Privacy threats, Extraction of security parameters

thing or try and re-program it to serve his needs.

- **Routing attack**: Routing information in IoT can be spoofed, altered, or replayed, in order to create routing loops, attract/repel network traffic, extend/shorten source routes, etc. Other relevant routing attacks include the followings [8]: 1) Sinkhole attack (or black-hole attack), where an attacker declares himself to have a high-quality route/path to the base station, thus allowing him to do anything to all packets passing through it, 2) Selective forwarding, where an attacker may selectively forward packets or simply drop a packet, 3) Wormhole attack, where an attacker may record packets at one location in the network and tunnel them to another location, thereby influencing perceived network behavior and potentially distorting statistics, thus greatly impacting the functionality of routing, and 4) Sybil attack, whereby an attacker presents multiple identities to other things in the network.
- **Privacy threat**: The typical privacy threats to the users may include the tracking of a thing's location and usage. An attacker may infer information based on data gathered about individual things, thus deducing behavioral patterns of the user of interest to him.
- **Denial-of-Service attack (DoS)**: Things may have tight memory and limited computation capability; they are thus vulnerable to resource exhaustion attack, for example DDoS (distributed denial of services). Attackers can continuously send requests to the specific things so as to deplete their resources.

2.8 Privacy Threats for IoT Devices

Privacy is defined as "the right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others" [47].

Privacy should be protected for data in the device, at rest, in transit and at processing [Kumar et al., 5]. Table 6 describes privacy threats as well as solution to address these privacy threats.

2.9 Threats for Applications and Platforms in IoT

The OWASP (Open Web Application Security Project) [48] provides security vulnerabilities for applications/platforms in the Internet of Things shown in Table 7. Various

Table 6 Privacy threats in the Internet of Things [5]

	Threats	solutions
Privacy in device	・Unauthorized access to IoT devices may result in sensitive information being leaked out.	・Location privacy of the device owner, protection of the personal information in case of the device theft or loss and resilience to side channel attacks should be provided.
Privacy in transit	・Sensitive information may be leaked out during the communication when plain text is transmitted without encryption.	・Encryption is a common tool to assure data confidentiality of data in transit. In case encryption adds data to packets which provides a way for tracing, pseudonyms could be replaced by identity information of IoT devices in order to decrease the vulnerability of the device's identity or user's being revealed.
Privacy at rest	・Unnecessary amount of personal information may be stored.	・Only necessary amount of information that is needed should be stored in the IoT device. ・Only personal information should be retained, if unavoidable. ・Information should be stored on the basis of the principle of "need-to-know".
Privacy at processing	・Personal information should be shared for the intended purpose of processing. ・Personal information should not be disclosed to third parties, without explicit acceptance and the knowledge of the data owner.	・Encryption with appropriate access control, such as Digital Rights Management (DRM) [36] could be an appropriate tool which defends against illegal access to data. ・User's permission and their awareness are required for disclosure, distribution of personal information. ・De-identification techniques [37] could be used to conceal the real identity linked with the processed data.

Table 7 Security vulnerabilities for applications/platforms in the Internet of Things [38]

vulnerabilities	Threats
Username Enumeration	・Attackers collect a set of valid usernames by interacting with the authentication mechanism.
Weak Passwords	・Attackers exploit weak account passwords, for example '1234' or '123456'.
Account Lockout	・Attackers continue sending authentication attempts after 3 - 5 failed login attempts.
Unencrypted Services	・Attackers eavesdrop on communication, which are not properly encrypted.
Two-factor Authentication	・Attackers utilize insufficient strength of single-factor authentication mechanisms. ・Two-factor authentication mechanisms are required to employ, using a combination of knowledge-based authentication factor and a security token or fingerprint scanner.
Poorly Implemented Encryption	・Attackers utilize the encryption software which is improperly implemented, configured or is not being properly updated, for example, using SSL (secure socket layer) v2, whose usage was prohibited by IETF RFC 6176 in [39].
Update Sent Without Encryption	・Updates are transmitted over the network without using TLS [40] or encrypting the update file itself, which can be abused by attackers.
Update Location Writable	・Storage location for update files is writable, potentially allowing firmware to be modified and distributed to all users.
Denial of Service	・Service can be attacked in a way that denies service to that service or the entire device.
Removal of Storage Media	・Attackers have capability to physically remove the storage media from the device.
No Manual Update Mechanism	・IoT device may have no capability to manually force an update check, which can be abused by attackers.
Missing Update Mechanism	・IoT may have no capability to update their devices, which can be abused by attackers.
Firmware Version Display	・Attackers exploit display of current firmware version and/or the last update date.

types of threats should be addressed by appropriate security measures.

2.10 Security Requirements for IoT

The 6 security requirements of the Internet of things (IoT)

are provided in [49] as follows:

- **Communication security**: Secure, trusted and privacy protected communication capability is required, so that unauthorized access to the content of data can be prohibited, integrity of data can be guaranteed and privacy-related content of data can be protected during data transmission or transfer in IoT.
- **Data management security**: Secure, trusted and privacy protected data management capability is required, so that unauthorized access to the content of data can be prohibited, integrity of data can be guaranteed and privacy-related content of data can be protected when storing or processing data in IoT.
- **Service provision security**: Secure, trusted and privacy protected service provision capability is required, so that unauthorized access to service and fraudulent service provision can be prohibited and privacy information related to IoT users can be protected.
- **Integration of security policies and techniques**: The ability to integrate different security policies and techniques is required, so as to ensure a consistent security control over the variety of devices and user networks in IoT.
- **Mutual authentication and authorization**: Before a device (or an IoT user) can access the IoT, mutual authentication and authorization between the device (or the IoT user) and IoT is required to be performed according to predefined security policies.
- **Security audit**: Security audit is required to be supported in IoT. Any data access or attempt to access IoT applications are required to be fully transparent, traceable and reproducible according to appropriate regulation and laws.

2.11 Basic Security Functions for IoT Devices

Similarly, [28] identifies 5 basic security functions for IoT devices: secure booting, access control, device authentication, firewalling and IPS, updates and patches as follow:

- **Secure booting**: When IoT device being booted, the authenticity and integrity of the software and applications on the device is verified using cryptographically generated digital signatures.
- **Access control**: Appropriate access controls should limit the privileges of device components and applications so they access only the resources they need to do their jobs.
- **Device authentication**: When the device being plugged into the network, it should authenticate itself prior to receiving or transmitting data. Just as user authentication allows a user to access a corporate network based on user name and password, device authentication allows a device to access a network based on a similar set of credentials stored in a secure storage area.
- **Firewalling and IPS (intrusion protection system)**: The device also needs a firewall or deep packet inspection capability to control traffic that is destined to terminate at the device.
- **Updates and patches**: Once the device is in operation, it will start receiving hot patches and software updates. Operators need to roll out patches, and devices need to authenticate them, in a way that does not consume bandwidth or impair the functional safety of the device.

In addition, basic security capabilities for IoT security standards that IoT system should support are identified by [57]: secure booting, authentication, secure communication, data protection, firewall, intrusion detection, event reporting, remote command audit, policy management and hardware integration, which are very similar to those described in [28].

3. Existing Security Protocols Applicable to IoT

This section describes some prominent existing protocols which are applicable to IoT and security characteristics of existing protocols.

3.1 Existing Protocols Stacks Applicable to IoT

The communication protocols available or being designed by the IEEE and IETF currently enable a standardized protocol stack in [58] and illustrated in Fig. 3, which describes the protocol stacks [59] applicable to IoT. Figure 4 presents payload space with DTLS on 6LoWPAN environment.

Table 8 provides description of existing protocols applicable IoT. The current IEEE 802.15.4 PHY layer(s) specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs). Given that a large amount of IoT applications requires only a few bits to be sent, a standardized PHY layer should be considered in order to allow for ultra-low rate transmissions over very narrow frequency bands. IEEE802.15.4e standard is very appropriate for a protocol stack for IoT because it is latest generation of highly reliable and low-power MAC pro-

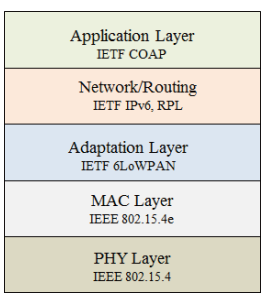

Fig. 3 IoT protocol stack

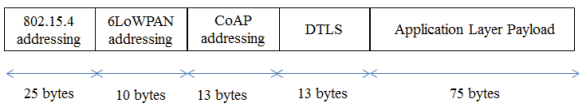

Fig. 4 Payload space with DTLS on 6LoWPAN environment

Table 8 Description of existing protocols applicable IoT environments

Layer	Protocol	Description
Application	IETF CoAP [41]	▪ The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained (e.g., low-power, lossy) networks. CoAP is an application layer protocol that is intended for use in resource-constrained internet devices, such as WSN nodes. ▪ The CoAP protocol defines binding to DTLS [42] (Data Transport Layer Security) to secure CoAP messages for constrained environments.
Network	IETF RPL [43]	▪ The Low-Power and Lossy Networks (LLNs) are a class of network in which both the routers and their devices are constrained. The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) provides a mechanism whereby multipoint-to-point traffic from devices inside the LLN towards a central control point as well as point-to-multipoint traffic from the central control point to the devices inside the LLN are supported. Support for point-to-point traffic is also available. ▪ The RPL defines how security is applied to routing control messages, and the current specification also defines the following three security modes: Unsecured, Preinstalled and Authenticated.
Adaptation	6LoWPAN [44] [45]	▪ The 6LoWPAN is an acronym of IPv6 over Low power Wireless Personal Area Networks. ▪ The 6LoWPAN IETF group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks. ▪ The 6LoWPAN adaptation layer optimizes the usage of this limited payload space through packet header compression, while also defining mechanisms for the support of operations required in IPv6, in particular neighbor discovery and address auto-configuration.
MAC/PHY	IEEE 802.15.4e [46]	▪ IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) which focuses on low-cost, low-speed ubiquitous communication between devices. ▪ It can be contrasted with other approaches, such as Wi-Fi, which offer more bandwidth and require more power. The basic framework conceives a 10-meter communications range with a transfer rate of, for example, 250 Kbit/s.

tocol. From a networking perspective, the IETF 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks.) protocol family defines encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802.15.4 based networks, which have been instrumental in connecting the low power radios to the Internet. It is the work of IETF ROLL allowed suitable routing protocols to achieve universal connectivity. From the transport layer and an application perspective, the IETF CoAP (Constrained Application Protocol) family has been instrumental in ensuring that application layers. The CoAP is an application layer protocol that is intended for use in resource-constrained internet devices over low-power embedded networks.

3.2 Security Characteristics for Existing Protocol Stacks Applicable to IoT

This clause describes security characteristics in existing protocols applicable to IoT as shown in Table 9 which is summarized [6]. These characteristics should be considered when security requirements are derived as a standard.

4. Work Items and Proposed Future Directions for International Standardization Activities

This clause describes security challenges and future topics that are needed for the international standardization.

4.1 Security Challenges for IoT

The Internet of Things (IoT) may introduce new security challenges in cryptographic security, credentialing, and identity management [65] from the standardization's point of view as described in Table 10.

4.2 Role of IoT Security Standards

A role of IoT security standards described in [57] includes protection for the device by ensuring only authentic code from a trusted source is allowed to run on the device, protection for data by providing secure communication, data-at-rest protection and secure decommissioning of devices, awareness of attacks by including security monitoring, intrusion detection and integration with security management systems, security management enabling updates to security policies in response to emerging threats, and device to device authentication ensuring that IoT devices are only communicating with other known, trusted entities.

4.3 Standardization Items by ISO/IEC JTC 1/SC 27

The SC 27 Study Group on Security and Privacy for Internet of Things (IoT) conducted gap analysis and identified 8 gaps which need to be studied with the aim of International Standards at the April 2016 Tampa SC27 meeting as follows [66], [67]:

Table 9 Security characteristics in existing protocols applicable to IoT

Layer	Protocol	Description		
Application	IETF CoAP	Security services	Confidentiality, authentication, integrity, non-repudiation and protection against replay attack	▪ Message for CoAP is encrypted by Datagram TLS (DTLS) [50] over UDP. ▪ DTLS provides security services of confidentiality, integrity, non-repudiation for application layer communication using CoAP. Security services for confidentiality, authentication, integrity and non-repudiation are provided using AES/CCM as the cryptographic algorithm to support security requirements in the current CoAP specification. ▪ Protection against replay attacks may also be achieved in the context of DTLS, using a different nonce value for each secured CoAP packet.
		Security mode	NoSec	▪ The CoAP messages are transmitted without any security.
			PresharedKey	▪ Devices that are pre-programmed with the symmetric cryptographic keys employ this security mode.
			RawPublicKey	▪ Devices based on public keys, but which are unable to participate in public-key infrastructures employ this security mode. A given device is preprogrammed with an asymmetric key pair that may be validated using an out-of-band mechanism.
			Certificates	▪ This security mode supports public keys. The device has an asymmetric key pair with an X.509 [51] certificate that binds it to its Authority Name and is signed by some common trusted root. The device also has a list of root trust anchors that can be used for certificate validation.
Network	IETF RPL	Security services	Integrity and data authenticity	▪ Integrity and data authenticity is provided using AES in the CCM mode (AES/CCM) [52] with 128-bits key length for MAC generation and RSA [53] with SHA-256 [54] for digital signature.
			Confidentiality	▪ Confidentiality and delay protection are provided using AES in the CCM mode, a generic authenticated encryption block cipher mode.
			Semantic security and protection against replay attack	▪ Semantic security and protection against packet replay attacks is provided with the help of the Counter field, which may be used to transport a timestamp.
			Key management	▪ The KIM (Key Identifier Mode) field of the Security section is used to indicate whether the cryptographic key required to process security for this message may be determined implicitly or explicitly.
		Security mode	Unsecured	▪ This mode is default and no security is applied to routing control information.
			Preinstalled	▪ Confidentiality, integrity and data authentication are applied to the routing control messages using the key.
			Authenticated	▪ A device may initially join the network using a preconfigured key and the preinstalled security mode, and next obtain a different cryptographic key from a key authority with which it may start functioning as a router.
Adaptation	6LoWPAN	▪ No security mechanisms are currently specified in the context of the 6LoWPAN adaptation layer, but the relevant documents include discussions on the security vulnerabilities, requirements and approaches to consider for the usage of network layer security.		
MAC/PHY	IEEE 802.15.4	Security services	Confidentiality	▪ Data is encrypted using AES in the counter mode (AES-CTR) [55] with 128-bit key length.
			Data Integrity	▪ Data integrity is provided using AES in the Cipher Block Chaining mode (AES-CBC) [56] with 32-bits, 64-bits, or 128 bits of Message Integrity Code.
			Confidentiality / data integrity	▪ Data is encrypted using AES in the counter mode (AES-CTR) with 128-bit key length and data integrity is provided using AES in the cypher Block Chaining mode (AES-CBC) with 32-bits, 64-bits, or 128 bits of Message Integrity Code.

- Gateway Security: The ISO/IEC 27033-4 [68] addresses gateway security for IoT in part, so, there is a room for improvement of this standard to fit it into IoT environment. It can be implemented with a firewall or deep packet inspection capability as well as monitoring functions.
- Network Function Virtualization security: It comprises NFV (network function virtualization) [69] and SDN (software defined network) [70] technology, where SDN is defined as the physical separation of the network control plane from the forwarding plane, and where a control plane controls several devices.

Table 10 Major challenges from standardization's point of view [65]

	Challenges	Possible solution
Cryptographic algorithm	▪ These cryptographic suites, for example, RSA[60], DH [61] and AES [62], which were designed to be operated with significant resources, may not be applied to IoT due to the constrained memory and processor speed of some IoT devices.	▪ A combined mode supporting authentication and encryption, and the ECC asymmetric algorithms [63] with at least 112-bits key length, for example, AES-GCM [64].
Key management	▪ Manual configuration (pre-shared keys) of the number of devices in the IoT is unlikely to scale.	▪ Automated re-key after deployment is essential, in case of manual keying on the initial deployment.
Credentialing	▪ The number of devices and the expected limitations in user interfaces will exacerbate credentialing IoT devices.	▪ Security techniques that combine automatic and manual techniques for initial deployment will likely be needed in the IoT.
Privacy	▪ The IoT has the potential to expose the precise application of that energy demand, further violating the privacy expectations of the population.	▪ Adoption for technologies designed to prevent information leakage.

Table 11 Allocation of security work related to IoT/SCC in ITU-T [86]

	Task	Responsibility
1	Example IoT/SCC security use cases, services and features	SG20
2	Identify security threats and conduct risk assessment (identification, analysis and evaluation)	Common project. (SG20, principal).
3	Security requirements for IoT/SCC solutions	Common project. (SG20, principal).
4	Allocation of Security functions to IoT/SCC functional architecture layers and functional blocks	Common project. (SG20, principal).
5	IoT Protocol Security	Common project (SG17, principal).
6	Security in ITS (intelligent transport system)	Common project (SG17, principal).
7	Detailed mechanisms for implementing IoT/SCC security requirements	Common project (SG17, principal).
8	Allocation of IoT/SCC security functions to fundamental concepts of security architecture	SG17
9	Security Management for IoT/SCC	Common project (SG17, principal).
10	Operational Security for IoT/SCC	Common project (SG17, principal)

- Management and measurement of IoT security: New management and measurement mechanisms to reflect IoT environments may be required to address the network technologies of the IoT such as SDN/NFV.
- Open Source assurance and security: Open software is a major part of the emerging, new technologies for the IoT, such as SDN (Open Flow [71]), NFV (Open Stack [72]) and Big data (Hadoop [73]). Open source may be used to implement software and application in IoT. Vulnerabilities in the Open Source should be managed in an appropriate manner.
- IoT Risk Assessment techniques: There is a room for improving current risk assessment process [74] due to data processing of IoT devices, cascading impacts and non-deterministic outcomes.
- Privacy and Big Data: Data collected in the IoT environment may contain a subset of personally Identifiable Information (PII). The PII is defined as any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal in ISO.IEC 29100 [75]. There may be a room for updating the ISO/IEC. 29100 (privacy framework) to reflect new requirements in the IoT environments.
- Application Security Guidance for IoT: ISO/IEC 27034 [76] offers guidance on information security to those specifying, designing and programming or procuring, implementing and using application systems. There is a room for improvement of these standards to address new challenges in implementing software for IoT.
- IoT Incident Response Guidance: There may be a room for updating ISO/IEC 27035-2 [77].

As a result of this activity, two Study Periods were initiated by ISO/IEC SC27/WG 4 and WG5 at the April 2016 Tampa SC27 meeting:

- SC 27/WG 4 Study period in the area of Guidelines for

Table 12 Relationship between some research topics and potential work items by ISO/IEC SC27 and ITU-T

Proposed research topics	Highlighting features	Items related to SC27	Category related to ITU-T
Kumar et al. [5]	▪ applicable to network and data link layer ▪ present lifecycle of things, attacks and their countermeasure and privacy and regulation	▪ gateway security, network function virtualization	▪ Requirement, capability and IoT protocol security
Granja et al. [6]	▪ Applicable to application, transport, network and data link layer ▪ present protocol stack, security for all layers and open research issues	▪ gateway security, network function virtualization	▪ Requirement, functions, capability, and IoT protocol security
Butun et al. [9]	▪ applicable to application layer ▪ present survey of state-or-art in IDS for wireless sensor network	▪ Gateway security, network function virtualization	▪ Requirement, security functions, and detailed mechanisms
WIND [28]	▪ Applicable to network and data link layer ▪ present a general topology and security functions	▪ gateway security	▪ Threats, requirement, security function, capability and detailed mechanisms
Kothmayr *et al*. [84]	▪ applicable to transport end-to-end security ▪ Implementation of two-way authentication security scheme, the Datagram Transport Layer Security (DTLS) protocol, based on RSA	▪ Gateway security, network function virtualization	▪ Requirement, security functions, and IoT protocol security
Chavan et al. [85]	▪ applicable to transport layer end-to-end security. ▪ propose a collaboration of DTLS and CoAP, DTLS header compression scheme that helps to reduce packet size, energy consumption and avoids fragmentation by complying the 6LoWPAN standards and DTLS header compression scheme does not compromises the point-to-point security provided by DTLS.	▪ Gateway security, network function virtualization	▪ Requirement, functions, and IoT protocol security
Granjal *et al*. [86]	▪ propose an end-to-end security architecture for Internet integrated sensing applications providing benefits not only in respect to the efficient support of ECC authentication and key agreement, but also of other mechanisms promoting security of LoWPAN devices and communications.	▪ Gateway security, network function virtualization	▪ Requirement, functions, detailed mechanisms and IoT protocol security
Hummen [87]	▪ usage of certificate pre-validation and session presumption to offload the public key authentication to the gateway.	▪ Gateway security, network function virtualization	▪ Requirement, functions, and detailed mechanisms
Le et al. [88]	▪ applicable to Routing layer ▪ raise the question of weakness of an RPL, which is the underlying routing protocol of 6LoWPAN ▪ reveal that attack in a high forwarding load area will have more impact on network performance than attack in other areas.	▪ Gateway security, network function virtualization	▪ Requirement, functions, and IoT protocol security
Raza *et al*. [89]	▪ applicable to datalink layer ▪ present the implementation of IEEE 802.15.4 link-layer security. ▪ show that it is possible to reuse crypto hardware within existing IEEE 802.15.4 transceivers for 6LoWPAN/IPsec.	▪ Gateway security, network function virtualization	▪ Requirement, functions, and IoT protocol security

security in Internet of Things (IoT) for 6 months [78]

- SC 27/WG 5 Study Period on Guidelines for privacy in Internet of Things (IoT) for 12 months [79]

Those two Study Periods which are currently underway in SC 27 may explore new work items in the area of IoT security and privacy at the October 2016 Abu Dhabi SC27 meeting or in the future.

4.4 Future Topics for IoT/SCC Work in ITU-T

The ITU TSAG agreed on allocation of security work between ITU-T SG17 and SG20, which is related to IoT/SCC (Internet of Things/Smart Sustainable Cities) at its July 2016 meeting as shown in Table 11 [80]. In this Table, common project defined as a means that both groups may participate in a certain activity and principal means that final decision on New Work Items and/or in approving Recommendations is made by the principal Study Group. Two SGs continue their work according to this decision by ITU-T TSAG. The Recommendation ITU-T X.iotsec-2 [24] describes the security framework and security capabilities for IoT systems. They include capabilities for authentication, key manage-

ment, authorization, audit, integration of various security policies, software module updates, vulnerabilities scanning, and monitoring. The consensus of ITU-T SG17 is to develop the further detailed security mechanisms based on the capabilities described ITU-T X.iotsec-2 in the future.

4.5 Future Directions for International Standardization

The collaboration between relevant bodies, for example ITU-T, ISO and IEC, is very important to avoid any duplication of efforts, diverse standards and unnecessary expense for the security experts that need to participate in activities of relevant bodies. The collaboration team or joint coordination activities for example ITU-T Joint Coordination Activity (JCA) [81] should be encouraged to establish for coordinated activities of all relevant standardization bodies related to IoT. The primary role of JCA is to harmonize activities in terms of subject matter, time-frames for meetings and publication goals. The first direction is to establish the Joint Coordination Activity (JCA) on IoT security and privacy with the leadership of ITU-T SG17. The member of this JCA should include at least ISO/IEC JTC 1/SC 27, IETF, GSMA [82], IEEE and ITU-T. Common text defined in [83] on the same topic between ITU-T SG17 and ISO/IEC JTC 1/SC 27 should be encouraged to be developed between two bodies, which is a standards developed both groups with exactly same text and different numbers.

Taking into account that two major bodies such as ITU-T and ISO/IEC JTC 1/SC 27 have already identified gaps (potential items) and there is a need for developing various kinds of new standards for application areas and detailed mechanisms of IoT and SCC, it is necessary to develop new standards about these gaps and detailed security mechanisms which are identified by both groups. The last direction is to enhance the existing collaboration mechanisms among the relevant bodies in accordance with [90]. The typical example of these collaboration mechanisms should include the liaison relationship, joint workshop, co-located meeting and exchange of relevant documents.

5. Conclusion

International standardization developing groups are striving to develop standards to address security and privacy issues for IoT. IoT has entered a phase of mass usage and it could not acceptable that 70% of IoT devices have major security vulnerabilities. It would take some time for IoT security standards to reach at a level where customers can feel confident in the security of a device based on a security rating, but it is believed that it is time to start this work to meet urgent market needs. As security may be an enabling factor of many of major IoT applications, detailed security mechanisms and protocols including organizational management issues to secure communications are fundamental.

In the case where IoT devices would be used for dozens of years without upgrade or update, it may be impossible to protect IoT devices itself against new upcoming threats or vulnerabilities. These security measures to prevent these new threats should be employed in the IoT devices. In addition, security aspects are considered throughout the standards development process. Since IoT device users have usually no knowledge of security technology, their default security setting should be employed to address this challenge. It is noted that many security holes are created during developing, since a developer is not so interested in security compared with developer of general-purpose computer. An education/training for development engineers becomes important.

In the paper, we conduct an exhaustive analysis on the security threats, protocols and mechanisms available to protect communications about IoT from standardization's point of view. We also propose relationship between some research topics and potential work items by ISO/IEC SC27 and ITU-T in Table 12, the relationship between research topics and standardization topics by ISO/IEC SC27 and ITU-T SG17 are presented, together with its related layer for further work by the international standardization bodies.

In conclusion, it is believed this paper may provide an important contribution to the standardization community, by providing all issues and solutions for international standardization activities, helping readers interested in developing new solutions address security and privacy in the context of communication protocols for the IoT.

References

[1] N. Eddy, "Gartner: 21 Billion IoT devices to invade by 2020," InformationWeek, Nov. 2015. Available at http://www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081
[2] E. Kovacs, "70% of Internet Of Things Devices Reveal Vulnerabilities," Hewlett Packard, July 2014. Available at http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.V-e1I7Wa1fA
[3] WIND White Paper, Managing the IoT Lifecycle From Design Through End-of-Life, Nov. 2015.
[4] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context Aware Computing for The Internet of Things: A Survey," IEEE, vol.16, no.1, pp.414–454, 2014.
[5] J. Sathish Kumar and D.R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," International Journal of Computer Applications, vol.90, no.11, pp.20–26, March 2014.
[6] J. Granjal, E. Monteiro, and J.S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Commun. Surveys Tuts., vol.17, no.3, pp.1294–1312, Jan. 2015.
[7] C. Lu, "An Overview of Privacy and Security Issues in the Internet of Things," Springer, May 2014. Available at http://www.cse.wustl.edu/~jain/cse574-14/ftp/security.pdf
[8] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of Security and Privacy Issues of Internet of Things," Jan. 2015. available at https://www.researchgate.net/publication/270763270_Survey_of_Security_and_Privacy_Issues_of_Internet_of_Things
[9] I. Butun, S.D. Morgera, and R. Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks," IEEE Commun. Surveys Tuts., vol.16, no.1, pp.266–282, 2014.
[10] ITU Telecommunication Standardization Sector (ITU-T), http://www.itu.int/en/ITU-T/Pages/default.aspx
[11] ISO/IEC JTC 1/SC 27 IT Security techniques, http://www.din.de/en/meta/jtc1sc27

[12] IEEE SA (standards association), http://standards.ieee.org/
[13] Internet Engineering Task Force (IETF), https://www.ietf.org/
[14] K.L. Lueth, "The 10 most popular Internet of Things applications right now," IoT Analytics, Feb. 2015. available at https://iot-analytics.com/10-internet-of-things-applications/
[15] K. Ashton, "That 'internet of things' thing in the real world, things matter more than ideas," RFID Journal, June 2009, http://www.rfidjournal.com/article/print/4986
[16] Wikipedia, https://en.wikipedia.org/wiki/Internet_of_things
[17] GSMA, IoT Security Guidelines Overview Document, version 1.0, Feb. 2016.
[18] P. Guillemin and P. Friess, "Internet of things strategic research roadmap," The Cluster of European Research Projects, Tech. Rep., Sept. 2009, available at http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2011.pdf
[19] European Commission, "Internet of things in 2020 road map for the future," Working Group RFID of the ETP EPOSS, Tech. Rep., May 2008, available at http://ec.europa.eu/informationsociety/policy/rfid/documents/iotprague2009.pdf [Accessed on: 2011-06-12].
[20] Recommendation ITU-T Y.2060, Overview of the Internet of things, June 2012.
[21] Recommendation ITU-T X.iotsec-1, Simple encryption procedure for Internet of things (IoT) environments, Sept. 2016.
[22] ITU WTSA-12, Resolution 1 - Rules of procedure of the ITU Telecommunication Standardization Sector, 2012.
[23] Recommendation ITU-T X.iotsec-2, Security Framework for Internet of Things, Sept. 2016.
[24] Recommendation X.itssec-1, Secure software update capability for intelligent transportation system communication devices, Sept. 2016.
[25] Recommendation X.itssec-2, Security Guidelines for V2X Communication Systems, Sept. 2016.
[26] Recommendation ITU-T Y.4100/Y.2066, Common requirements of the Internet of things, June 2014.
[27] Recommendation ITU-T Y.4401/Y.2068, Functional framework and capabilities of the Internet of things, March 2015.
[28] WIND white paper, Security in the Internet of Things: Lessons from the Past for the Connected Future, Jan. 2015.
[29] WIKI sensor node, available at https://en.wikipedia.org/wiki/Sensor_node Recommendation.
[30] ITU-T X.1311, Information technology - Security framework for ubiquitous sensor networks, Feb. 2011.
[31] ITU-T SG17 (Security), http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx
[32] ITU-T SG 20 (IoT and its applications including smart cities and communities), available at http://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx
[33] M. Cohodas, "The Internet of Things: 7 Scary Security Scenarios," Oct. 2016. (http://www.darkreading.com/perimeter/the-internet-of-things-7-scary-security-scenarios/d/d-id/1316659?image_number=1)
[34] A. Ross, "Privacy In All Things Includes the Internet of Things," The online privacy blog, July 2014.
[35] O. Garcia-Morchon, S. Kumar, et al., "Security Considerations in the IP-based Internet of Things," IETF Internet Draft, Sept. 2013. http://tools.ietf.org/html/draft-garcia-core-security-06
[36] E. Liu, Z. Liu, and F. Shao, "Digital Rights Management and Access Control in Multimedia Social Networks," In Genetic and Evolutionary Computing, Springer International Publishing, pp.257–266, 2014.
[37] ISO/IEC 20889, Information technology – Security techniques – Privacy enhancing data de-identification techniques, Oct. 2016.
[38] OWASP Internet of Things Project, (online available at https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities)
[39] S. Turne and T. Polk, Prohibiting Secure Sockets Layer (SSL) Version 2.0, IETF 6176, March 2011.
[40] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, DOI 10.17487/RFC5246, Aug. 2008.
[41] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," IETF RFC 7252, June 2014.
[42] E. Rescorla and N. Modadugu, "DTLS: Datagram Transport Layer Security," IETF RFC 4347, 2006.
[43] T. Winter, Ed. and P. Thubert, Ed., A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.P. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," IETF RFC 6550, March 2012.
[44] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, Transmission of IPv6 Packets Over IEEE 802.15.4 Networks, IETF RFC 4944, 2007.
[45] J. Hui and P. Thubert, Compression Format for IPv6 Datagrams Over IEEE 802.15.4-Based Networks, IETF RFC 6282, 2011.
[46] IEEE Standard for Local and metropolitan area networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), 2011.
[47] R. Shirey, Internet Security Glossary, Version 2 IETF RFC 4849, Aug. 2007.
[48] Open Web Application Security Project (OWASP), available at https://www.owasp.org/index.php/Main_Page
[49] Recommendation ITU-T Y.4100/Y.2066, Common requirements of the Internet of things, June 2016.
[50] E. Rescorla and N. Modadugu, Datagram Transport Layer Security Version 1.2, IETF RFC 6347, Jan. 2012.
[51] Recommendation ITU-T X.509, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, Oct. 2012.
[52] D. Whiting, R. Housley, and N. Ferguson, "Counter with CBC-MAC (CCM)," IETF RFC 3610, Sept. 2003.
[53] J. Jonsson and B. Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, IETF RFC 3447, Feb. 2003.
[54] D. Eastlake 3rd and T. Hansen, US Secure Hash Algorithms (SHA and HMAC-SHA), IETF 4634, July 2006.
[55] R. Housley, "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)," IETF RFC 3686, Jan. 2004.
[56] S. Frankel, R. Glenn, and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec," IETF RFC 3602, Sept. 2003.
[57] A. Grau, IoT Security Standards – Paving the Way for Customer Confidence, IEEE Standard University, Feb. 2016.
[58] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (important) things," Proc. IEEE, pp.1–18, 2012.
[59] WIKI protocol stacks, available at https://en.wikipedia.org/wiki/Protocol_stack
[60] B. Kaliski, PKCS #1: RSA Encryption Version 1.5, IETF RFC 2437, March 1998.
[61] E. Rescorla, Diffie-Hellman Key Agreement Method, IETF RFC 2631, June 1999.
[62] National Institute of Standards, FIPS Pub 197, Advanced Encryption Standard (AES), Nov. 2001.
[63] D. McGrew, K. Igoe, and M. Salter, Fundamental Elliptic Curve Cryptography Algorithms, IETF RFC 6090, Feb. 2011.
[64] J. Salowey, A. Choudhury, and D. McGrew, AES Galois Counter Mode (GCM) Cipher Suites for TLS, IETF, RFC 5288, Aug. 2008.
[65] T. Polk and S. Turner, Security Challenges For the Internet Of Things, Feb. 2011, available at https://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf
[66] ISO/IEC JTC 1/SC 27 N16051, Summary of NB contributions to the SC 27 Study Group on Security and Privacy Issues on Internet of Things (IoT) (in response to SC 27 N15885), March 2016.
[67] ISO/IEC JTC 1/SC 27 N15298, Draft meeting report of SC 27/SG Security and Privacy Issues on IoT, Kuching, Malaysia, 3rd May 2015, June 2015.

[68] ISO/IEC 27033-4:2014, Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways
[69] What is NFV – Network Functions Virtualization – Definition? available at https://www.sdxcentral.com/nfv/definitions/whats-network-functions-virtualization-nfv/
[70] Software-Defined Networking (SDN) Definition, available at https://www.opennetworking.org/sdn-resources/sdn-definition
[71] OpenFlow, available at https://www.opennetworking.org/sdn-resources/openflow
[72] OpenStack, available at https://openvirtualizationalliance.org/what-kvm/openstack
[73] What Is Apache Hadoop?, available at http://hadoop.apache.org/
[74] ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management
[75] ISO/IEC 29100:2011, Information technology – Security techniques – Privacy framework
[76] ISO/IEC 27034:2011+ Information technology — Security techniques — Application security, available at http://www.iso27001security.com/html/27034.html
[77] ISO/IEC 27035-2, Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response
[78] ISO/IEC JTC 1/SC 27/WG 4 N 1500, SoC SP IoT - Comments and contributions received on the call for contributions to the six month Study period in the area of Guidelines for security in Internet of Things (IoT), Aug. 2016.
[79] ISO/IEC JTC 1/SC 27/WG 5 N 1502, WG 5 SoC SP Privacy IoT - Contributions received to the SC 27/WG 5 Study Period on Guidelines for privacy in Internet of Things, Aug. 2016.
[80] ITU-T SG17 TD 2637, Summary of agreements between ITU-T Study Groups 17 and 20 on IoT security studies, Sept. 2016.
[81] Recommendation ITU-T A.1, Working methods for study groups of the ITU Telecommunication Standardization Sector, Nov. 2012.
[82] GSMA, http://www.gsma.com/aboutus/
[83] Recommendation A.23 (2000) Annex A, Guide for ITU-T and ISO/IEC JTC 1 cooperation, June 2014.
[84] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two way authentication," Proc. 37th IEEE Conf. LCN Workshops, pp.956–963, 2012.
[85] A.A. Chavan and M.K. Nighot, "Secure CoAP Using Enhanced DTLS for Internet of Things," International Journal of Innovative Research in Computer and Communication Engineering, vol.2, no.12, pp.7601–7608, Dec. 2014.
[86] J. Granjal, E. Monteiro, and J.S. Silva, "End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication," Proc. IFIP Network, pp.1–9, 2013.
[87] R. Hummen, J.H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, "Towards viable certificate-based authentication for the Internet of things," Proc. 2nd ACM Workshop Hot Topics Wireless Netw. Security Privacy, pp.37–42, 2013.
[88] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks," IEEE Sensors J., vol.13, no.10, pp.3685–3692, Oct. 2013.
[89] S. Raza, S. Duquennoy, J. Höglund, and T. Voigt, "Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN," Security and Communication Networks, vol.7, no.12, pp.2654–2668, Dec. 2014.
[90] ITU-T WTSA Resolution 7 – Collaboration with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), Oct. 2012.

Heung Youl Youm received his PhD degree in Electronics Engineering from Hanyang University, Seoul, Korea in 1990. He received his Master and Bachelor degree in Electronics Engineering from Hanyang University, Seoul Korea, in 1981 and 1983, respectively. Currently, he is a Professor in the department of information security engineering at the Soonchunhyang University, Korea. He is a director of SCH cybersecurity research center since December 2014. He is the emeritus president of KIISC (Korea institute of information security and cryptology) and was the president of KIISC in 2011. He is a chairman of ITU-T SG17 since November 2016. He had been a vice-chairman of ITU-T SG17 during 2009 to 2016. He was a chairman of ITU-T WP 3/SG 17 during 2013 to 2016 and a chairman of ITU-T WP 2/SG 17 during 2009 to 2012. He had been working for the former MIC (Ministry of Information and Communication), Korea as a Project Manager for information security, from November 2006 to February 2008. His current interest includes theoretical and practical study on various security technologies/protocols such as IPTV/USN/NGN/IoT security. He had been an editor-in-chief for the KIISC Journal for KIISC (Korea Institute of Information Security and Cryptology) from January 2008 to December 2009, respectively. Since 2005, he has contributed to ITU-T by serving as an editor of 19 approved ITU-T Recommendations or Supplements such as Recommendation X.1034 (Guideline on extensible authentication protocol based authentication and key management in a data communication network), X.1111, X.1311 (Information technology – Security framework for ubiquitous sensor networks), X.1151 (Guideline on secure password-based authentication protocol with key exchange), X.1158 (Multi-factor authentication mechanisms using a mobile device), X.1191 (Functional requirements and architecture for IPTV security aspects), X.1193 (Key management for IPTV services), X.1196 (Framework for the downloadable service and content protection system in the mobile Internet Protocol television environment), X.1197 (Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection), X.1208 (A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies), ITU-T X.1210 (Overview of source-based security troubleshooting mechanisms for Internet protocol-based networks) and X Suppl. 10 (ITU-T X.1205 – Supplement on usability of network traceback).