# SIMPL: Secure IoT Management Platform

Thomas Prantl*, Ala Eddine Ben Yahya*, Alexandra Dmitrienko*, Samuel Kounev*, Fabian Lipp†, David Hock†
Christoph Rathfelder ‡, Martin Hofherr §
* {firstname.lastname}@uni-wuerzburg.de, University of Würzburg, Germany
† {lastname}@infosim.net, Infosim GmbH & Co. KG, Germany
‡ {firstname.lastname}@hahn-schickard.de, Hahn-Schickard-Gesellschaft fur angewandte Forschung e.V., Germany
§ {firstname.lastname}@mixed-mode.de, Mixed Mode GmbH, Germany

***Abstract*—The proliferation of IoT devices is increasing at a fast pace, whether for private or business use. However, despite their growing popularity, their safe operation is often not guaranteed. To tackle the security challenges of modern IoT environments, the German Federal Ministry of Education and Research is funding the SIMPL project in order to support research in this area. The contribution of this paper is to introduce the main goal, objectives, and key features of SIMPL.**

***Index Terms*—KMU-inovative Project, SIMPL, IoT, Security**

## I. Introduction

With one of the largest digital transformations taking place this year, we are seeing the release of 5G which will provide the basic infrastructure and technology for a smart future [1]. The backbone of this intelligent future will consist of countless Internet of Things (IoT) devices—many already in use today—that will connect physical objects to networks using 5G technology and enable their communication and autonomous operation thus creating a pervasive environment for users. These technological changes, however, will result in an increase of the amount of digital information stored, processed and exchanged daily to entirely new levels. At the same time, security and trust become even more important for IoT systems as these have the potential of penetrating deeply into our day-to-day activities, like self-driving cars that can smartly reduce traffic jams, but at the same time open the possibility of mass disruption by attacking whole fleets at once.

**IoT Security and Privacy Challenges.** IoT technology poses new challenges to security and privacy, which cannot be sufficiently addressed by well-established state-of-the-art security methods. In particular, the typical approach to secure IT systems nowadays is to rely on centralized security and management components. However, IoT technology has to deal with a potentially unbounded number of interacting devices and substantial differences in communication patterns, which causes scalability and introperability problems in centralized systems. For instance, device authentication and access control mechanisms in traditional systems often rely on trusted third parties (TTPs) for distribution of keys and access control management, which limits interoperability across devices (e.g., if devices are certified by different authorities), affects scalability due to bottlenecks when communicating with centralized servers, and may impair user privacy (e.g., if TTPs collect user-specific data).

**IoT Security Disaster of Today.** Weak to absent security in IoT devices made IoT systems attractive attack targets – for instance, it was shown that it only takes five minutes on average until an IoT device is attacked after being connected [2]. At the same time, once compromised, IoT devices can be used as entry points to spread over the entire targeted system or to coordinate sophisticated attacks, such as Distributed Denial of Service (DDoS) as shown by the Mirai botnet [3].

In the light of discovered security vulnerabilities and reported incidents, IoT security has already earned the reputation of a security disaster [4]. Hence, it seems paramount to success of IoT technology to develop new generation security mechanisms which consider scalability, interoperability, tamper resilience, and user privacy as primary design goals.

**SIMPL Project.** As a step towards addressing these challenges, the German Federal Ministry of Education and Research is funding the KMU-innovativ project for small and medium-sized enterprises entitled *Secure IoT Management Platform* (SIMPL). SIMPL is driven by the University of Würzburg, Infosim, Hahn-Schickard and Mixed Mode. In the following, we introduce the main goal, objectives and key features of SIMPL.

## II. SIMPL Project

The main goal of the project is to develop a security management solution for IoT platforms. In particular, the platform is intended to enhance security of IoT systems and enable their advanced management while preserving compatibility to well-established and widely used communication protocols and middleware. For instance, SIMPL shall provide such functionality as security management and secure communication, and be realized in a form of communication adapter that can be plugged in between the communication channel and IoT application, thus being compatible to underlying IoT protocols and almost transparent to applications.

Such a platform can take care of autonomous security bootstrapping on IoT devices, thus taking the burden of security configuration and management from the end user, while avoiding the need for re-using master keys. In operational phase, the platform is responsible for autonomous and transparent key management while providing end-to-end secure communication to IoT applications. It further includes enhanced security features such as security monitoring and resilience management which enable the system to detect compromised devices and to either restore them to secure state or exclude from the network.

**Three Pillars of SIMPL.** To achieve the main goal of the project outlined above, SIMPL relies on three pillars. The first pillar is the idea to leverage properties of blockchains and advantages they provide for autonomous distributed systems. Hence, within SIMPL, we aim to design novel blockchain-based security mechanisms for IoT, which are higly scalable and interoperable with heterogeneous devices in highly dynamic environments, in contrast to state-of-the-art solutions which are limited in terms of scalability, interoperability and capture resilience [5].

The second pillar is compatibility with transport communication protocols commonly used in today's IoT systems, such as MQTT. To achieve such a compatibility, SIMPL follows a modular design approach which contains the necessary components for connecting appropriate plug-ins for various capabilities and provides a unified user interface accommodating various interaction modalities for monitoring and management of individual components.

The third pillar is the objective to achieve good efficiency and suitability for battery-powered and resource-constrained devices – platforms that are typical in IoT systems. To fulfill this objective, we aim to adapt the most recent research results in the field of efficient crypto primitives which are carefully evaluated within the project through theoretical analysis and using intensive performance testing.

**Planned Project Results** The final project results will include the design and implementation of the SIMPL architecture, along with a security and efficiency evaluation of the developed prototype. The developed concepts will be instantiated and their feasibility will be evaluated in two use cases: The first one is targeting an eHealth scenario and the second one intended for capacity sharing in smart factories.

## III. End-to-End Security in SIMPL

In the following, we would like to shed light on challenges of end-to-end secure communication in IoT systems and show how SIMPL will tackle them.

MQTT has become the de facto standard for IoT communication protocols [3] and thus Publish/Subscribe (Pub/Sub) architectures. In Pub/Sub protocols, the communication between IoT devices is mediated by intermediate components, called brokers. In particular, IoT devices are expected to send data they collect to a broker with the request to publish it at a given channel (called topic). The broker then distributes the received data to interested clients who subscribed to a given topic. This implies, that even if the system employs secure communication connections such as SSL/TLS, the communication is protected only between IoT devices and brokers, but there is no end-to-end secure communication between IoT devices and clients interested in data. Consequently, compromised or malicious brokers can freely drop, delay, replay, modify, or spoof IoT data.

The challenge in providing end-to-end security for IoT communication in Pub/Sub systems lies in the fact that the communication channels have multicast nature since the data sent by one sender needs to be received by multiple receivers. Additionally, IoT devices publishing data do not typically know which devices will eventually receive it. Furthermore, the clients may dynamically subscribe/unsubscribe to the topic which results in a highly dynamic set of receivers. Finally, the scheme must be efficient in terms of key sizes, energy demand, and encryption/decryption times, since IoT devices usually have little storage space, computing power, and energy supply.

While it might be feasible to apply an existing group or broadcast encryption scheme in order to achieve protected multicast communication, the additional challenges mentioned above make it non trivial to apply them in IoT context. While many of them exist (e.g., [6], [7]), none seem to be ideal for the targeted application area of IoT systems, but rather provide different trade-offs in terms of efficiency, communication overhead and ability to support dynamic groups. Hence, the goal of SIMPL project is to evaluate and improve existing solutions and ensure their applicability to the targeted use cases through theoretical analysis and performance benchmarking.

## IV. Conclusion

To summarize, SIMPL Project aims to tackle challenging security and privacy problems in IoT systems. It aims to develop an architecture and the prototype for the secure IoT management platform, and it based on three main pillars: novel blockchain-based security mechanisms, compatibility to standard IoT protocols and the objective to achieve efficiency suitable for embedded platforms. The platform will provide end-to-end secure communication to IoT applications, effortless management and wide range of advanced security features such as monitoring, intrusion detection and resilience management.

## References

[1] Daniel Newman. *Top 10 Digital Transformation Trends For 2020*. https://www.forbes.com/sites/danielnewman/2019/07/14/top-10-digital-transformation-trends-for-2020/ (accessed 03.01.2020).

[2] Netscout. NETSCOUT Threat Intelligence Report. Dawn of the Terrorbit Era. Findings from Second Half 2018. Technical report, 2018.

[3] Giovanni Perrone et al. The Day After Mirai: A Survey on MQTT Security Solutions After the Largest Cyber-attack Carried Out through an Army of IoT Devices. In *Proceedings of IoTBDS*, 2017.

[4] Lindsey O'Donnell. Top 10 iot disasters of 2019, 2019. https://threatpost.com/top-10-iot-disasters-of-2019/151235/ (accessed 03.01.2020).

[5] Bitkom. IT-Sicherheit, Cloud Computing und Internet of Things sind Top-Themen des Jahres in der Digitalwirtschaft, 2017. https://www.bitkom.org/Presse/Presseinformation/IT-Sicherheit-Cloud-Computing-und-Internet-of-Things-sind-Top-Themen-des-Jahres-in-der-Digitalwirtschaft.html (accessed 03.01.2020).

[6] Norranut Saguansakdiyotin et al. Broadcast Encryption Based on Braid Groups. *ACDT*, 2015.

[7] Jan Camenisch et al. Verifiable Encryption, Group Encryption, and Their Applications to Separable Group Signatures and Signature Sharing Schemes. In *ASIACRYPT*, 2000.