Internet of Things (IoT): Smart and Secure Service Delivery

ELISA BERTINO, Purdue University

KIM-KWANG RAYMOND CHOO, University of Texas at San Antonio

DIMITRIOS GEORGAKOPOLOUS, Swinburne University of Technology

SURYA NEPAL, CSIRO Data61

The Internet of Things (IoT) is the latest Internet evolution that incorporates a diverse range of things such as sensors, actuators, and services deployed by different organizations and individuals to support a variety of applications. The information captured by IoT present an unprecedented opportunity to solve large-scale problems in those application domains to deliver services; example applications include precision agriculture, environment monitoring, smart health, smart manufacturing, and smart cities. Like all other Internet based services in the past, IoT-based services are also being developed and deployed without security consideration. By nature, IoT devices and services are vulnerable to malicious cyber threats as they cannot be given the same protection that is received by enterprise services within an enterprise perimeter. While IoT services will play an important role in our daily life resulting in improved productivity and quality of life, the trend has also “encouraged” cyber-exploitation and evolution and diversification of malicious cyber threats. Hence, there is a need for coordinated efforts from the research community to address resulting concerns, such as those presented in this special section. Several potential research topics are also identified in this special section.

Categories and Subject Descriptors: C.2.2 [Security and Privacy]: Systems Security

General Terms: Applied Cryptography, Network Security

Additional Key Words and Phrases: Internet of things, security and privacy

ACM Reference Format:

Elisa Bertino, Kim-Kwang Raymond Choo, Dimitrios Georgakopolous, and Surya Nepal. 2016. Internet of things (IoT): Smart and secure service delivery. *ACM Trans. Internet Technol.* 16, 4, Article 22 (December 2016), 7 pages.

DOI: <http://dx.doi.org/10.1145/3013520>

1. BACKGROUND

Recent advances in sensing technologies, online social networking, the Internet of Things (IoT), and mobile and cloud technologies are blurring the boundaries between the physical, social, and cyber worlds, fueling the astonishing growth of internet users (from 1.158 billion in 2007 to 3 billion in 2014) and internet-connected devices (to 15 billion in 2014), and resulting in an explosion of data produced from a myriad of internet-connected devices and social networks.

Despite an expanding array of business, government and scientific applications that require distilling knowledge from big IoT cyber-physical and social (cyber-social) data,

Authors' addresses: E. Bertino, CS Dept., LWSN Bldg., Purdue University, West Lafayette, IN 47907, USA; email: bertino@purdue.edu; K.-K. R. Choo, Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249-0631, USA; email: raymond.choo@fulbrightmail.org; D. Georgakopoulos, Department of Computer Science and Software Engineering, Swinburne University of Technology, John St, Hawthorn, Victoria, 3122, Australia; email: dgeorgakopoulos@swin.edu.au; S. Nepal, CSIRO Data61, Corner of Vimiera and Pembroke Road, Marsfield NSW 2122, Australia; email: surya.nepal@data61.csiro.au.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies show this notice on the first page or initial screen of a display along with the full citation. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, to redistribute to lists, or to use any component of this work in other works requires prior specific permission and/or a fee. Permissions may be requested from Publications Dept., ACM, Inc., 2 Penn Plaza, Suite 701, New York, NY 10121-0701 USA, fax +1 (212) 869-0481, or permissions@acm.org.

© 2016 ACM 1533-5399/2016/12-ART22 \$15.00

DOI: <http://dx.doi.org/10.1145/3013520>

there is no easy way to exploit such big data, particularly in real-time, or develop secure IoT-based services. The ability to harness such big data has become a priority for researchers, organizations, and governments. However, it also raises important questions and introduces new challenges for the security of IoT-based services and the privacy of individuals.

In particular, as discussed by Bertino [2016], IoT systems are high security risks for several reasons. They do not have well-defined perimeters, are highly dynamic, and continuously change because of mobility. In addition, IoT systems are highly heterogeneous with respect to the communication medium and protocols, platforms, and devices. IoT systems may also include “objects” not designed to be connected to the Internet. Finally, IoT systems, or parts of them, may be physically unprotected and/or controlled by different parties. Attacks, against which there are established defense techniques in the context of conventional information systems and mobile environments, are thus much more difficult to protect against in the IoT. Also human interaction is not scalable in IoT devices and this makes it difficult for security analysts or end-users to carry out security activities, such as approving the granting of permissions to devices, and setting up access control policies and configurations. Addressing such security challenges requires revisiting or substantially extending current security solutions.

2. ARTICLES IN THIS SPECIAL ISSUE

This special section is dedicated to reporting cutting-edge research with a particular emphasis on novel and innovative techniques to ensure the security and privacy of IoT-based services and users. We received 22 submissions for this special issue, of which 5 were accepted for publication (i.e., $\sim 23\%$ acceptance rate). Each article went through a rigorous peer review process, in addition to multiple follow-up rounds with the authors. We will now summarize the articles below, before identifying research issues and challenges.

We categorize five papers in this special issue into two broad categories in terms of the solutions presented: cryptographic solutions, and vulnerability, and intrusion identification. Within cryptographic solutions, three articles were selected to address two key research issues: access control mechanism [Duan et al. 2016] and key establishment protocol [Zhang et al. 2016; Saxena et al. 2016]. Similarly, within vulnerability and intrusion identification, one article is selected in each area of vulnerability assessment [Siboni et al. 2016] and another article in the area of intrusion detection [Saeed et al. 2016].

2.1. Cryptographic Solutions

In our increasingly data-centric society, the capability to authenticate users and devices, and provide a secure means of online collaboration is crucial in promoting productivity. Access control schemes and authenticated key exchange schemes are two such solutions [Shebaro et al. 2015; Yang et al. 2015b].

Access Control Mechanism. In this special issue, Duan et al. [2016] present a data-centric access control framework designed to provide secure access control for smart-grid services in a publish/subscribe model. In their approach, a fully homomorphic encryption scheme and bloom-filter-encoded control policies and access credentials are used as the underpinning techniques to preserve the indirect, anonymous, and multi-cast features required in publish/subscribe communications.

Key establishment schemes or protocols, such as key agreement and key exchange, have been widely studied in the literature. In particular recent work has focused on developing and benchmarking lightweight key management protocols [Seo et al. 2016] and on designing scalable, distributed authentication infrastructures [Milagro Project

2016]. However, there are still worthwhile contributions to be made, perhaps because the design of provably secure schemes or protocols is still challenging [Boyd 2003; Choo 2009]. This is the gap that Zhang et al. [2016] and Saxena et al. [2016] seek to address in this special issue.

Key Establishment Schemes or Protocols. In this special issue, two articles are presented to address this issue: Zhang et al. [2016] propose a password-authenticated group key exchange protocol and prove its security in the standard model. However, unlike most previous protocols, the proposed protocol does not require the short passwords to be pre-shared among users. Saxena et al. [2016] explain the limitations in the evolved packet system-based authentication and key agreement protocol of the long-term evolution (LTE) network, and design a lightweight authentication and key agreement protocol to support secure and efficient communications between IoT devices and their users.

2.2. Vulnerability and Intrusion Identification

In addition to designing secure cryptographic schemes to ensure the confidentiality, integrity and availability of services and data in an IoT deployment, it is important to acknowledge that we will not achieve perfect security. Therefore, we need to be able to constantly evaluate and identify any vulnerabilities and design flaws in the software and system deployed in the IoT (and other networked) infrastructure, such as those reported by Do et al. [2016] and Li et al. [2016].

Vulnerability Assessment. It can be an expensive exercise for IoT software and system developers to subject their products to extensive testing prior to market. This is an observation shared by Siboni et al. [2016] in this special issue. Therefore, the authors present a security testbed framework that allows wearable device designers and manufacturers to evaluate the security of the devices in a simulated environment.

Intrusion Detection. Similar to cryptographic research, intrusion detection and prevention is an area that has been actively researched upon but remains one of ongoing interest and relevance [Kamra and Bertino 2011; Prokhorenko et al. 2016]. In this special issue, Saeed et al. [2016] reiterate the importance of having the capability to detect intrusion in the IoT infrastructure in real-time. The authors then present an intrusion detection and prevention scheme based on random neural networks, and demonstrate the utility of their scheme is validated in an experimental IoT environment.

3. RESEARCH CHALLENGES

Even though the articles in this special issue propose timely and interesting solutions to security for IoT, they certainly do not cover all the aspects of IoT security. Much more work needs to be done along several directions, including: device discovery, identification, and authentication; secure device locations; analysis and protection of firmware; and IoT software management, including patch management. We briefly describe a few key IoT security challenges below.

Middleware Security. The IoT middleware is one of the key components in the realization of IoT services, which led to the development of a number of IoT middleware solutions such as OpenIoT, Hydra, GSN, and Ptolemy Accessor Host. Ngu et al. [2016] studied and classified these different types of IoT middleware solutions into three different categories, namely: Service-based, Cloud-based, and Actor-based. They observed that none of these IoT middleware solutions is designed with security as a built-in feature. The troubling part is that these middleware solutions have been used and deployed in many real-life applications. The secure service delivery in IoT relies

on the security features offered by the middleware. Hence, building trustworthy IoT middleware still remains an open research and development challenge.

Device Authentication. In IoT services, a lightweight device interacts with either other lightweight devices or a powerful cloud-based server. IoT devices often operate in low radio frequency and hence have limited capacity to transmit large messages. Furthermore, many IoT devices are lightweight, i.e., they have limited battery power. Due to these reasons, many traditional authentication protocols cannot be used on IoT devices. A number of existing solutions based on AE, ECC, and NTRU have been proposed in the literature. ECC-based solutions are highly popular and widely used due to their tested and verified security features. However, they are not the most efficient solutions in the literature. The key research challenge is to develop a mutual authentication protocol that provides high efficiency without compromising security and privacy. Another critical research challenge is the concurrent execution of multiple authentication requests among devices with different computing power, as often devices need to manage authenticated communications at the same time. Notable examples include communications in vehicular communications networks and communications between drones and sensors on the ground [Won et al. 2015]. Yang et al. [2015a] suggested a paradigm shift in designing security solutions for IoT systems. Specifically, the authors suggested that “rather than focusing on designing lightweight and individual cryptographic primitives, security solution designers should consider taking a whole-of-system approach to achieve system/collective lightweight-ness, outsource expensive computations from resource-constrained field devices to neighboring devices and equipment with more computational capacity, and selectively protect critical data (partial/selective protection of data of interest).

Vulnerability and Patch Management. An IoT system can include a large number of small mobile devices, deployed in an open environment. It is critical to patch IoT devices in time for various purposes, such as improving their security features to close vulnerabilities and adding new functionalities. However, unlike ordinary computing systems, the constrained embedded IoT devices are always not patchable, due to the limited computation and communication capability. For a large IoT network, which is usually not a fast network, the download of patches by all IoT devices at the same time may cause the traffic congestion problem. IoT devices might not always be connected to a patch distribution server in the external network. In this case, IoT devices are even harder to patch, since patches cannot be distributed in a usual way by downloading from the patch sever with a reliable network connection. Furthermore, a patch distribution protocol might be exploited to launch denial-of-service (DoS) attacks or attacks that drain the battery of IoT devices. The open question is how to perform the secure and reliable patch of IoT devices with limited device and communication capacities.

Data Stream Security. In many IoT services, the sensing devices capture the data from the deployed environment and send to the cloud-based server for analysis. In real-time services, the data is transmitted as data streams. Data Stream Manager (DSM) at the server collects the data streams to perform real-time analysis and decision-making. Securing such data streams is an open research challenge. The challenges include maintaining confidentiality and integrity of the data stream, verifying the authenticity of the data in real-time, etc. [Puthal et al. 2016b]. Selective encryption in conjunction with the well-researched information flow control techniques is one of the promising approaches that can be further investigated to address the problem.

Identity and Access Management. IoT services are offered through coordination of a large number of IoT devices that communicate with each other and are required to perform mutual authentication. Thus, they need to manage more identities than any existing Identity and Access Management (IAM) systems. Cloud Security Alliance

[CSA 2015] provides several recommendations and guidelines to manage the identities in IoT system. The other complex issue in IoT is the relationships between identity and ownerships. The ownership might change over the duration of the IoT service lifecycle from the manufacturer to different users and administrations. The challenge is how to protect the device identity from abuse so that it can be used to support device authentication. The blockchain technology, which supports decentralized trust, could be potentially exploited to support identity management in IoT system rather than a centralized certificate authority.

Device Discovery. IoT systems can have a large number of devices at one time, and most often than not these devices are difficult to discover in an open environment. Device discovery is needed for a number of practical reasons such as device recovery, device-to-device communication, and device software maintenance. It is also important that only authenticated “things” could locate and discover the devices so that they do not become easy targets of malicious users. The challenge is compounded when the discovery operation has to be performed in a difficult terrain for lightweight devices. Techniques such as Secure Device Discovery and Recovery (SDDR) proposed for mobile devices and applications [Lentz et al. 2014] could be potentially deployed for IoT systems.

Perimeter Defense. The enterprise system is protected by traditional perimeter defense mechanisms. However, this protection may not be effective for IoT systems. Heterogeneous devices (i.e., different devices from different vendors) can be connected to the network at any time and offering potential entry points. A new approach is needed, where only data from authenticated and authorized devices whose software and location have been pre validated and deemed acceptable are transferred to cloud data centers. Three promising approaches that have been surfaced in recent times, namely: zero trust, deperimeterization and software-defined perimeter (SDP) [Puthal et al. 2016a]. Further research and development is needed to evaluate and refine these approaches.

Access Control. The access control mechanisms limit the privileges of device components and applications so that they can only access the resources required to perform their tasks. One of the key advantages of such access control mechanisms is that even if a device is compromised, the intruder may not have the privilege to access sensitive information. Developing access control mechanisms for lightweight IoT devices is a challenging research problem.

4. CONCLUDING REMARKS

IoT systems introduce a large number of vulnerabilities as each single device represents a potential risk and is a potential attack vector. The hardware, firmware as well as applications running on these devices could potentially provide backdoors for unauthorized access. Transparent and usable management of security in IoT systems demand development of novel techniques using multi-disciplinary approaches. Just like the Internet services, IoT services will evolve along with the emergence of new vulnerabilities and threats. There is no silver bullet that can effectively solve all security issues and challenges in IoT systems. Further research and development is needed to mitigate the threats and close the vulnerabilities. We expect IoT security will remain as an active area of research in the foreseeable future.

ACKNOWLEDGMENTS

The authors would like to thank all reviewers who have provided reviews on time and ACM TOIT editorial board and administration, more specifically Editor-In-Chief Prof. Munindar P. Singh and Ms. Jayel Tecson

from editorial support services. Without their help and support, this special issue would not have been possible.

REFERENCES

- Elisa Bertino. 2016. Data Security and Privacy in the IoT. Keynote Summary, *Proceedings of EDBT 2016*.
- Colin Boyd. 2003. Protocols for Authentication and Key Establishment. In *Information Security and Cryptography*, Springer
- Kim-Kwang Raymond Choo. 2009. Secure Key Establishment. *Advances in Information Security* 41, Springer
- CSA. 2015. Identity and Access Management for the Internet of Things - Summary Guidance. <https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf> (accessed Oct 13, 2016).
- Quang Do, Ben Martini, Kim-Kwang Raymond Choo. 2016. A Data Exfiltration and Remote Exploitation Attack on Consumer 3D Printers. *IEEE Trans. Inf. Foren. Secur.* 11, 10, 2174–2186.
- Li Duan, Dongxi Liu, Yang Zhang, Shiping Chen, Ren Ping Liu, Bo Cheng, and Junliang Chen. 2016. Secure Data-centric Access Control for Smart Grid Services based on Publish/Subscribe Systems. *ACM Trans. Internet Tech.*
- Ashish Kamra and Elisa Bertino. 2011. Design and Implementation of an Intrusion Response System for Relational Databases. *IEEE Trans. Knowl. Data Engin.* 23, 6, 875–888.
- Matthew Lentz, Viktor Erdélyi, Paarijaat Aditya, Elaine Shi, Peter Druschel, and Bobby Bhattacharjee. 2014. SDDR: Light-weight, Secure Mobile Encounters. In *Proceedings of the 23rd USENIX Security Symposium (USENIX Security'14)*. pp. 925–940.
- Beibei Li, Rongxing Lu, Wei Wang, Kim-Kwang Raymond Choo. 2016. DDOA: A Dirichlet-Based Detection Scheme for Opportunistic Attacks in Smart Grid Cyber-Physical System. *IEEE Trans. Inf. Foren. Secur.* 11, 11, 2415–2425.
- Milagro Project. 2016. <http://dev.docs.milagro.io.s3-website-us-east-1.amazonaws.com/en/milagro-a-case-for-something-new-part-1.html>, Accessed Oct. 12, 2016.
- Anne H. H. Ngu, Mario Gutierrez, Vangelis Metsis, Surya Nepal, and Quan Z. Sheng. 2016. IoT Middleware Survey: Issues and Enabling Technologies. *IEEE Internet of Things Journal*. online, DOI: 10.1109/JIOT.2016.2615180 <http://ieeexplore.ieee.org/document/7582463/>.
- Victor Prokhorenko, Kim-Kwang Raymond Choo, and Helen Ashman. 2016. Intent-Based Extensible Real-Time PHP Supervision Framework. *IEEE Trans. Inf. Foren. Secur.* 11, 10, 2215–2226.
- Deepak Puthal, Surya Nepal, Rajiv Ranjan, and Jinjun Chen. 2016a. Threats to Networking Cloud and Edge Datacenters in the Internet of Things. *IEEE Cloud Computing* 3, 3, 64–71.
- Deepak Puthal, Surya Nepal, Rajiv Ranjan, and Jinjun Chen. 2016b. DLSeF: A Dynamic Key Length Based Efficient Real-Time Security Verification Model for Big Data Streams. *ACM Trans. Embedd. Comput. Syst.*
- Ahmed Saeed, Ali Ahmadina, Abbas Javed, and Hadi Larijani. 2016. Random Neural Network based Intelligent Intrusion Detection and Prevention Mechanism for IoT Applications. *ACM Trans. Internet Tech.*
- Neetesh Saxena, Santiago Grijalva, and Narendra S. Chaudhari. 2016. Authentication Protocol for IoT-Enabled LTE Network. *ACM Trans. Internet Tech.*
- Seung-Hyun Seo, Jongho Won, and Elisa Bertino. 2016. pCLSC-TKEM: A Pairing-free Certificateless Signcryption-tag Key Encapsulation Mechanism for a Privacy-Preserving IoT. *Trans. Data Priv.* 9, 2, 101–130.
- Bilal Shebaro, Oyindamola Oluwatimi, and Elisa Bertino. 2015. Context-Based Access Control Systems for Mobile Devices. *IEEE Trans. Depend. Sec. Comput.* 12, 2, 150–163.
- Shachar Siboni, Asaf Shabtai, Yuval Elovici, Nils Ole Tippenhauer, and Jemin Lee. 2016. Advanced security testbed framework for wearable IoT devices. *ACM Trans. on Internet Tech.*
- Jongho Won, Seung-Yun Seo, and Elisa Bertino. 2015. A Secure Communication Protocol for Drones and Smart Objects. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIA CCS'15)*. (Singapore, April 14–17, 2015).
- Yanjiang Yang, Jiqiang Lu, Kim-Kwang Raymond Choo, and Joseph K. Liu. 2015a. On Lightweight Security Enforcement in Cyber-Physical Systems. In *Proceedings of 4th International Workshop on Lightweight Cryptography for Security and Privacy (LightSec 2015)* (Bochum, Germany). Volume 9542/2015 of Lecture Notes in Computer Science, Springer-Verlag, pp. 97–112.

- Yanjiang Yang, Joseph K. Liu, Kaitai Liang, Kim-Kwang Raymond Choo, and Jianying Zhou. 2015b. Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Cloud Data Encryption. In *Proceedings of 20th European Symposium on Research in Computer Security (ESORICS 2015)* (Vienna, Austria). Volume 9327/2015 of Lecture Notes in Computer Science. Springer-Verlag, pp. 146–166.
- Yuxin Zhang, Yang Xiang, and Xinyi Huang. 2016. Password Authenticated Group Key Exchange: A Cross-Layer Design. *ACM Trans. Internet Tech.*

Received October 2016; accepted October 2016