Editorial

Internet of Things security and forensics: Challenges and opportunities

Mauro Conti [a,*,1], Ali Dehghantanha [b,1], Katrin Franke [c,1], Steve Watson [d,1]

[a] *Department of Mathematics, University of Padua, Italy*
[b] *Department of Computer Science, University of Salford, UK*
[c] *Testimon Forensics Group, Norwegian University of Science and Technology, Norway*
[d] *VTO Labs, Denver, CO, USA*

ARTICLE INFO

ABSTRACT

The Internet of Things (IoT) envisions pervasive, connected, and smart nodes interacting autonomously while offering all sorts of services. Wide distribution, openness and relatively high processing power of IoT objects made them an ideal target for cyber attacks. Moreover, as many of IoT nodes are collecting and processing private information, they are becoming a goldmine of data for malicious actors. Therefore, security and specifically the ability to detect compromised nodes, together with collecting and preserving evidences of an attack or malicious activities emerge as a priority in successful deployment of IoT networks. In this paper, we first introduce existing major security and forensics challenges within IoT domain and then briefly discuss about papers published in this special issue targeting identified challenges.

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

The Internet of Things (IoT) integrates various sensors, objects and smart nodes that are capable of communicating with each other without human intervention [1] . The objects/things function autonomously in connection with other objects. IoT nodes are capable of delivering lightweight data, accessing and authorising cloud-based resources for collecting and extracting data and making decisions by analysing collected data. The emergence of IoT has led to pervasive connection of people, services, sensors and objects. IoT devices are now deployed in a wide range of applications from smart grids to healthcare and intelligence transport systems [2]. Huge business opportunities that exist within IoT domain significantly increased number of smart devices and intelligent, autonomous services offered in IoT networks. Moreover, reliance of IoT devices on cloud infrastructure for data transfer, storage and analysis led to development of cloud-enabled IoT networks [3].

Security issues such as privacy, access control, secure communication and secure storage of data are becoming significant challenges in IoT environment [4]. Moreover, every single device that we create, every new sensor that we deploy, and every single byte that is synchronised within an IoT environment may at some point come under scrutiny in the course of an investigation.

The fast growth of IoT devices and services led to deployment of many vulnerable and insecure nodes [5]. Moreover, conventional user-driven security architectures are of little use in object-driven IoT networks [6]. Therefore, we require specialised tools, techniques and procedures for securing IoT networks and collecting, preserving and analysing residual evidences of IoT environments. In this special issue we sought new and unpublished works in the domain of IoT security and forensics.

The remainder of this paper is organised as follows. In the next section, we briefly discuss about security challenges in IoT environment. In Section 3, we provide a brief discussion of forensics challenges within IoT networks. We offer a brief review of accepted articles in this special issue in Section 4, and finally conclude the paper.

2. Security challenges in IoT environments

Wide distribution of IoT nodes and private nature of data that are collected and transferred by IoT devices made security a major challenge. In this section, we are briefly looking at major security challenges that exist in IoT environments.

2.1. Authentication

In IoT domain, authentication allows integration of different IoT devices that are deployed in different contexts. Authentication process involves authentication of routing peers that involve in

---

transferring data as well as authentication of the source of data route (data origin node) [7]. Efficient key deployment and key management is a challenge in IoT devices authentication. Any cryptographic key generation and key exchange should not cause a major overhead on IoT nodes [8]. Moreover, in the absence of a guaranteed Certificate Authority (CA), other mechanisms are required for validating cryptographic keys and ensuring integrity of key transfer.

2.2. Authorisation and access control

Authorisation involves specification of access rights to different resources while Access Control mechanisms should guarantee access right of only authorised resources [9]. Each and every IoT node may only support limited mechanisms for access verification which could be different from other connected objects to the same node [10]. Therefore, deployment and management of a variety of authorisation and access control mechanisms which are tailored to different nodes capabilities is a challenge in a heterogeneous IoT network [11].

2.3. Privacy

Deployment of autonomous objects in IoT that sense people private information (such as health data) pose a new level of threat to individuals' privacy. Unlike conventional scenarios in which users have to take some actions (i.e. searching for a keyword or posting some data) to put their privacy at stake, IoT nodes are collecting people's private data without them even noticing [12]. Existing mechanisms are providing user centric privacy, content oriented privacy or context oriented privacy. However, IoT networks are naturally contains autonomous nodes that collect information and require object-oriented privacy models. Moreover, majority of privacy regulations mandate keeping users informed about how their private data is managed and administered. Identifying nodes that may have access to passively collected users' private information is a huge challenge in heterogeneous IoT networks [13].

2.4. Secure architecture

Building an architecture that overcomes aforementioned security challenges in IoT environments is not trivial. Any IoT architecture should not only address previously mentioned security issues but deal with challenges that are introduced by deploying IoT devices over Software Defined Networks (SDN) and cloud infrastructure [14]. Majority of SDN and cloud environment security issues would inevitability inherited to underlying IoT sensors. Moreover, Complexities that involve in securely connecting object-oriented IoT networks to data-oriented cloud infrastructures would introduce many unprecedented security challenges [15]. Finally, detection of malicious traffics rerouted over networks with different natures (i.e. SDN, Cloud and IoT) and hunting for malicious actors is a very challenging task for existing intrusion detection and prevention systems [16].

3. Forensics challenges in IoT environments

IoT would soon pervade all aspects of our life from managing our home temperature to thinking cars and smart management of the cities. So it will not take long to see people suing each other for misusing their smart things, thinking cars that have accident and attackers who compromised smart sensors. The Internet of everything is developing a haystack which contains lots of valuable forensics artefacts while identification, collection, preservation and reporting of evidences as well as attack or deficit attribution would be challenging in this environment. In this section we briefly introduce main forensics challenges in IoT environments.

3.1. Evidence identification, collection and preservation

Search and seizure is an important step in any forensics examination. However, detecting presence of IoT systems is quite a challenge considering these devices are designed to work passively and autonomously [17]! Even, in most cases when an IoT device is identified there is no documented method or a reliable tool to collect residual evidences from the device in a forensically sound manner [18]. Moreover, there are very limited methods to create forensic image of a given IoT device ignoring ethical considerations when collecting evidences from devices running in a multi-tenancy environment.

While preservation of collected data using traditional techniques such as hashing is not difficult, preservation of the scene is an enormous challenge in an IoT environment. Real-time and autonomous interactions between different nodes, would make it very difficult if not impossible to identify scope of a compromise and boundaries of a crime scene.

3.2. Evidence analysis and correlation

Majority of IoT nodes are not storing any metadata including temporal information which makes provenance of evidences a challenge for an investigator! In the absence of temporal information such as modified, accessed and created time, correlation of evidences gathered from different IoT devices is almost impossible. Beyond technical challenges, privacy is a major issue to consider when analysing and correlating collected data especially as majority of IoT sensors are collecting innate personal information [19]. Moreover, the sheer volume of data that are collected in heterogeneous IoT environments make it close to impossible to provide an end-to-end analysis of residual evidences.

3.3. Attack or deficit attribution

A common outcome of any forensics investigation is to identify criminal actors or liabilities of involved parties in the case of an incident. With fast rate of development in autonomous vehicles industry identifying liabilities of different parties (i.e. human driver or car autonomous driving system) in an accident would soon become a cyber forensics challenge! Answering such questions would be impossible in the absence of documented methods and forensically sound tools for collection, preservation and analysis of cyber–physical systems data [20]. Moreover, in the absence of a proper authentication system, identifying activities and liabilities of different parties having access to an IoT node would be challenging. Finally, attribution of malicious activities detected in an IoT environment even in the possession of evidences is quite challenging in the absence of a reliable and secure architecture that guarantees a forensically sound logging and monitoring system.

4. A brief review of accepted articles of this special issue

In this special issue we have accepted three papers in the domains of IoT privacy, IoT forensics and security in SDN-based IoT networks.

The first paper is Privacy-Preserving Protocols for Secure and Reliable Data Aggregation in IoT-Enabled Smart Metering Systems by Samet Tonyali, et al. [21]. This paper tackles privacy issues raised by frequent data collection of smart metering systems. Current systems achieve privacy by concealing aggregated in-network data using Fully Homomorphic Encryption (FHE) and secure MultiParty Computation (secure MPC). However, both FHE and secure MPC are producing overhead in IoT environments. Therefore, Samet Tonyali, et al. [21] suggested a new protocol which utilises FHE

and secure MPC in Smart Grid (SG) Advanced Metering Infrastructure (AMI) to reduce overheads while providing a viable privacy-preserving data aggregation mechanism.

The Digital Forensic Intelligence: Data Subsets and Open Source Intelligence (DFINT+OSINT): a Timely and Cohesive Mix paper by Darren Quick and Kim-Kwang Raymond Choo [22] addresses the issue of analysing big digital forensics data resulted from investigation of IoT objects. The paper presents a framework for entity identification and open source information cohesion within digital forensics domain. Authors analysis using real world data demonstrated benefits of their framework in real world investigations.

The last paper of this special issue, has suggested a mechanism to change attack surface in SDN-based IoT networks to increase attackers efforts for a successful exploitation. Internet of Things; Software-Defined Networking; Attack Graphs;Security Modeling by Mengmeng Ge, et al. [23] utilised SDN to reconfigure IoT network topology as a proactive defence mechanism. Their simulated results showed how their mechanisms increased attackers efforts while maintained the average shortest path length in a SDN-IoT network.

5. Conclusion

The fast pace of development and nature of IoT environments bring a variety of security and forensics challenges. In this paper, we briefly presented major security and forensics issues along with potentially promising solutions. Papers included in this special issue offer state of art view of privacy, security and forensics challenges in IoT environments along with innovative solutions that paves the way towards secure and forensically sound deployment of IoT networks.

Acknowledgements

References

[1] M. Ambrosin, A. Anzanpour, M. Conti, T. Dargahi, S.R. Moosavi, A.M. Rahmani, P. Liljeberg, On the feasibility of attribute-based encryption on Internet of Things devices, IEEE Micro 36 (6) (2016) 25–35. http://dx.doi.org/10.1109/MM.2016.101.

[2] B.-C. Chifor, I. Bica, V.-V. Patriciu, F. Pop, A security authorization scheme for smart home Internet of Things devices, Future Gener. Comput. Syst. (2017). http://dx.doi.org/10.1016/j.future.2017.05.048.

[3] V. Mai, I. Khalil, Design and implementation of a secure cloud-based billing model for smart meters as an Internet of Things using homomorphic cryptography, Future Gener. Comput. Syst. 72 (2017) 327–338. http://dx.doi.org/10.1016/j.future.2016.06.003.

[4] B.B. Zarpelão, R.S. Miani, C.T. Kawakani, S.C. de Alvarenga, A survey of intrusion detection in Internet of Things, J. Netw. Comput. Appl. 84 (2017) 25–37. http://dx.doi.org/10.1016/j.jnca.2017.02.009.

[5] A. Giaretta, S. Balasubramaniam, M. Conti, Security vulnerabilities and countermeasures for target localization in bio-nanothings communication networks, EEE Trans. Inf. Forensics Secur. 11 (4) (2016) 665–676. http://dx.doi.org/10.1109/TIFS.2015.2505632.

[6] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of Things security: A survey, J. Netw. Comput. Appl. 88 (2017) 10–28. http://dx.doi.org/10.1016/j.jnca.2017.04.002.

[7] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K.-K.R. Choo, et al., An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment, J. Netw. Comput. Appl. 89 (2017) 72–85. http://dx.doi.org/10.1016/j.jnca.2016.12.008.

[8] Y. Yang, H. Cai, Z. Wei, H. Lu, K.-K.R. Choo, Towards Lightweight Anonymous Entity Authentication for IoT Applications, Springer, Cham, 2016, pp. 265–280. http://dx.doi.org/10.1007/978-3-319-40253-6_16.

[9] E. Bertino, K.-K.R. Choo, D. Georgakopolous, S. Nepal, Internet of Things (IoT): smart and secure service delovery, ACM Trans. Internet Technol. 16 (4) (2016) 1–7. http://dx.doi.org/10.1145/3013520.

[10] S.R. Moosavi, T.N. Gia, E. Nigussie, A.M. Rahmani, S. Virtanen, H. Tenhunen, J. Isoaho, End-to-end security scheme for mobility enabled healthcare Internet of Things, Future Gener. Comput. Syst. 64 (2016) 108–124. http://dx.doi.org/10.1016/j.future.2016.02.020.

[11] F. Li, J. Hong, A.A. Omala, Efficient certificateless access control for industrial Internet of Things, Future Gener. Comput. Syst. (2017). http://dx.doi.org/10.1016/j.future.2016.12.036.

[12] J. Lopez, R. Rios, F. Bao, G. Wang, Evolving privacy: from sensors to the Internet of Things, Future Gener. Comput. Syst. 75 (2017) 46–57. http://dx.doi.org/10.1016/j.future.2017.04.045.

[13] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, K. Wehrle, A comprehensive approach to privacy in the cloud-based Internet of Things, Future Gener. Comput. Syst. 56 (2016) 701–718. http://dx.doi.org/10.1016/j.future.2015.09.016.

[14] S. Raza, T. Helgason, P. Papadimitratos, T. Voigt, SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things, Future Gener. Comput. Syst. (2017). http://dx.doi.org/10.1016/j.future.2017.06.008.

[15] C. Stergiou, K.E. Psannis, B.-G. Kim, B. Gupta, Secure integration of IoT and cloud computing, Future Gener. Comput. Syst. (2016). http://dx.doi.org/10.1016/j.future.2016.11.031.

[16] H. Haddad Pajouh, R. Javidan, R. Khayami, D. Ali, K.-K.R. Choo, A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks, IEEE Trans. Emerg. Top. Comput. (2016) 1. http://dx.doi.org/10.1109/TETC.2016.2633228.

[17] M. Harbawi, A. Varol, An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework, in: 2017 5th International Symposium on Digital Forensic and Security, ISDFS, IEEE, 2017, pp. 1–6. http://dx.doi.org/10.1109/ISDFS.2017.7916508.

[18] C.J. D'Orazio, K.-K.R. Choo, L.T. Yang, Data exfiltration from Internet of Things devices: IoS devices as case studies, IEEE Internet of Things J. 4 (2) (2017) 524–535. http://dx.doi.org/10.1109/JIOT.2016.2569094.

[19] A. Dehghantanha, K. Franke, Privacy-respecting digital investigation, in: Proceedings of 2014 Twelfth Annual International Conference on Privacy, Security and Trust, PST, 2014, pp. 129–138. http://dx.doi.org/10.1109/PST.2014.6890932.

[20] S. Watson, A. Dehghantanha, Digital forensics: the missing piece of the Internet of Things promise, Comput. Fraud & Secur. 2016 (6) (2016) 5–8. http://dx.doi.org/10.1016/S1361-3723(15)30045-2.

[21] Samet Tonyali, Kemal Akkaya, Nico Saputro, A. Selcuk Uluagac, Mehrdad Nojoumian, Privacy-preserving protocols for secure and reliable data aggregation in iot-enabled smart metering systems, Future Gener. Comput. Syst. 78 (2018) 547–557. http://dx.doi.org/10.1016/j.future.2017.04.031.

[22] Darren Quick, Kim-Kwang Raymond Choo, Digital forensic intelligence: Data subsets and open source intelligence (DFINT+OSINT): a timely and cohesive mix, Future Gener. Comput. Syst. 78 (2018) 558–567. http://dx.doi.org/10.1016/j.future.2016.12.032.

[23] Mengmeng Ge, Jin B. Hong, Simon Yusuf, Dong Seong Kim, Internet of Things; Software-defined networking; attack graphs; security modeling, Future Gener. Comput. Syst. (2017) in press.