Feasibility of Societal Model for Securing Internet of Things

Hiroshi TSUNODA
Tohoku Institute of Technology
35-1, Yagiyama Kasumi-cho, Taihaku-ku,
Sendai-shi, Miyagi, 982–8577 JAPAN
E-mail: tsuno@m.ieice.org

Glenn Mansfield KEENI
Cyber Solutions Inc.
ICR Bldg, 6-6-3, Minami Yoshinari, Aoba-ku,
Sendai-shi, Miyagi, 989–3204 JAPAN
E-mail:glenn@cysols.com

***Abstract*—In the Internet of Things (IoT) concept, devices communicate autonomously with applications in the Internet. A significant aspect of IoT that makes it stand apart from present day networked devices and applications is a) the very large number of devices, produced by diverse makers and used by an even more diverse group of users; b) the applications residing and functioning in what were very private sanctums of life e.g. the car, home, and the people themselves. Since these diverse devices require high-level security, an operational model for an IoT system is required, which has built-in security. We have proposed the societal model as a simple operational model. The basic concept of the model is borrowed from human society - there will be infants, the weak and the handicapped who will need to be protected by guardians. This natural security mechanism works very well for IoT networks which seem to have inherently weak security mechanisms. In this paper, we discuss the requirements of the societal model and examine its feasibility by doing a proof-of-concept implementation.**

***Keywords*—Internet of Things, security, network architecture, operational model, SNMP**

I. Introduction

Internet of Things (IoT) has penetrated almost every sphere of society. In the IoT concept, various devices such as sensors and actuators possess computing capability and network connectivity. As a result, these devices are accessible for monitoring, control and information collection, via the literally ubiquitous Internet. The IoT concept is bringing in an entirely new gamut of services and applications. At the consumer end, driver-less cars with automatic control and braking mechanisms are emerging and smart homes with automatically controlled electrical appliances are maturing. In the industry, automated systems to monitor and control factory and plant processes are developing rapidly.

While the IoT paradigm will bring various attractive services and economic impact, security and privacy issues have been a major focus area for IoT [1], [2]. One of the reasons is that IoT devices will potentially be used in very private sanctums of life e.g. in the car, inside the home and maybe even inside the human body. In addition, various critical infrastructures such as smart grid and energy plants are extensively deploying IoT devices for wide area monitoring and control. Consequently, if IoT systems are compromised, there is a serious risk that human life will be at risk and life-line services will be disrupted and social order will be breached.

Several IoT related security incidents in both industrial and consumer areas have been reported. In the consumer area, various problems have been found and reported for vehicles made by different car vendors [3]–[5]. IoT devices are utilized for wellness and health care. In [6], the author discusses the theoretical attacks on network connected insulin pumps and continuous glucose monitors. In the industry area, there were attacks against important infrastructures.

A relatively new type of attacks has been reported wherein the communication and processing resources of several vulnerable IoT devices with Internet access have been used to mount massive DDoS attacks on targets. In [7], [8], large scale DDoS attacks by a large number of infected webcams and home routers is reported. One of the largest DDoS attacks to date recorded a traffic of nearly 1.1 terabits from more than 150,000 vulnerable Internet-connected cameras and digital video recorders [9]. In [10], the authors have used honeypot and sandbox systems to show that a significant number of IoT devices are compromised and are targets of malware infection.

When we consider security countermeasures in IoT area, we should understand a major difference between a conventional computing device and an IoT device. According to [11] and [12], the difference is the scope or purpose of the device. Conventional computing devices such as personal computers and smartphones are general purpose computing devices. On the other hand, IoT devices are dedicated purpose devices basically designed for very specific functions such as measuring some data, controlling some device etc. For our work, we define an IoT device as one that interacts with some entities that are in the *things* domain, and that interacts with the rest of the world via the Internet. The former interaction is probably done using some proprietary/private mechanism, to generate data (i.e., probing, measurement, etc) and/or to set data (i.e., configuration). The later interaction is done over communication channels using the Internet standard TCP/IP protocol suite, to transfer the generated data to a destination on the Internet and/or to receive requests to set data. IoT devices generally have severe constraints on resources and functionalities due to cost and/or size limitations. Therefore, it is difficult to assume that IoT devices can be provided with enough security mechanisms.

For securing IoT, we have proposed the societal model,

978-1-5090-4372-9/17/$31.00 ©2017 IEEE

a simple operational model which has built-in security [13]. In this paper, we investigate the requirements of the societal model and discuss its feasibility. The contributions of this paper are summarized as follows:

- We present a societal model for IoT.
- We clarify the core requirements of the societal model.
- We establish the feasibility of the model by doing a proof-of-concept implementation.
- We discuss the difference between the societal model and traditional security measures in the Internet.

II. Related works

IoT security issues have been analyzed from various points of view. Internet Society (ISOC) has outlined a list of security issues [14]. Open Web Application Security Projects (OWASP) has described several concerns about the insufficient security of IoT devices and enumerated the top 10 IoT vulnerabilities [15]. IEEE spectrum did a special feature on IoT security in 2015 [16]. Hewlett Packard [17] analyzed various IoT devices such as TVs, webcams, home thermostats, door locks etc. According to their survey, the average number of vulnerabilities found per device was significantly high. The devices were found vulnerable to a wide range of attacks from Heartbleed to denial of service to weak passwords to cross-site scripting.

In [2], [18], [19] IoT related standardization activities of the Internet Engineering Task Force (IETF) are discussed. While most of the erstwhile work has been on minimizing the communication costs and complexity, the somewhat late realization that without good security, IoT poses a significant risk, has resulted in the launching of several working groups in the IETF Security Area. The DICE-WG has produced a TLS/DTLS profile for IoT devices. The ACE-WG is looking at the issue of authentication and authorization in constrained environments. The COSE-WG is working on simplified JSON object signing and encryption methods that may be used by IoT devices.

In [20] security requirements for a body sensor network (BSN) is discussed. All the sensors in BSN interface with the outer world via a Local Processing Unit (LPU), which acts as a ”router”. Various security requirements are addressed. However, the system is limited in scope as it basically treats sensors as monitoring devices and not control devices. Also, the mechanism for adding a new type of sensor is not discussed. [21] examines the additional threats due to IoT systems when exposed to a cloud environment. In [22] the authors state that it is almost impossible to ensure security and privacy of IoT due to the weak communication protocols, and the inherent heterogeneous nature of the entities involved in the communication. [23] concludes that some Wireless Sensor Network (WSN) applications should not connect to the Internet, due to security considerations. [24] describes the experiences from experimentation with the oneM2M global standards developed by the global standardization body for M2M and IoT. The extension of the test framework to cover security is listed among the future works.

In [25] a biometric-based advanced authentication mechanism that is more resistant to theft and loss than the traditional authentication mechanisms using secrets etc. is described. In [26] the importance of a standard security architecture for Service Oriented Architecture based IoT middleware is discussed. In [27] the focus is basically on what happens when information moves from IoT devices to the cloud. In [28] an IoT system is characterized by an input-capability or an output-capability. The authors then go on to describe a management system - an application that works on the inputs and outputs. Some security is built in but the scope is narrow and while software blocks may be introduced for new types of processing, there is little or no provision for new types of IoT devices to be introduced. [29] argues that a network has to play a critical role in the security of IoT deployments and shows a proof-of-concept secure architecture for IoT network that employs SDN (Software Defined Network) and NFV (Network Functions Virtualization) technologies.

It is clear that despite the significant amount of work in the area of security for IoT networks, and the several solutions that have been proposed, investigated, implemented and deployed, a comprehensive solution that addresses the generic needs of IoT devices are yet to emerge. In this context, we have proposed our societal model for IoT security.

III. Societal model for securing IoT

A. Concept of Societal model

In human society, considering the survival and expansion of the human race, it appears that some form of security that has ensured survival is built-in. While reproduction is a biological factor that has ensured that new members join the society, there is also a built-in mechanism that ensures that babies and infants are protected. Otherwise, they would not reach the reproductive age, the number would dwindle and the race would become extinct.

In an ensemble that is as diverse as the human race, the survival mechanism cannot depend solely on individual effort or awareness but is ensured by rules, traditions, and conventions. An important aspect seems to be the awareness that infants need protection. The protection is provided by a designated group of members e.g., parents and/or guardians. An underlying principle seems to be that the guardian will be the interface between the infant and the rest of the world.

We argue that an IoT device needs a guardian to protect it by interfacing with the Internet to allow the IoT device to survive and function in the desired manner. The guardian must be a device that has enough resource and functionalities.

B. Network Architecture

In the societal model context, IoT devices are designed for a dedicated purpose and are connected in what we will call a *ThingNet (T-Net)*. A guardian device, the *I-Guardian*, resides on the border between the T-Net and the rest of the Internet. I-Guardian devices are responsible for keeping a T-Net secure by interacting with devices on the Internet. I-Guardian must be equipped with enough resources for providing appropriate

security measures, such as data encryption, authentication, and data integrity check.

The architecture for the societal model envisages a collection of IoT devices, which are served by a relatively smaller collection of I-Guardians and a collection of *IoT Applications (I-Applications)*.

I-Applications access IoT devices via the I-Guardians.

One or more IoT devices will be connected in a T-Net. A T-Net will be serviced by an I-Guardian. The size of a T-Net could range from a few IoT devices in a small space to several hundred thousand devices dispersed over a large area. The membership list of a T-Net will be available to the I-Guardian. The code of conduct of members also will be well defined. When an IoT device joins or leaves a T-Net, the T-Net's membership list will be updated. The engineering challenge lies in how smoothly and seamlessly this can be achieved.

C. Operational Model

The societal model that secures the IoT devices in a T-Net will have the following operational requirements.

1) IoT devices will communicate only with the designated I-Guardian
   a) IoT devices must not communicate with any device on the Internet
   b) In some special cases, an IoT device may need to communicate with another device in the same T-Net. For simplicity, we will leave this out of the scope of this work.
2) Legitimate users (I-Applications) will be able to access the services of IoT devices via the I-Guardian over the Internet
   a) I-Guardian must allow legitimate users to have legitimate access to their devices seamlessly
3) It must be possible to add new devices to the realm of an I-Guardian with relative ease. Even in the case where the device is a new type.

To satisfy the above requirements, we propose an operational model as illustrated in Fig. 1.

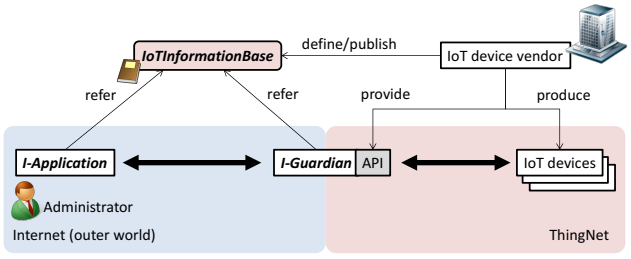

Fig. 1. Operational Model

In our proposed architecture, operations on IoT devices are modeled as inspections or modifications of some information component on the IoT device. This is a device-independent simple atomic model of IoT access on which complex operations may be based. The information component itself would be any one of diverse types. We will call this information component an *IoTInformationObject*. A collection of such objects will form a *IoTInformationBase (IIB)*.

The vendor of an IoT device will develop an IIB module (i.e., a set of IoTInformationObjects) for her device and make it available for concerned parties, as given; I-Application developers and I-Guardian developers. The vendor also provides some application program interfaces (APIs) corresponding to the IIB module so that I-Guardian vendors can provide the instrumentation for accessing specific IoT devices available to I-Guardian users. The transaction between an I-Application and I-Guardian is done based on the name and type of an IoTInformationObject. Once the I-Guardian receives a request pertaining to an IoTInformationObject, the I-Guardian accesses the correspondent IoT device by using the instrumentation. An end-user of an IoT device must have an I-Guardian which has the necessary instrumentation to access the IoT device and service the corresponding IIB module. This simple operational model enables the I-Guardian to accommodate a new type of device only by obtaining the IIB module and corresponding APIs from the vendor of the device and preparing instrumentation using the APIs.

In the simplest design, an IoT device will not be allowed to communicate with IoT devices. All communications will happen via the corresponding I-Guardian and all transactions are mediated by an I-Guardian. The I-Guardian device terminates every communication to and from a T-Net, and it vets the transaction and processes it only if the transaction satisfies the T-Net security requirements. For example, if the transaction originator cannot be authenticated, or the transaction is authenticated but is found to be harmful, it will be (silently) rejected.

The important point is that an I-Guardian must not serve as a routing service between the inside and outside of T-Net, but make a transaction with an IoT device and with outer world independently. Thus, an I-Guardian is not identical to a conventional router, gateway, or a firewall. The behavior of an I-Guardian is somewhat similar to that of an application gateway, but it differs significantly from the conventional wisdom of an application gateway in that an I-Guardian is not application specific. It will serve various IoT devices and various I-Applications. This is a major difference from the enforcement mechanism proposed in [29].

D. Functional Requirements

The functional components required to realize the proposed societal model-based network are discussed below.

1) A Mechanism for Defining IoTInformationObjects: A virtual IoT information store lies at the core of the societal model. Objects in this virtual IoT information store are defined in an IIB. Each IoTInformationObject in the IIB is an abstraction of some facet of an IoT device, instances of which will be accessed via I-Guardians by I-Applications. The IIB must be a scalable, extensible, and maintainable in a multivendor, distributed environment.

An IoTInformationObjects will have a name, syntax and corresponding semantics. The access functions to an object would refer to the name of the object and its corresponding value. To handle various types of information, we will need a unique name space that scales globally from the operational and maintenance point of view and, a language to define the corresponding value, its syntax and semantics.

2) A Universal Access Protocol for IoTInformationObjects: A protocol will be required for communication of IoT-related information between an I-Application and an I-Guardian. Since operations on IoT devices are modeled as inspections or modifications of some "value" of the corresponding IoTInformationObject, the protocol operations would be modeled as simple GET and/or SET functions. The asynchronous notification would require an additional NOTIFY function.

By providing a universal access protocol, the development of I-Applications will be easier.

3) A Mechanism for Managing ThingNet Membership: When a new device joins a T-Net as an IoT device, it will be explicitly registered by an administrator. A similar process will be done when a member leaves the T-Net; it must be explicitly de-registered.

In our societal model, membership verification will be carried out based on strict authentication. It must not be based on trivially spoofable identities like IP address and/or MAC address. The mechanism must be strong and robust enough to ensure that a non-member will not have any access to members in the T-Net.

4) Group Security for ThingNet Members: A T-Net must have following mechanisms to provide group security for T-Net members.

- Ensuring that IoT devices communicate only with the designated I-Guardian.
- Detecting and notifying attempts of IoT devices to communicate with devices other than the designated I-Guardian.
- Ensuring that only known (member) devices are present in the T-Net.
- Ensuring that the designated I-Guardian is authentic.

Several off-the-shelf technologies may be utilized to realize the above mechanisms. For example, stateless and stateful filtering, misuse and anomaly detection used in existing firewalls and IDSs will be useful in detecting and preventing violation of T-Net group's rule. Layer 2 mechanisms may be used to control the flow of packets to and from the T-Net.

I-Guardian and IoT devices must collaborate to realize group security.

Basically, IoT devices and the designated I-Guardian will be made aware of each other through some registration process. Thereafter, member IoT devices will communicate only with the designated I-Guardian. If a member IoT device notices another IoT device is attempting to communicate with a device other than the I-Guardian, the IoT device should log that event and/or alert the I-Guardian. An advanced IoT device with the capability may block such illegal communication.

5) A Mechanism for Raising Alarms: It is common for everyday applications to raise an alarm to draw human attention. IoT devices must have a mechanism to alert an I-Guardian. The I-Guardian device will then use appropriate mechanisms to alert the designated Network Monitoring Systems or administrators. The alert mechanism must meet the basic security requirements, namely, confidentiality, integrity, availability, accountability, authenticity, and non-repudiation. It must also have provisions for describing the alert in terms of IoTInformationObjects corresponding to the IoT device. The latency of the alert will be an important issue.

IV. Feasibility of the Societal Model

In this section, we discuss the feasibility of our proposal through a proof-of-concept implementation based on the Internet standard management framework. Since the early days of Internet, researchers and engineers have been working on the challenging issue of a management architecture where in all networked (and other) devices could be managed in an open extensible and scalable framework. The problem has great similarities with the issues related to the societal model for IoT systems described above. This is the reason why we choose the Internet standard management framework as the first option for the proof-of-concept implementation.

In the Internet standard network management framework [30], Managed Objects (MOs) are accessed via a virtual information store, the Management Information Base or MIB and are accessed using the Simple Network Management Protocol (SNMP) [31]. The protocol uses simple constructs, GET, SET, NOTIFY and a few variations of these constructs to operate on the managed objects. The objects are defined using the Structure of Management Information (SMI) [32]. A side effect of this scheme is that, all operations on the managed devices are carried out via agents on the devices. Management application does not have "direct" access to the managed devices/entities. The managed devices are shielded by the agent which is expected to carry out the security procedures before acting on a request from a management application. This aspect serves the core requirement of protection for the IoT devices in the societal model.

By modeling an IoT device, or the corresponding Information Object as a managed object we can use all the features of the network management framework to access and manipulate IoT devices.

The agent, which serves as the guardian in the societal model context, provides access to the IoT devices via the *IIB*. The SNMP protocol constructs such as GET, SET and NOTIFY are used for communication between the I-Guardian and I-Applications.

The management information base is where the information objects will be defined. It has a distributed scalable and flexible framework that allows vendors to possess and maintain their own name space.

To summarize, the points of the proof-of-concept implementation of the societal model:

- IoT devices are represented by Information Objects in a virtual information store.
- The objects are named and defined using SMI constructs in a globally unique name space
- An I-Application in the Internet accesses the Information Objects in the virtual information store by interacting with an I-Guardian using the SNMP protocol.
- Security mechanisms, authenticity, confidentiality, integrity, and access control for the outer world are handled by the I-Guardian using mechanisms made available in the SNMP USM (User-based Security Model) [33] and VACM (View-based Access Control Model) [34]
- An alert from an IoT device is transmitted to destinations in the Internet with the asynchronous notification mechanism of Informs/Traps available in SNMP
- The addition and removal of members from a T-Net group will be manually handled by a T-Net administrator
- Simple group security in T-Net is provided using an off-the-shelf solution like a firewall

Figure 2 shows an overview of our proof-of-concept implementation.

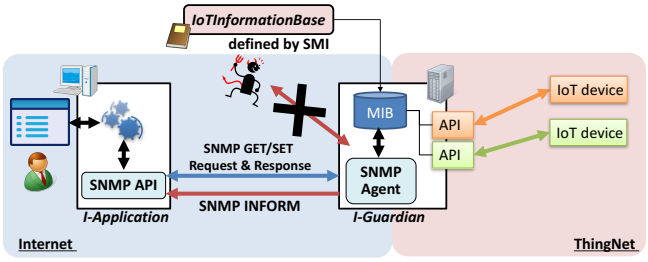

Fig. 2. Implementation overview

The proof of concept implementation uses NetSNMP [35], a widely available reference implementation of SNMP. We envisaged a smart home scenario where several IoT devices, such as thermometers, illuminometers, TVs, refrigerators, air-conditioners, smart keys etc., are used. We setup some Linux hosts to act as pseudo IoT devices. An I-Application and an I-Guardian are hosted on other Linux hosts.

Pseudo IoT devices are connected to a T-Net which is accessed via an I-Guardian. We designed a prototype MIB for a few IoT devices and implemented corresponding instrumentation for servicing the corresponding IoT information objects on the I-Guardian device.

An SNMP API and agent are deployed on the I-Application device and I-Guardian device respectively. A user will monitor and control IoT devices in her smart home using an I-Application. The SNMP agent plays the role of the I-Guardian. The I-Application sends appropriate SNMP requests along with the user's authentication information to the I-Guardian. The I-Guardian confirms the authenticity and corresponding authorization of the user. If the authenticated user has appropriate authority, the I-Guardian will attempt to service the request. Otherwise, the request is silently ignored. We have confirmed that an authentic user can monitor the status of IoT devices seamlessly and securely and an unauthorized attempt is neutralized by the security mechanisms.

In order to confirm that the group security inside the T-net is working, we connected an attacker node to the T-Net. The attacker tried to carry out a DoS attack against an IoT device and to log in to the IoT device using telnet. We have confirmed that neither of the attacker's trials were successful and the IoT device was protected.

V. Considerations

A. Differences from Traditional Security Models

The societal model differs from traditional perimeter defense measures like firewalls etc., in the following aspects.

- In the societal model, all transactions are terminated at an I-Guardian. Packets are not allowed to pass through beyond the I-Guardian under any circumstances.
- Communication with IoT devices is done under the auspices of the I-Guardian.
- Authorized members of a T-Net are not allowed to communicate with members other than their respective I-Guardians.

B. Advanced I-Applications

Advanced I-Applications may need efficient mechanisms to access large volumes of data. The issue of efficient and accurate data collection has been examined in the network management arena [36]. The authors show how a managed object aggregation MIB [37] will build complex aggregate MOs from simple MOs. This technique may be conveniently used to improve performance in cases where multiple instances of multiple objects need to be accessed periodically.

C. Downside of the Societal Model

- **Realtimeness**
  Since all transactions must be checked and validated by the I-Guardian, the "realtimeness" will be impacted. In order to minimize the additional delay incurred by the validation, an I-Guardian must be carefully designed to have the enough resource (CPU, memory, etc) for handling required number of transactions. In addition, the size of T-Net should be determined based on the required level of the realtimeness.
- **Robustness** An I-Guardian will be a single point of failure that will make the entire T-Net unavailable. The I-Guardian may be an additional target of spoofing by an attacker with grave consequences. Thus, the I-Guardian will be the focus of security and will require utmost care and consideration.

VI. Conclusion

In this paper, we have discussed the security aspects of Internet of Things (IoT), proposed a societal model that provides enhanced security and assessed the feasibility of the proposal. The societal model does look attractive with security risks greatly reduced by moving the onus of handling security

related matters from the potentially resource-constrained IoT device to a security proficient guardian IoT device. The feasibility of the societal model is established using off-the-shelf technology available in the Internet standard network management framework.

Security is a moving goal. At no point of time can we expect all the aspects of security to be fully understood and corresponding countermeasures to be in place. In this context, our proposal makes the IoT devices immune to security issues. Guardian IoT devices will handle security matters and, as such, security patches, fixes and updates will be carried out on the guardian(s). The IoT devices, some of which may be hidden out of sight and out of mind, will not be expected and/or required to be patched/secured/upgraded frequently. We believe this will be a significant advantage of delegating the security to the guardian(s).

We believe that security management of IoT devices based on the societal model will make society safer. In this paper, we limited ourselves to discussing only the simplest model where an IoT device can only communicate with its guardian in order to build the most secure environment. The more advanced and useful design where IoT devices will communicate with each other within a T-Net will bring more security threats and need further considerations.

REFERENCES

[1] R. Roman, P. Najera, and J. Lopez. Securing the Internet of Things. *IEEE Computer*, 44(9):51–58, Sept 2011.

[2] S. L. Keoh, S. S. Kumar, and H. Tschofenig. Securing the internet of things: A standardization perspective. *IEEE Internet of Things Journal*, 1(3):265–275, June 2014.

[3] Andy Greenberg. This Gadget Hacks GM Cars to Locate, Unlock, and Start Them,. WIRED, July 2015. http://www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/.

[4] Andy Greenberg. Hackers Remotely Kill a Jeep on the Highway—With Me in It. WIRED, July 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[5] Troy Hunt. Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs, February 2016. http://www.troyhunt.com/2016/02/controlling-vehicle-features-of-nissan.html.

[6] Jerome Radcliffe. Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System. In *BLACK HAT USA 2011*, August 2011.

[7] Daniel Cid. Large CCTV Botnet Leveraged in DDoS Attacks, June 2016. SUCURI Blog https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html.

[8] Daniel Cid. IoT Home Router Botnet Leveraged in Large DDoS Attack, September 2016. SUCURI Blog https://blog.sucuri.net/2016/09/iot-home-router-botnet-leveraged-in-large-ddos-attack.html.

[9] Pierluigi Paganini. 150,000 IoT Devices behind the 1Tbps DDoS attack on OVH, September 2016. http://securityaffairs.co/wordpress/51726/cyber-crime/ovh-hit-botnet-iot.html.

[10] Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, and Christian Rossow. IoTPOT: Analysing the Rise of IoT Compromises. In *9th USENIX Workshop on Offensive Technologies (WOOT 15)*, Washington, D.C., August 2015. USENIX Association.

[11] Jeffrey Voas. Networks of 'Things', July 2016. NIST Special Publication 800-183, http://dx.doi.org/10.6028/NIST.SP.800-183.

[12] IEEE IoT Initiative. Towards a definition of the Internet of Things, May 2015. http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.

[13] Hiroshi Tsunoda and Glenn Mansfield Keeni. Societal Model for Securitng Internet of Things. In *International Conference on Business and Industrial Research (ICBIR 2016)*, May 2016.

[14] Internet Society. The Internet of Things: An Overview, Oct 2015. http://www.internetsociety.org/doc/iot-overview.

[15] OWASP Internet of Things Project. Top 10 IoT Vulnerabilities (2014) Project, 2014. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Top_10_IoT_Vulnerabilities__282014_29.

[16] A. Grau. Can you trust your fridge? *Spectrum, IEEE*, 52(3):50–56, March 2015.

[17] Hewlett Packard Enterprise. Internet of things research study 2015 report, 2015. http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[18] Ari Keranen and Carsten Bormann. Internet of Things: Standards and Guidance from the IETF. *IETF Journal*, 11(3), April 2016.

[19] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. Mccann, and K. K. Leung. A survey on the IETF protocol suite for the internet of things: standards, challenges, and opportunities. *IEEE Wireless Communications*, 20(6):91–98, December 2013.

[20] P. Gope and T. Hwang. Bsn-care: A secure iot-based modern healthcare system using body sensor network. *IEEE Sensors Journal*, 16(5):1368–1376, March 2016.

[21] A. Sajid, H. Abbas, and K. Saleem. Cloud-assisted iot-based scada systems security: A review of the state of the art and future challenges. *IEEE Access*, 4:1375–1384, 2016.

[22] K. Xu, Y. Qu, and K. Yang. A tutorial on the internet of things: from a heterogeneous network integration perspective. *IEEE Network*, 30(2):102–108, March 2016.

[23] C. Alcaraz, P. Najera, J. Lopez, and R. Roman. Wireless sensor networks and the internet of things: Do we need a complete integration? In *1st International Workshop on the Security of the Internet of Things (SecIoT'10)*, Tokyo (Japan), December 2010. IEEE.

[24] Jaeho Kim, Jaeseok Yun, Sung-Chan Choi, Dale N Seed, Guang Lu, Martin Bauer, Adel Al-Hezmi, Konrad Campowsky, and JaeSeung Song. Standard-Based IoT Platforms Interworking: Implementation, Experiences, and Lessons Learned. *IEEE Communications Magazine*, July 2016.

[25] M. Shamim Hossain, Ghulam Muhammad, Sk Md Mizanur Rahman, Wadood Abdul, Abdulhameed Alelaiwi, and Atif Alamri. Toward End-to-End Biometrics-Based Security for IoT Infrastructure. *IEEE Wireless Communications*, October 2016.

[26] Ramao Tiago Tiburski, Leonardo Albernaz Amaral, Everton de Matos, and Fabiano Hessel. The Importance of a Standard Security Architecture for SOA-Based IoT Middleware. *IEEE Communications Magazine*, December 2015.

[27] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers. Twenty Security Considerations for Cloud-Supported Internet of Things. *IEEE INTERNET OF THINGS JOURNAL*, 3(3), June 2016.

[28] Yi-Bing Lin, Yun-Wei Lin, Chang-Yen Chih, Tzu-Yi Li, Chia-Chun Tai, Yung-Ching Wang, Fuchun Joseph Lin, Hsien-Chung Kuo, Chih-Chieh Huang, and Su-Chu Hsu. EasyConnect: A Management System for IoT Devices and Its Applications for Interactive Design and Art. *IEEE INTERNET OF THINGS JOURNAL*, 2(6), December 2015.

[29] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu. Handling a trillion (unfixable) flaws on a billion devices. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks - HotNets-XIV*, pages 1–7, 2015.

[30] J. Case, R. Mundy, D. Partain, and B. Stewart. Introduction and Applicability Statements for Internet-Standard Management Framework. RFC3410, December 2002.

[31] J. Case, M. Fedor, M. Schoffstall, and J. Davin. A Simple Network Management Protocol (SNMP). RFC1157, May 1990.

[32] Ed. McCloghrie, K., Ed. Perkins, D., and Ed. J. Schoenwaelder. Structure of Management Information Version 2 (SMIv2). STD 58, RFC 2578, April 1999.

[33] U. Blumenthal and B. Wijnen. User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). RFC3414, December 2002.

[34] B. Wijnen, R. Presuhn, and K. McCloghrie. View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). RFC3415, December 2002.

[35] Net-SNMP. Net-SNMP, 2013. http://www.net-snmp.org/.

[36] G. Mansfield, S. Karakala, T. Saitoh, and N. Shiratori. High Resolution Traffic Measurement. In *Proc. of A workshop on Passive and Active Measurements on the Internet(PAM2001)*, pages 67–73, 2001.

[37] G. Keeni. The Managed Object Aggregation MIB. RFC4498, May 2006. http://www.ietf.org/rfc/rfc4498.txt.