Internship proposal 2017-18

Topic: Device fingerprinting in the Internet of Things

Duration: 4 to 6 months

Hosting team: MiMove, Inria Paris (https://mimove.inria.fr/)
Joint team between Inria and Princeton University, HomeNet (https://team.inria.fr/homenet/)

Apply at: https://goo.gl/forms/CUYdaBmCA4iYaYpL2

Mentors: Vassilis Christophides, Senior Researcher, Inria (https://who.rocq.inria.fr/Vassilis.Christophides/)
Nick Feamster, Full Professor, Princeton University (https://www.cs.princeton.edu/~feamster/)
Renata Teixeira, Directeur de Recherche, Inria (https://who.rocq.inria.fr/Renata.Teixeira/)

Keywords: IoT network traffic characterization, IoT device signature extraction, network security, machine learning

Description:

The Internet of Things (IoT), comprising everyday objects such as lights, cameras, motion, sensors, power switches and appliances, is heralded to bring the next wave of Internet growth.[1] Homes, enterprises, campuses, and cities are expected to be instrumented with thousands of "smart" IoT devices that can autonomy interact with each other and be remotely monitored/controlled. The increasing prevalence of physical spaces equipped with Internet-connected devices, creates serious security concerns at unprecedented levels [1]. Today's IT security ecosystem is first challenged by the large heterogeneity in IoT devices (each with its own hardware, firmware and software) making the security vulnerabilities diverse and the attack vectors manifold. Furthermore, device manufacturers are rather lax in embedding security best practices (e.g., regular software/firmware patches) in consumer devices, dissuaded by low margins, time-to-market pressures, and limited resources. Unlike traditional IT ecosystems where host-based detection and prevention are prevalent, we believe that the realities of the IoT marketplace make the network to (re)emerge as the key vantage point for enforcing security policies [2]. 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 (e.g., motion sensory triggering lighting, temperature sensor opening a window), as well as, interoperability constraints (e.g., devices of the same type but from different vendors cannot always communicate) [3].

The goal of this internship is to develop effective and efficient analytical methods in order to characterize network traffic profiles generated by IoT devices and classify the IoT devices based on these profiles. More precisely, we are interested in analysing the traffic of passively observed home or campus networks in order to discover the type of connected IoT devices and associate them with known IoT vulnerabilities from public databases (e.g., SHODAN[2], OWASP[3] or other[4]). In this respect, we are interested in analyzing network traffic generated by IP-enabled devices (e.g., IP packet headers, TCP packet headers, send/receive rates, DNS). We will leverage datasets collected at a smart home in Princeton University. Our analysis aims to extract device profiles in terms of distinct activity patterns (traffic rate, bustiness, idle periods) [3] and sequences of DNS lookups to service IPs specific to a device or its manufacturer [4]. Our research will involve both (1) identifying the tradeoffs between the *cost* of different feature extraction methods (traffic metadata vs DNS-based signatures) and the *precision* of the device type classification techniques and (2) exploiting state-of-the-art classification techniques that can accurately identify the unique software and hardware characteristics of devices.

Bibliography

[1] E. Fernandes, A. Rahmati, K. Eykholt, A. Prakash: Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges? CoRR abs/1705.08522 (2017)

[1] https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by-2020/#c8d2f6e609bd
[2] https://www.shodan.io/
[3] https://www.owasp.org/index.php/OWASP_Internet_of_Things
[4] https://web.nvd.nist.gov/view/vuln/search

[2] 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 (HotNets-XIV) 2015. New York, NY, USA, Article 5, 7 pages.

[3] A. Sivanathan, D. Sherratt, H. Gharakheili, V. Sivaraman, A. Vishwanath: Low-Cost Flow-Based Security Solutions for Smart-Home IoT Devices IEEE ANTS, Bangalore, India, Nov 2016.

[4] Noah Apthorpe, Dillon Reisman, Nick Feamster A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. In Workshop on Data and Algorithmic Transparency (DAT'16) Nov 2016, New York University Law School, co-located with the Data Transparency Lab Conference and the FATML'16 Workshop