Thesis subject: Privacy-preserving communications for the IoT

Privatics Team – INSA-Lyon CITI – Inria

2021

1 Scientific Context

The emerging Internet of Things (IoT) is expected to host billions of devices that regularly communicate by using long- or short-range radio channels. Meta-data generated by those communications can be easily collected by third parties and leveraged to infer personal information. Identifiers included in headers and collateral traffic (e.g. DNS) expose users to privacy issues such as tracking and inference of activity and context. New mechanisms tailored for low-end devices are thus required to protect users against leakage of personal data.

IoT metadata and Privacy Beyond the content of messages exchanged by IoT devices, the privacy of users can be compromised by the metada data of the corresponding communications. Identifiers exposed in network traffic are source of privacy issue. Identifiers of the device itself as well as the identifiers of remote hosts can be leveraged to fingerprint the device and potentially infer personal data [4, 6, 2, 3]. For instance identifying a medical appliance in a household could reveal a medical condition of on of the inhabitant, which is considered as a sensitive by the European regulation GDPR.

Random identifiers are pseudonyms that are periodically rotated to prevent an external observer from uniquely identifying a device and following its activities over an extended period. Random identifiers were recently adopted at the link layer of wireless networks to protect users of mobile devices from being tracked. In particular, 802.11 MAC address randomization has been adopted by vendors [8] and has recently been included in the IEEE 802.11 aq amendment [1]. Similar measures have been included in Bluetooth [7, Vol 3, (C), sec. 10.7] by adding three new classes of device addresses.

Resolvable random identifiers have been introduced to allow identification by legitimate parties while preventing tracking from others. Those identifiers are generated using a secret key that can be used to ”resolve” the random pseudonym to a stable identity. Resolvable identifiers are part of the Bluetooth standard which include ”Resolvable Private Address” [7, Vol 3, (C), sec. 10.7].

IoT naming and Privacy The most common naming system in the global Internet is the Domain Name System (DNS). It is a distributed database that allows to resolve resource records assigned to names, and resource records may reflect any service on the top of the Internet. In addition to name resolution, the DNS provides an ecosystem to maintain the namespace on global scale. The feasibility of naming arbitrary content objects based on DNS is still an ongoing research topic [5]. Privacy protection against on-path eavesdropper such as DNS over HTTPS or DNS over TLS do not fit in the low-end IoT because stateful transport requires too many resources.

2 Thesis objectives

The overall objective of this thesis lies in assuring privacy of data and of identifiers that may disclose the data sources and contexts in the Internet of Things (IoT). The secure protection of data and metadata will in particular extend to low-end devices and low-power radio networks of the ultra-constrained IoT (possible integration in the RIOT open source platform).

- Privacy Extensions in name management systems (e.g. DNS): Analysis and design of extensions to hide names or any identifier that may conflict with privacy requirements.
- Resolvable Private Addresses: Analysis of resolvable IDs available in current technologies (e.g., Bluetooth) and design of possible adaptation to other technologies.
- Metadata and Privacy Violations: Identification and analysis of common IoT traffic patterns to model privacy violations based on metadata.

3 Research team: Privatics

The PRIVATICS team[1] is a research group affiliated to Inria and INSA-Lyon based in Grenoble and Lyon. PRIVATICS follows a multidisciplinary approach in considering the scientific and technical issues, but also economic, legal and social aspects of privacy. The team has expertise in the identification of privacy issues (Inria project Mobilitics with the French Data Protection Agency - CNIL), anonymization techniques and sanitization database (activity "Security and privacy for location- based services" EIT-ICT Labs and project "Investissement d'Avenir " XData) and design of Privacy Enhancing Technologies (PETs). PRIVATICS has a long history of contributing to Standards Developing Organisations, IETF and IEEE in particular, in order to contribute designing more privacy friendly systems, in the real world. The present subject could nicely contribute to such standardization activities.

This thesis is supported by the PIVOT (Privacy-Integrated design and Validation in the constrained IoT) project funded by the ANR-BMBF.

Location: Lyon / Villeurbanne, la Doua, INSA-Lyon, Laboratoire CITI.

4 Contact

- Mathieu Cunche: mathieu.cunche@insa-lyon.fr
- Vincent Roca: vincent.roca@inria.fr

5 Desired skills & application

Minimum qualifications: master or engineering degree in computer sciences and/or networking.
Knowledge topics: networking, wireless networking, privacy-protection, cryptography, embedded systems
Programming and working environment: GNU/Linux, C/C++, Python ...
Application documents: Detailed CV (training, projects, tools, skills, etc), cover letter (future projects, and motivations), scores of the last two years, reference contacts, recommendations letters are appreciated.

References

[1] 802.11aq-2018 - IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Preassociation Discovery. Technical report, IEEE standard association, August 2018.

[2] Guillaume Celosia and Mathieu Cunche. Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism. In *MobiQuitous 2019 - 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pages 1–10, Houston, United States, December 2019. Core A, 28.67%.

[1] https://team.inria.fr/privatics/

[3] Guillaume Celosia and Mathieu Cunche. Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols. *Proceedings on Privacy Enhancing Technologies*, 2020(1):26–46, January 2020.

[4] Kassem Fawaz, Kyu-Han Kim, and Kang G. Shin. Protecting Privacy of BLE Device Users. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 1205–1221, Austin, TX, 2016. USENIX Association.

[5] Dirk Kutscher, Suyong Eum, Kostas Pentikousis, Ioannis Psaras, Daniel Corujo, Damien Saucez, Thomas C. Schmidt, and Matthias Wählisch. Information-Centric Networking (ICN) Research Challenges. RFC 7927, RFC Editor, IRTF, July 2016.

[6] Sandra Siby, Rajib Ranjan Maiti, and Nils Tippenhauer. IoTScanner: Detecting and Classifying Privacy Threats in IoT Neighborhoods. *arXiv:1701.05007 [cs]*, January 2017. arXiv: 1701.05007.

[7] Bluetooth SIG. *Bluetooth Core Specification v5.1.* 2019. Accessed: 2019-08-30.

[8] Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo S. Cardoso, and Frank Piessens. Why MAC Address Randomization is Not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '16, pages 413–424, New York, NY, USA, 2016. ACM.