Journal of Business Administration and Languages
Vol.4 No.1 January - June 2016

Societal Model for Securing Internet of Things

Hiroshi TSUNODA[#1], Glenn Mansfield KEENI[*2]

[#]*Tohoku Institute of Technology*
35-1, Yagiyama Kasumi-cho, Taihaku-ku, Sendai-shi, Miyagi, 982–8577 JAPAN
[1]tsuno@m.ieice.org

[*]*Cyber Solutions Inc.*
ICR Bldg, 6-6-3, Minami Yoshinari, Aoba-ku, Sendai-shi, Miyagi, 989–3204 JAPAN
[2]glenn@cysols.com

***Abstract*-From transportation to home and health care, In- ternet of Things (IoT) has penetrated almost every sphere of society. In the IoT concept, devices communicate autonomously to provide services. A significant aspect of IoTs 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. Despite the fact that these devices require high level security, there has not been enough discussion on the security aspects of IoTs. In this paper, we propose a simple security model for IoT, the societal model. The basic concept of the model is borrowed from our human society. In the societal model, members play an important role in maintaining the security for the group. An IoT network mimics a society. IoT devices are members. Behavior of each member generally follows the group's norms. Abnormal behavior evokes some reaction which includes rejection and/or notification to appropriate authorities. This paper investigates the requirements for realizing secure IoT networks based on the societal model.**

I. Introduction

From transportation to home and health care, 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 network. This integration of physical devices with cyber space, has ushered in the concept of Cyber Physical Systems [1] wherein physical devices and the underlying processes may be ubiqui- tously accessed, monitored and controlled.

Cyber physical systems will bring in an entirely new gamut of services and applications. At the consumer end, the following applications and services will mature:

- driver-less cars by automatic control and braking mech- anisms
- smart homes with automatically controlled electrical appliances

In the industry, automated systems to monitor and control factory and plant processes will develop.

According to the forecast by Gartner, Inc. [2], processor costs will continue the downward trend below $1 to the point that connectivity will become a standard feature. They estimate that usage of IoT devices will grow to the extent that 26 billion units will be in use by 2020. McKinsey Global Institute [3] state that "the IoT has a total potential economic impact of $3.9 trillion to $11.1 trillion a year by 2025".

The significant aspects of IoTs that makes them stand apart from present day networked devices and applications are as below.

- there will be a very large number of devices, produced by diverse makers and used by an even more diverse group of users.
- the applications will potentially reside and function in what were very private sanctums of life e.g. the car, home and the people themselves.

Thus, IoT devices and systems are expected to require high level security. However, there has not been enough discussion on the security aspects of IoTs.

In this paper, we propose a simple security model for IoT, called societal model. The basic concept of the model is borrowed from our human society. Human society has a loose hierarchy with groups and subgroups. In one view the smallest group would be a nuclear family. Other groups would be the locality, school, ward, prefecture, state and so on. In the societal model, members play an important role in providing security to the group. An IoT network mimics a group in human society. IoT devices are members. Behavior of each member generally follows the group's norms. Abnormal behavior evokes some reaction which includes rejection and/or notification to appropriate authorities. This paper investigates the requirements for realizing secure IoT networks based on the societal model.

The remainder of the paper is organized as follows. Current status of IoT technologies and applications and its security related challenges are surveyed in Sec. II. In Sec. III, we pro- pose a simple security model, the societal model, for IoT. The concept and requirements of the societal model are discussed in this section. In Sec. IV we discuss the role of societal model in IoT security and considerations in implementing the societal model, followed by conclusions in Sec. V.

II. Internet of Things and Its Security Issues

A. Overview of Internet of Things

An IoT device can be modeled as a combination of the following three components as shown in Fig. 1.

1) Physical Input and/or Output
2) Computing capability
3) Network connectivity

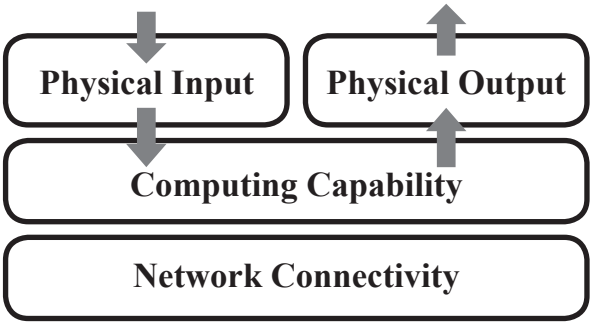

Fig. 1. Components of an IoT device

Some IoT devices have sensors which generate physical data via sensing. This physical data forms the input for the IoT devices. Some IoT devices provide output via actuators, speakers, or LED lights. A tiny embedded computer provides computing capability for IoT devices. Thanks to the computing capability, input and output can be controlled and automated by software. IoT devices may have one or more wired or wireless network interfaces. The data input to the IoT may be monitored remotely by accessing the device via a network interface. In a similar manner the output from IoT device may be controlled via a network interface.

A major difference between a conventional computing device and an IoT is the scope or purpose. Conventional computing devices such as personal computers and smart-phones 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 mechanical devices etc.

IoT devices may be used in very private sanctums of life e.g. in the car, inside the home and sometimes even inside the human body. Various critical infrastructures such as smart grid and energy plants are extensively deploying IoT devices for wide area monitoring and control. Security and privacy issues have become a major focus area for IoTs.

B. IoT Security

Various organizations have discussed IoT security issues from various point of view. IEEE spectrum did a special feature on IoT security in 2015 [4]. The Internet Society (ISOC) published an overview document of IoTs [5]. Security and privacy issues have been discussed in this document. Open Web Application Security Projects (OWASP) enumerates top 10 IoT vulnerabilities [6].

Actual vulnerabilities of various IoT devices were discussed in a survey by Hewlett Packard [7]. They analyzed various IoT devices such as TVs, webcams, home thermo-stats, door locks etc. Most devices used some form of cloud service. All devices included mobile applications that can be used to access or control the devices remotely. 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 [8], the authors propose an IoT honeypot and sandbox systems. They show that a significant number of IoT devices are compromised and are targets of malware infection.

In recent years, many 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 various vehicles made by several car vendors [9]–[11]. IoT devices are utilized for wellness and health care. In [12], 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. In 2010, Stuxnet worms attacked Iran's nuclear development program [13]. During the end of 2015, parts of Ukraine's energy grid went down for some time. It is believed that this incident was caused by cyber attacks using the DarkEnergy worm [14].

III. Societal Model for Secure IoT

A. Concept

The concept of the societal model is borrowed from our human society. It has a loose hierarchy with groups and subgroups. The nuclear family, a locality, school, ward, prefecture, state all are examples of groups. Security is taken care of to a certain extent within the groups. To a large extent the security mechanism seems to have held firm under diverse and even unanticipated circumstances. Thus, common building blocks of the security of our society will be useful for securing a complex IoT system. In this section, we discuss the building blocks of the societal model.

In the context of the societal model, we will assume that the basic unit in the IoT network society is a family. Thus, we would call this IoT network group a FAMINET (FAMIly NETwork).

In human society an average family will have children and adults. The membership of a family is well defined as is the hierarchy. Children will be protected by and cared for by adults (e.g., parents). The activities of children are limited and supervised by adults. The family privacy is well maintained, whereas within the family there is a degree of transparency (openness) or lack of privacy. Trespassing the family boundary is by default not allowed (by any member of the family). Abnormal behavior of a member, or presence of an outsider will be detected by a member who will raise an alarm of some sort. The alarm or action will be of the form of a report to an adult, seeking of external help, calling the emergency assistance line etc.

Based on the essence of security in human society, the concept for securing a IoT FAMINET is summarized in Fig. 2

In a IoT FAMINET, an enumeration of the members and their behaviors forms a rule. If any deviation from the rule is detected, a notification must be sent to appropriate authorities like an emergency call in a human society.

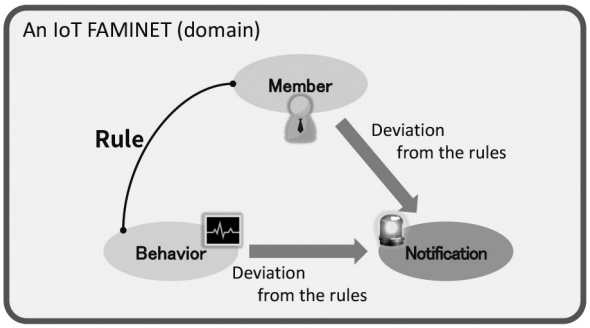

Fig. 2. Concept of the societal model

B. Network architecture

Similarly a family in human society, a **FAMINET** should be composed of following two types of devices:

1) *Child IoT (C-IoT)* devices
2) *Adult IoT (A-IoT)* devices

C-IoT devices are usual IoT devices designed for a dedicated purpose. A-IoT devices are devices that have enough resources and can conduct additional tasks for protecting C-IoT devices. C-IoT devices are not likely to have sufficient functions to ensure security for the devices itself and for the group it belongs to. Thus, like children in a human society, C-IoT devices will be under supervision of advanced A-IoT devices. A-IoT devices are further categorized into two types of device, Parent1 IoT (P1-IoT) device and Parent 2 IoT (P2-IoT) device based on the role in a FAMINET.

Fig. 3 illustrates the fundamental image of our IoT FAMINET in a smart home application. IoT FAMINET will be located adjacent to the home network in a smart home and connected to the Internet via the home network. A FAMINET gateway is a P1-IoT device. A FAMINET controller is a P2- IoT device and will take care of C-IoT devices.

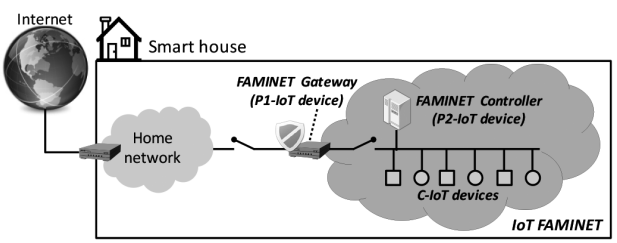

Fig. 3. Fundamental image of IoT FAMINET

In the next subsection, we will give a detailed discussion on the roles of A-IoT devices and other requirements of the societal model.

• Partially connected network

Considering a family in human society, unknown members never exist in the family. No ambiguity exists in the definition of members. Moreover, there are some disciplines or customs about their behavior. Similarly, in the societal model, unknown IoT devices never exist in a FAMINET and permitted behaviors of each device should be strictly defined. An P2-IoT device will have the responsibility to make this concept possible.

In a human society, we make an emergency call to the police if an emergency happens. Thus, notification is the life line of the society. IoT FAMINET also should have notification methods. C-IoT devices will send notifications to A-IoT devices. A-IoT devices will send notifications to an administrator.

Children are not allowed to talk with unknown people. Similarly, C-IoT devices will not directly communicate with any device outside the FAMINET. Only an P1-IoT device will have the responsibility to communicate outside the domain. Direct transaction between C-IoT devices and any device outside the domain is prohibited. For protecting the FAMINET and its members, an P1-IoT device must carefully investigate the information which it receives in all respects. The information will be sent to the destination only if the P1-IoT device decides that the information is secure and reliable. The FAMINET should be a partially connected to the externally network in the sense that the default state is 'disconnected'. Only when there is a requirement, the P1-IoT device of the FAMINET will establish a connection.

In the rest of this subsection, the requirements are discussed in detail.

1) Strict definition of members and its behaviors: Members and allowed behaviors for each member must be strictly defined. When a user starts to use a new device in her IoT FAMINET, the user must register the device in the member list. The user must also define the normal (allowed) behavior of the device. For example, air conditioners are allowed to obtain temperature information from temperature sensors because air conditioners require room temperature information for adjusting room temperature. Without such valid purpose, no device is allowed to get temperature information from sensors. These definitions work as rules in an IoT FAMINET domain.

Tables. I and II illustrate brief examples of member list and behavior rules.

TABLE I
EXAMPLE OF MEMBER LIST

Address	Device type	Location
192.168.0.1	FAMINET Gateway	Living room
192.168.0.2	Temperature Sensor	Living room
192.168.0.3	Temperature Sensor	Living room
192.168.0.4	Temperature Sensor	Bed room
192.168.0.5	Light	Living room
192.168.0.6	Light	Bed room
192.168.0.7	Air conditioner	Living room
:	:	:
192.168.0.254	FAMINET Controller	Living room

TABLE II
EXAMPLE OF BEHAVIOR LIST

From	To	Period	Oper.	InfoType	Value
FAMINET Controller	Temp. Sensor	00:00-23:59	Get	Temp.	-
FAMINET Controller	Air conditioner	00:00-23:59	Set	Temp.	-
FAMINET Controller	Room key	06:00-21:00	Set	StateLock	False
Room key	FAMINET Controller	00:00-23:59	Notify	StateLock	True

2) *FAMINET controller*: IoT FAMINET requires a special device to provide the following functions.

- Managing members and its behaviors rules
- Monitoring status of IoT devices
- Supporting information exchange between family members

We would call this device a FAMINET controller.

A FAMINET controller should know about every member and everything that happens in the FAMINET. It should also enforce security policies in FAMINET on every member. The controller raises an alarm if it finds unknown members, abnormal status of members, and/or violation of some security policy. In short, a FAMINET controller works like a parent in a family.

3) FAMINET gateway: A gateway will be required to interface between an IoT FAMINET and other networks. It acts like a parent and protects family members.

A FAMINET should not always be connected to other networks for strict security purpose. For securing IoT FAMINET, a gateway connecting other networks and IoT FAMINET establishes the connection only in case it is required. Otherwise, IoT FAMINET is independent from other networks in order to avoid unwanted data flow from outside the domain.

Moreover, no direct transaction between an IoT device inside the domain and any device outside the domain even when the connection is established. Every communication between IoT FAMINET and the outside world must be terminated at the gateway. The gateway carefully investigates the contents of the communication and sends it to the destination only if the contents do not violate the rules in IoT FAMINET.

4) Notification scheme: Notification is the life line of a society. Every IoT device must have a way to send notification to the controller or an administrator when it detects illegal or anomalous event. The notification method must fulfill the basic security requirements: confidentiality, integrity, availability, accountability, authenticity, and non-repudiation. For taking quick action against detected events, notification requires some levels of realtime-ness.

5) Scalabe information model: IoT devices are dedicated purpose devices basically designed for very specific functions. Thus different types of IoT devices will handle different types of information. Hence, it is expected that a wide variety of information is handled in IoT FAMINET. For example, an IoT device with a thermometer will receive a request and provide temperature information. Similarly, an IoT device illuminometer will provide the intensity of illumination. A smart key will provide the current status of key locks and may accept a request for changing the status of key locks.

To handle various types of information, we need a unified information model. The information model should also be scalable and flexible.

6) Transparency of inside communication: Like a family in real space, communication in an IoT FAMINET requires some degrees of transparency.

At least, a FAMINET controller must be able to know which IoT device is talking with who, in order to protect IoT devices from communicating with unknown devices both inside and outside the FAMINET domain. Transparency will enable mutual surveillance. IoT devices can monitor each other and send alarms to the controller when they detect any violation of family rules.

IV. CONSIDERATIONS

A. The societal model's role in IoT security

In [5] ISOC has outlined the security issues related to IoT deployments as follows.

- Massive deployment
- Device homogeneity
- Relatively long lifetime
- Difficulties in upgrading
- Little real visibility
- Poor physical security
- Difficulty in noticing devices and in monitoring its operational status and/or activities
- Privately developed device

In [6] OWASP has enumerated the security vulnerabilities observed in IoT devices.

- Insecure Web Interface
- Insufficient Authentication/Authorization
- Insecure Network Services
- Lack of Transport Encryption/Integrity Verification
- Privacy Concerns
- Insecure Cloud Interface
- Insecure Mobile Interface
- Insufficient Security Configurability
- Insecure Software/Firmware
- Poor Physical Security

In the following we discuss security related issues in the context of our proposed societal model.

1) Massive deployment: IoT devices will be deployed on a massive scale. The large number of deployed devices itself makes security a challenging issue. That issue gets even more complicated when these devices communicate with each other and/or with the Internet in an unpredictable and dynamic fashion.

In the societal model, every device belongs to the domain where its activities will be supervised and monitored. Each device is allowed only predefined and limited behavior. Un- predictable behavior will not be expected and when observed will raise alarms.

2) Device homogeneity: Homogeneity magnifies the potential impact of any single security vulnerability as

several similar devices will be deployed.

In the societal model since the devices are under supervision, an administrator of the domain can take appropriate action for the vulnerable devices. This could include shutting off the vulnerable devices.

3) Relatively long lifetime: Security mechanisms that were adequate at deployment time might not be adequate for the lifespan of the device as security threats continue to evolve.

The administrator of the concerned domain may decide to deactivate the device as and when the security mechanisms are found to be inadequate.

4) Difficulties in upgrading: Many IoT devices are intentionally or unintentionally designed without any provisions for firmware upgrade. In some cases the upgrade process is cumbersome and/or impractical.

The administrator of the concerned domain may decide to deactivate the device as and when the security mechanisms are found to be inadequate.

5) Little real visibility: User has little or no real visibility of the internal workings of the device or the precise data streams they produce. A device might be performing unwanted functions or collecting more data than the user intends.

In the societal model such devices will not be allowed in a secure domain. The activities of the device within the domain must be transparent and explicitly allowed.

6) Poor physical security: IoT devices are likely to be deployed where physical security is difficult or impossible. Attackers may have direct physical access to IoT devices.

In places where the physical security is a concern, the administrator is expected to be responsible to ensure the physical security and/or not deploy the device and/or declare the domain insecure.

7) Difficulty in noticing devices and in monitoring its operational status and/or activities: A security breach might persist for a long time before being noticed.

In the societal model, a primary requirement is that the presence of the device, its status and activities will be transparent within the domain. And any unusual activity will be quickly detected by other members (devices) or the supervisor.

8) Privately developed devices: Privately developed devices may not apply industry best practice security standards. Irrespective of the origin of the device, the domain rules of the societal model are a primary requirement. Any device that does not comply with the requirements will not be allowed as a member of the domain, or the domain will be insecure.

9) Insecurity and insufficiency in various functions, interfaces, services: As OWASP has enumerated, there are many concerns about insecurity and insufficiency in various aspects of IoT devices and services. For example, an insecure web interface enables attackers to perform account enumeration. It may not have account lockout function and may allow the use of weak password and credentials. Lack of transport encryption may cause the leakage of personal information and incur privacy issues.

In the societal model, every device should be investigated before it is registered to a member list. Devices having insecure functions/interfaces/services will not be allowed to join the IoT FAMINET. A FAMINET controller will have a responsibility for checking the security level of every child (IoT device).

B. Authentication of members

Authentication of members is a basic requirement in the societal model. Access control will be carried out based on strict authentication of members. A non-member will not have any access and/or presence in the IoT FAMINET.

In the societal model, the authentication will be based on information that is cosmetic or superficial. For example, network address-based authentication will not be sufficient as it is well-known that network addresses are easily spoofed. In human society authentication is much more than just matching names.

In one scenario, it is envisaged that an IoT device will be issued public and private key pair by the FAMINET controller when the device is registered as a member (adopted into the FAMINET). An IoT will authenticate itself to other members of the FAMINET, using its private key. The FAMINET con- troller will serve as CA (Certificate Authority) and guarantee the validity of public keys. The FAMINET Controller is the repository of trust in the FAMINET.

C. Scalable information model

For scalable and flexible operations, the naming of IoT devices and their functions will be a critical issue. Various naming schemes have been proposed and are used in the Internet. Examples are domain names in DNS (Domain Name System), URI (Uniform Resource Identifier), OID (Object IDentifier) in SNMP (Simple Network Management Protocol). This existing knowledge will be useful in designing the information model and naming scheme for the societal model. Moreover, it is required to investigate the applicability of existing communication protocols to the societal model. In IoT area, several light-weight protocols such as CoAP (Constrained Application Protocol) [15] and MQTT (MQ Telemetry Transport) [16], are proposed. Information model and naming schemes in these protocols should be evaluated in the context
of the societal model.

D. Notification scheme

Syslog [17] is a promising candidate for the notification scheme. It is a light-weight protocol and has been widely used from the early days of the Internet to convey event notification messages. Despite syslog's wide usage, due to lack of standards, interoperability problems like inconsistency in the format of syslog messages existed among implementations. However, through the activities of IETF syslog Working Group [18] from 2000 to 2010, various aspects of syslog have been enhanced and standardized. RFC 5424 [17] describes the standard format of syslog messages and the fundamental layered architecture of syslog pro- tocol. On the basis of RFC 5424, some transport

mappings for the transmission of syslog messages were standardized. These are the encryption and authentication of syslog messages using Transport Layer Security (TLS) [19], the basic transport for syslog messages over UDP/ IPv4 or UDP/IPv6 [20], and the secure connectionless transport of log messages using Datagram Transport Layer Security (DTLS) [21]. Signed syslog [22] describes the signing of a syslog message for origin authentication, message integrity and so on.

However, the management aspect of syslog continues to be neglected. The standardization effort for syslog monitoring and management has not progressed beyond the definition of tex- tual conventions published as RFC 5427 [23] in 2009. Without a standard framework for monitoring and management, little can be said about the operations of the syslog system let alone guarantee its reliability and availability. It means that reliability and availability of IoT FAMINET depending on the notification using syslog becomes doubtful.

Therefore, the management aspect of syslog must be discussed. Active development of management technology for syslog is required.

E. Transaction between inside and outside of a FAMINET

Every transaction is mediated by an P1-IoT device Every communication between inside and outside of a FAMINET is terminated at the P1-IoT device. Then the P1-IoT device checks the payload in a transaction if the transaction has per- mission according to the rules in a FAMINET. Only permitted transactions are handed over from the outside to the inside, and vice versa. For example, no transaction should be allowed if an originator cannot be authenticated. A request which may incur depletion of re-source in any IoT device in the FAMINET must be filtered.

V. CONCLUSION

In this paper, we have discussed the security aspects of Internet of Things (IoT) and proposed a new security model, the societal model.

While IoTs are a promising technology with far reaching applications and consequences in our daily life and industrial activities, attention should be paid to problems arising out of IoT technology. Most of the existing IoT devices are dedicated-purpose, tiny, resource-limited, immature devices. Conventional measures for security may not be appropriate for IoT devices and their network.

The concept of the societal model is borrowed from our human society. In the societal model, an IoT network is considered as a family where every member knows the others. IoT devices are considered as children in a family. Children must be taken care of by other mature devices (adults).

We have presented the concept and requirements of the societal model. We have discussed the role of the societal model in IoT security and suggested means of implementing the proposed model.

We believe that security management of IoTs based on the societal model will make society safer.

REFERENCES

[1] A. L. Edward, "Cyber Physical Systems: Design Challenges," in 2008 *11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, Orlando, FL, USA, 2008, pp. 363–369.

[2] STAMFORD Conn, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020," *newsroom*, 2013. [Online]. Available: http://www.gartner.com/newsroom/id/2636073.

[3] M. James, C. Michael, B. Peter, W. Jonathan, D. Richard, B. Jacques, and A. Dan, "Unlocking the potential of the Internet of Things," McKinsey Global Institute, 2015.

[4] G. Alan, "Can you trust your fridge?," *IEEE Spectrum*, vol. 52, no. 3, pp. 50 - 56, 2015.

[5] Internet society, "The Internet of Things (IoT): An Overview," *internet society*, 2015. [Online]. Available: http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf.

[6] Open Web Application Security Project (OWASP), "Top 10 IoT Vulnerabilities (2014)," 2015. [Online]. Available: https://www.owasp.org/index.php/Top_10_IoT_Vulnerabilities_(2014).

[7] Hewlett packard enterprise, "Internet of things research study," 2015. [Online]. Available: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[8] P. P. Yin Minn, S. Shogo, Y. Katsunari, and M. Tsutomu, "IoTPOT: Analysing the Rise of IoT Compromises," presented at the 9th USENIX Workshop on Offensive Technologies (WOOT 15), Washington, D.C., 2015.

[9] G. Andy, "This Gadget Hacks GM Cars to Locate, Unlock, and Start Them (UPDATED)," *Wired*, 2015. [Online]. Available: https://www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/.

[10] G. Andy, "Hackers Remotely Kill a Jeep on the Highway-With Me in It," *Wired*, 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[11] H. Troy, "Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs," 2016. [Online]. Available: https://www.troyhunt.com/controlling-vehicle-features-of-nissan/.

[12] R. Jerome, "Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System," 2011. [Online]. Available: https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf.

[13] K. Stamatis, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society*, Crown Conference Centre Melbourne, Vic, Australia, 2011, pp. 4490–4494.

[14] P. Jose, "Scary questions in Ukraine energy grid hack," *CNN Money*, 2016. [Online]. Available: http://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/.

[15] C. Bormann, K. Hartke, and Z. Shelby, "The Constrained Application Protocol (CoAP)," *RFC 7252*, 2014. [Online]. Available: https://tools.ietf.org/html/rfc7252.

[16] International Business Machines Corporation (IBM) and Eurotech, "MQTT V3.1 Protocol Specification," 2010. [Online]. Available: http://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt-v3r1.html.

[17] R. Gerhards, "The Syslog Protocol," *RFC* 5424, 2009. [Online]. Available: https://tools.ietf.org/html/rfc5424.

[18] IETF Datatracker, "Security Issues in Network Event Logging (syslog)," 2016. [Online]. Available: https://datatracker.ietf.org/wg/syslog/charter/.

[19] F. Miao, Y. Ma, Huawei Technologies, J. Salowey, and Cisco Systems, Inc., "Transport Layer Security (TLS) Transport Mapping for Syslog," *RFC 5425*, 2009. [Online]. Available: https://tools.ietf.org/html/rfc5425.

[20] A. Okmianski and Cisco Systems, Inc., "Transmission of Syslog Messages over UDP," *RFC 5426*, 2009. [Online]. Available: https://tools.ietf.org/html/rfc5426.

[21] J. Salowey, Cisco Systems, Inc., T. Petch, Engineering Networks Ltd, R. Gerhards, H. Feng, and Huaweisymantec Technologies, "Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog," *RFC 6012*, 2010. [Online]. Available: https://tools.ietf.org/html/rfc

[22] J. Kelsey, NIST, J. Callas, PGP Corporation, A. Clem, and Cisco Systems, "Signed Syslog Messages," *RFC 5848*, 2010. [Online]. Available: https://tools.ietf.org/html/rfc5848.

[23] G. Keeni and Cyber Solutions Inc., "Textual Conventions for Syslog Management," R*FC 5427*, 2009. [Online]. Available: https://tools.ietf.org/html/rfc5427.