SIOTOME: An Edge-ISP Collaborative Architecture for IoT Security

Hamed Haddadi*, Vassilis Christophides†, Renata Cruz Teixeira†, Kenjiro Cho‡, Shigeya Suzuki§, Adrian Perrig¶
*Imperial College London
†Inria Paris
‡IIJ Research Lab
§Keio University
¶ETH Zurich

***Abstract*—We are observing an increasing rate in the introduction of always-on Internet of Things (IoT) devices in our households and public environments. These devices range from voice-enabled personal assistants, entertainment systems, health monitoring devices, infrastructure monitoring equipment, the quantified self sector, to kitchen utensils and equipment. As each of these devices comes with its own data sensing and sharing ecosystem and data collection and reporting strategy, providing unified security solutions for the users will be of utmost importance.**

In this paper we propose a novel, cooperative system between the home gateway and the Internet Service Provider (ISP) to provide data driven security solutions for detecting and isolating IoT security attacks. Our approach is based on a combination of a large-scale view from the ISP (using powerful machine learning techniques on traffic traces), and the fine-grained view of the per-device activity from the home (using edge processing techniques) to provide efficient, yet privacy-aware IoT security services.

I. Introduction

Today we are observing an increasing rate in the introduction of connected, Internet of Things (IoT) [9] devices in our everyday life.[1] Homes and public buildings and spaces (e.g., campuses, pedestrian zones, airports) are increasingly instrumented with a variety of IoT devices that can interact with each other and/or be remotely monitored and controlled. These devices range from voice-enabled personal assistants, entertainment systems, health and well-being monitoring devices (i.e., quantified self), home automation (i.e., smart plugs and pet doors) and connected appliances, as well as monitoring equipment such as light, temperature, and humidity sensors, cameras, and motion detectors. As IoT devices are typically embedded inside the networks (i.e., continuously interacting using primary local and third party cloud-based services), they are attractive attack targets for breaking into a secure network infrastructure [6], [20], or for leaking sensitive information about users and their behaviors [2], [11], [10], [19].

The rapid development of the consumer IoT sector and the focus on time-to-market has been generally at the sacrifice of privacy and security. Many of the current devices remain vulnerable to attacks, do not receive regular updates without user intervention, or use insecure communication methods such as telnet[2] or HTTP-based communication. Often, device vendors and manufacturers may be unable or unwilling to release software updates that address vulnerabilities.[3] A study identified more than 500,000 insecure, publicly accessible embedded networked devices [18]. Vulnerable IoT devices make home networks open to attacks or privacy leaks and make the Internet subject to large-scale Distributed Denial of Service (DDoS) attacks such as the Dyn Attack by the Mirai botnet.[4][5] Providing security for the consumer IoT market will be a big challenge in the next decade.[6]

Traditional network security solutions combining *static perimeter network defenses* (e.g., firewalls and intrusion detection/prevention systems), with ubiquitous use of end-host based defenses (e.g., antivirus), and software patches from vendors (e.g., Patch Tuesday) [20] are challenged by the dynamic landscape of the IoT threats and the *technical skills* required by the end-users for maintaining secure IoT devices. An operation deep inside the network renders traditional perimeter defenses ineffective while the longevity of IoT devices implies that despite IT security best practices, several vulnerabilities (e.g., default passwords, unpatched bugs) will remain deployed long after vendors cease to produce or support them. Moreover, devices can be moved between private, communal, or public spaces. Given overlapping wireless connectivity within or across spaces, it became easier for a device on one network to inadvertently or maliciously breach the security and mismanage another device on another overlapping network [1]. The existing rule-based security measures cannot cope with unpredictability in ever-changing traffic behaviors, as IoT interactions are evolving with increasing complexity. Last but not least, end-users in the consumer IoT space often lack

[1] https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by-2020/

[2] https://arstechnica.com/information-technology/2017/08/leak-of-1700-valid-passwords-could-make-the-iot-mess-much-worse/

[3] http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/

[4] https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html

[5] https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

[6] http://www.gartner.com/smarterwithgartner/navigating-the-security-landscape-in-the-iot-era/

1st International Workshop on Security and Privacy for the Internet-of-Things (IoTSec)
17 April 2018
http://dx.doi.org/XYZ

access to a technically skilled network administrator [8]. As the number of devices increase (even within a household), the traditional firewall and port-based monitoring approaches will not be effective at mitigating the threats, while enabling the range of services and applications in the IoT ecosystem to operate flawlessly.

The complex inter-dependancies of the IoT ecosystem force the network to (re)emerge as the key vantage point for enforcing security policies [20]. Network-based security solutions are better suited to the scale of deployed IoT devices, the nature of Machine-to-Machine (M2M) communication, the sheer diversity of the device hardware, as well as interoperability constraints (e.g., devices of the same type but from different vendors cannot always communicate) [19]. We thus propose to move the responsibility of securing consumer IoT devices from users to a *collaborative system between the network edge and the Internet Service Provider* (ISP).

In this context, we propose a security system that learns and adapts to the changing environment, and reacts to unexpected events in a quick and autonomous manner, by means of collecting data, performing analytics, creating network access rules, and controlling traffic accordingly for defense. As dynamic IoT threat detection requires a close view on traffic from the users' devices, we should employ security analytics methods that guarantee privacy of raw users' data. Furthermore, we need to develop mechanisms that protect against a wide range of network-based attacks such as vulnerability scanning, intrusion attacks, network eavesdropping, data alteration, as well as Denial-of-Service (DoS) attacks. Given that network conditions and device behaviors can change rapidly, we need to continuously reassess and update the IoT security posture. Our overarching goal here is to create a protection system that enables secure operation of an IoT deployment despite potentially vulnerable or even compromised IoT devices.

In this paper we present SIOTOME, a cooperative architecture between the edge network and the ISP for early detection and mitigation of security vulnerabilities and threats due to IoT device misconfigurations and malicious attacks. In SIOTOME, instead of trying to secure an increasing number of heterogeneous devices, we focus on securing the network connecting them. With no communication, malicious devices cannot compromise other devices or launch attacks. We propose to design, develop, and evaluate a system that relies on the *cooperation among defense mechanisms deployed at multiple layers at the network edge*: the cloud, the ISP, and the home gateway. We advocate a *data-driven* approach to detect and isolate security threats based on a combination of large-scale view from the cloud (using machine learning techniques on traffic traces) and the fine-grained view of the per-device activity from within the home. To mitigate security breaches, SIOTOME relies on a set of defense mechanisms, for example, *network isolation* for limiting the attack surface, *key management* approaches to establish cryptographic keys between devices to provide communication secrecy and authenticity, and *allowed network input and output* to prevent vulnerability scanning and DDoS.

We assume that home users are independent and autonomous for protecting user's privacy. Thus, the ISP does not know the details of devices deployed in the home. An obvious case that requires cooperation between the edge and the ISP is when identifying an infected device in the home. When the ISP detects a suspicious communication originated from a certain home, the ISP can only tell the home gateway about the threat information and its signature for detection. Then, it is the home gateway that identifies the device using the provided signature, and notifies the user along with augmented device information such as model and installation date extracted from the home-internal device registry.

II. System Framework

Building up on existing network-based intrusion detection and security systems, which focus on defending a single domain/service with rule-based approaches, SIOTOME leverages data from a large number of domains to learn from the environment to identify attack signals so that it can react more quickly and effectively to emerging threats. A domain in SIOTOME can be an individual home network, a cloud provider, or an individual ISP network (the traditional definition of Autonomous System in Internet routing). As shown in Fig. 1, SIOTOME has two high-level types of domains: SIOTOME/edge and SIOTOME/cloud.

Inside the user's home, we find the following components:

- The home gateway provides network connectivity to the access ISP and enforces local connectivity under the control of the home controller.
- The edge data collector is responsible to observe network traffic to monitor the behavior of IoT devices. It can also run active probing tests to profile devices. This home collector can be hosted in the home gateway or in a separate device that is directly connected to the gateway.
- The edge analyzer takes information from the home data collector to profile the behavior of local IoT devices and identify threats and attacks. Upon the detection of a threat, it will notify the home controller. It also shares relevant information with SIOTOME/cloud after applying privacy-preserving data modifications.
- The edge controller is responsible for configuring the home gateway to steer local network traffic: among devices in the home as well as with the outside world. The edge controller contains an SDN controller for fine-gained control of network traffic from/to connected devices in the home, as well as additional management functions. Examples of management functions include simple mechanisms to create small groups of devices (similar to Virtual LANs but more convenient for IoT devices and easier to handle for users), and also all classical control and management functions in the home, e.g., DHCP, firewall, user management. It is responsible for applying specific countermeasures to protect users' security and privacy. The home controller functionality can also be offloaded to SIOTOME/cloud when needed as equipment in user's homes may have limited resources.

SIOTOME/cloud hosts the following components of the system:

- The Cloud collector is the software system that collects reports from home collectors as well as performs additional monitoring at the ISP level (when

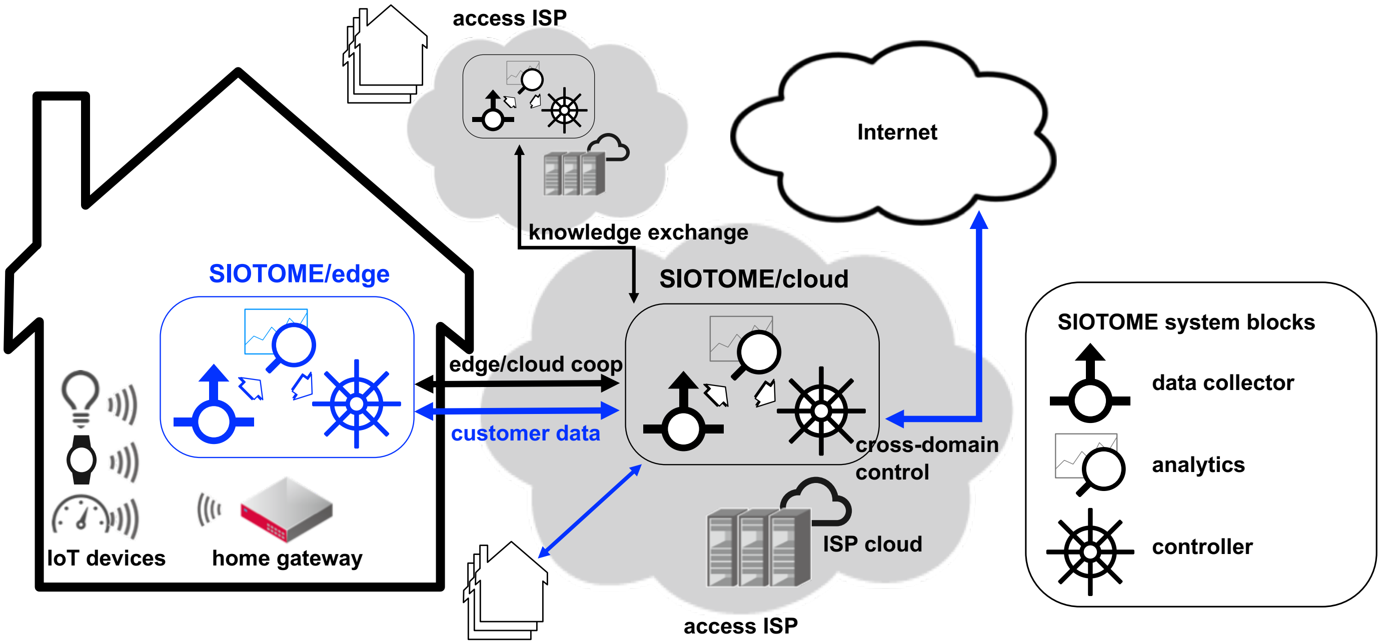

Fig. 1. SIOTOME Architecture and System Components

SIOTOME/cloud is running in the ISP), so it can observe malicious patterns that span several customers.

- The Cloud analyzer is similar to the edge analyzer in that it analyses network traffic to identify threats. The methods running in the cloud analyzer benefit from the large volume of data coming from multiple homes and ISP traffic. It is responsible for collecting the device profiles learned across homes into a central database as well as for populating this database with signatures of attacks it discovers or learns from edge analyzers.
- The Cloud controller is an SDN controller that can steer local network traffic at the ISP level and trigger countermeasures to the threats identified by the cloud analyzer.
- The cross-domain controller steers traffic between domains. It can make a destination reachable from only a subset of sources or ensure that outgoing traffic stays within a selected network region.
- The secure communication component maintains secure communication between various SIOTOME components.

SIOTOME allows for *delegating parts of such security functionality from the cloud to the edge*, enabled by a common framework called SIOTOME/cloud and SIOTOME/edge. It aims to balance local learning/defense and global learning/defense, and to quickly propagate detected threat information among users. The SIOTOME/edge in a user's home adapts to individual user environments, and provides front-end defense mechanisms close to IoT devices. It also *preserves user privacy* by processing sensitive data locally without exposing them to a third-party [5]. We rely on the home gateway architectures such as the Databox system [14], where privacy-preserving IoT and sensor data analytics can be performed using containerized libraries and isolated data sources, while minimizing the risk of sensitive inferences from third parties and the ISP [13], [12]. Collaborative and hybrid machine learning frameworks have recently been developed, leveraging edge processing to aid in preserving privacy, and increasing the resource efficiency of IoT systems [7], [16].

The SIOTOME/cloud in the access ISP has a more global view by collecting and analyzing data from a large number of customers, as well as exchanging knowledge information with SIOTOME/clouds in other ISPs. It also provides back-end defense mechanisms for isolating individual customers and for cross-domain communications. The SIOTOME/cloud and SIOTOME/edge can run the same set of security primitives, although the edge has only limited resources. A specific security service is composed by chaining security primitives; each security primitive can be dynamically created, deleted, or migrated between the SIOTOME/cloud and the SIOTOME/edge.

Finally, SIOTOME makes extensive use of *network slicing* for isolating IoT device communications; devices are grouped by attributes and observed behaviors, and then, assigned to a network slice with a specific security policy. SIOTOME will rely on intra- and cross-domain network environments that only permit approved network communications, which we call *permissioned network input and output*. Intra-domain mechanisms will rely on a technique called SDN-based home network steering that whitelists communication between groups of devices and devices and external entities (i.e., websites) in network-isolated slices, leveraging the Majord'Home platform [3], [4]. For cross-domain mechanisms, we plan to leverage the SCION secure Internet architecture [17], an inter-domain architecture that provides source-controlled path selection, multipath operation, and DoS defenses. For intra-domain, cross-domain and edge-to-cloud coordination, secure communucation mechanism is essential. SIOTOME plan to make use of blockchain as a secure broadcast channel based on [15].

III. Future Direction

In this paper we proposed SIOTOME, an architecture for a collaborative, privacy-preserving analytics architecture between the edge of the network and an ISP, to provide a first step security defense against distributed attacks by compromised IoT devices. As the first step towards realizing this vision, we are evaluating the interactive behavior of a number of IoT devices to advance our understanding of IoT security threats in the wild. Understanding these interactions and network utilization profiles allows us to train machine learning models and establish optimal operational configurations between the edge and the cloud.

SIOTOME is inspired by the vision to make IoT security analysis, threat detection, and defenses intuitive and effective for the non-expert users at the home environment. Our ambition is to build a service where data and inferences from the edge are combined with the insights gained from the cloud to provide a coherent system for early detection of security threats and take autonomous action, and consequently alert the user and the ISP. Most importantly, privacy-preserving inferences of the normal device behavior and network characteristics, and cooperative sharing of this knowledge in combination with the ISP traffic characterization, allows SIOTOME to monitor an IoT network, providing user security and privacy, despite potentially vulnerable or compromised devices.

Acknowledgment

The authors would like to thank Felipe Huici, Matthieu Boussard, Nicolas Le Sauze, Ludovic Noirie, Romain Fontugne, Kensuke Fukuda, Ping Du, and Aki Nakao for their extensive discussions on SIOTOME. We also appreciate constructive feedback from the anonymous reviewers at IoTSec 2018. Hamed Haddadi was supported by the EPSRC Databox grant (Ref: EP/N028260/1) and a Microsoft Azure for Research grant.

References

[1] W. Aman, "Assessing the feasibility of adaptive security models for the internet of things," in *Human Aspects of Information Security, Privacy, and Trust*, T. Tryfonas, Ed. Cham: Springer International Publishing, 2016, pp. 201–211.

[2] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic," *CoRR*, vol. abs/1708.05044, 2017. [Online]. Available: http://arxiv.org/abs/1708.05044

[3] S. Bera, S. Misra, and A. V. Vasilakos, "Software-defined networking for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1994–2008, Dec 2017.

[4] D. T. Bui, R. Douville, and M. Boussard, "Supporting multicast and broadcast traffic for groups of connected devices," in *2016 IEEE NetSoft Conference and Workshops (NetSoft)*, June 2016, pp. 48–52.

[5] A. Chaudhry, J. Crowcroft, H. Howard, A. Madhavapeddy, R. Mortier, H. Haddadi, and D. McAuley, "Personal data: Thinking inside the box," in *Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives*, ser. AA '15. Aarhus University Press, 2015, pp. 29–32. [Online]. Available: http://dx.doi.org/10.7146/aahcc.v1i1.21312

[6] E. Fernandes, A. Rahmati, K. Eykholt, and A. Prakash, "Internet of things security research: A rehash of old ideas or new intellectual challenges?" *IEEE Security Privacy*, vol. 15, no. 4, pp. 79–84, 2017.

[7] L. Georgopoulos and M. Hasler, "Distributed machine learning in networks by consensus," *Neurocomputing*, vol. 124, pp. 2 – 12, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0925231213003639

[8] R. E. Grinter, W. K. Edwards, M. Chetty, E. S. Poole, J.-Y. Sung, J. Yang, A. Crabtree, P. Tolmie, T. Rodden, C. Greenhalgh, and S. Benford, "The ins and outs of home networking: The case for useful and usable domestic networking," *ACM Trans. Comput.-Hum. Interact.*, vol. 16, no. 2, pp. 8:1–8:28, Jun. 2009. [Online]. Available: http://doi.acm.org/10.1145/1534903.1534905

[9] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[10] M. Krämer, D. Aspinall, and M. Wolters, "Poster: Weighing in ehealth security," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: ACM, 2016, pp. 1832–1834. [Online]. Available: http://doi.acm.org/10.1145/2976749.2989044

[11] D. Leibenger, F. Möllers, A. Petrlic, R. Petrlic, and C. Sorge, "Privacy challenges in the quantified self movement - an EU perspective," *PoPETs*, vol. 2016, no. 4, pp. 315–334, 2016. [Online]. Available: https://doi.org/10.1515/popets-2016-0042

[12] M. Malekzadeh, R. G. Clegg, A. Cavallaro, and H. Haddadi, "Protecting sensory data against sensitive inferences," *the 1st EuroSys Workshop on Privacy by Design in Distributed Systems*, 2018.

[13] M. Malekzadeh, R. G. Clegg, and H. Haddadi, "Replacement autoencoder: A privacy-preserving algorithm for sensory data analysis," *The 3rd ACM/IEEE International Conference on Internet-of-Things Design and Implementation*, 2018.

[14] R. Mortier, J. Zhao, J. Crowcroft, L. Wang, Q. Li, H. Haddadi, Y. Amar, A. Crabtree, J. Colley, T. Lodge, T. Brown, D. McAuley, and C. Greenhalgh, "Personal data management with the databox: What's inside the box?" in *Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking*, ser. CAN '16. New York, NY, USA: ACM, 2016, pp. 49–54. [Online]. Available: http://doi.acm.org/10.1145/3010079.3010082

[15] J. Murai and S. Suzuki, "Blockchain as an audit-able communication channel," in *Computer Software and Applications Conference (COMPSAC), 2017 IEEE 41st Annual*, July 2017, pp. 516–522.

[16] S. A. Osia, A. S. Shamsabadi, A. Taheri, H. R. Rabiee, N. Lane, and H. Haddadi, "A hybrid deep learning architecture for privacy-preserving mobile analytics," *arXiv preprint arXiv:1703.02952*, 2017.

[17] A. Perrig, P. Szalachowski, R. M. Reischuk, and L. Chuat, *The SCION Architecture*. Cham: Springer International Publishing, 2017, pp. 17–42. [Online]. Available: https://doi.org/10.1007/978-3-319-67080-5_2

[18] A. Sivanathan, D. Sherratt, H. H. Gharakheili, V. Sivaraman, and A. Vishwanath, "Low-cost flow-based security solutions for smart-home iot devices," in *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Nov 2016, pp. 1–6.

[19] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home iot devices," in *WiMob*. IEEE Computer Society, 2015, pp. 163–167.

[20] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*, ser. HotNets-XIV. New York, NY, USA: ACM, 2015, pp. 5:1–5:7. [Online]. Available: http://doi.acm.org/10.1145/2834050.2834095