ERCIM "ALAIN BENSOUSSAN"
FELLOWSHIP PROGRAMME

ERCIM
European Research Consortium
for Informatics and Mathematics

Scientific Report

First name / Family name	Simon Bouget
Nationality	French
Name of the *Host Organisation*	RISE Research Institute of Sweden AB
First Name / family name of the *Scientific Coordinator*	Shahid Raza
Period of the fellowship	01/08/2019 to 31/07/2020

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

The scientific activity during the fellowship was organized around two main axis:

- leverage formal verifications techniques for better applied security
- enable lifelong, end-to-end, secure communications for resource-constrained devices, such as Internet-of-Things (IoT) devices

The first axis was executed in collaboration with other security researchers in RISE and KTH (Stockholm Royal Institute of Technology), and we used the Tamarin Prover to provide formal guarantees about the security of several communication protocols, in various domains such as distance-bounding credentials or lightweight certificate revocation. More details in the publication list below.

The second axis was realized in collaboration with RISE industrial partners in the security infrastructure and automotive sectors and complements RISE works in European projects. A continuation of RISE efforts to create and promote new secure and lightweight standard protocols for constrained devices in the IETF (Internet Engineering Task Force), we designed a standard-based network architecture and bootstrap procedure that enables IoT

devices to establish a secure channel with a distant back-end server. This is especially useful in large heterogeneous vehicular networks where a device does not necessarily trust the infrastructure. This work will be submitted for scientific publication soon.

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

Paper 1: Security and Trust Preserving Inter- and Intra-Cloud VM Migrations
Authors: Mudassar Aslam, Simon Bouget, Shahid Raza
Abstract: *"This paper focus on providing a secure and trustworthy solution for virtual machine (VM) migration within an existing cloud provider domain, and/or to the other federating cloud providers. The Infrastructure-as-a-Service (IaaS) cloud service model is mainly addressed to extend and complement the previous Trusted Computing techniques for secure VM launch and VM migration case. The VM migration solution proposed in this paper uses a Trust_Token based to guarantee that the user VMs can only be migrated and hosted on a trustworthy and/or compliant cloud platforms. The possibility to also check the compliance of the cloud platforms with the predefined baseline configurations makes our solution compatible with an existing widely accepted standards-based, security focused cloud frameworks like FedRAMP. Our proposed solution can be used for both, inter- and intra-cloud VM migrations. Different from previous schemes, our solution is not dependent on an active (on-line) trusted third party, that is, the trusted third party only performs the platform certification and is not involved in the actual VM migration process. We use the Tamarin solver to realize a formal security analysis of the proposed migration protocol and show that our protocol is safe under Dolev-Yao intruder model. Finally, we show how our proposed mechanisms fulfil major security and trust requirements for secure VM migration in cloud environments."*
Publisher: International Journal of Network Management (Elsevier)
Current status: Accepted

Paper 2: Distance-bounding, privacy-preserving attribute-based credentials
Authors: Daniel Bosk, Sonja Buchegger and Simon Bouget
Abstract: *"Distance-bounding anonymous credentials could be used for any location proofs that do not need to identify the prover and thus could make even notoriously invasive mechanisms such as location-based services privacy-preserving. There is, however, no secure distance-bounding protocol for generalattribute-basedanonymous credentials. Brands and Chaum's (EUROCRYPT'93) protocol combining distance-bounding and Schnorr comes close, but does not fulfill the requirements of modern distance-bounding protocols. For that, we need a secure distance-bounding zero-knowledge proof-of-knowledge resisting mafia fraud, distance fraud, distance hijacking and terrorist fraud.*
Our approach is another attempt toward combining distance bounding and Schnorr to construct a distance-bounding zero-knowledge proof-of-knowledge. We construct such a protocol and prove it secure in the (extended) Dürholz-Fischlin-Kasper-Onete model (DFKO model) for distance bounding. We also performed a symbolic verification of security properties needed for resisting these attacks, implemented in Tamarin. Encouraged by results from Singh et al. (NDSS'19), we take advantageof lessened constraints on how much can be sent in the fast phase of the distance-bounding protocol and achieve a more efficient protocol. We also provide a version that does not rely on being able to send more than one bit at a time which yields the same properties except for (full) terrorist fraud resistance."
Current status: Submitted to the 19th International Conference on Cryptology And Network Security (CANS 2020), pending

Paper 3: Lightweight Certificate Revocation with End-to-end Security for Low-power IoT Devices

Authors: Samuel Lindemer, **Simon Bouget**, Shahid Raza

Abstract: *"Pre-shared key (PSK) security, though practical in small sensor networks, does not scale well for IoT deployments comprising of thousands of devices. There is no notion of end-to-end security where many devices share a key, and there is no practical recourse in the event a PSK is compromised. For these reasons, virtually all Internet-connected devices will use certificate-based security in the near future. Standardization efforts are already under way to facilitate certificate enrollment with a public key infrastructure (PKI) on constrained devices. However, a complementary certificate revocation system has not yet been proposed. In this paper, we present a lightweight, formally verified protocol for this purpose.*

We begin this work by verifying the security claims of OCSP, the current standard for certificate validation on the Web, using the Tamarin Prover. Then, we restructure the symbolic model and remove rarely-used fields which cater to uncommon use cases. This forms the basis of our novel solution, TinyOCSP. We verify this new protocol against the security claims of OCSP, and design an encoding for it in CBOR. In our experiments on constrained hardware, validating eight certificates simultaneously with TinyOCSP required 41% less energy than validating a single certificate with OCSP over an IEEE 802.15.4 network. The RAM use was roughly halved.

For the sake of completeness, we also investigate whether combining TinyOCSP with compressed certificate revocation lists (CCRL) could further increase performance. Our findings indicate that although this approach can outperform TinyOCSP in some use cases, TinyOCSP is more efficient in the general case."

Current status: Submitted to the IEEE Internet of Things Journal, pending

Paper 4: Lightweight End-to-End Security for Constrained Devices in Vehicular Networks

Authors: **Simon Bouget** and Shahid Raza

Abstract: *"Internet of Things (IoT) is becoming a vital part of future connected critical infrastructure. Transportation systems, one of the critical infrastructures, are also getting smarter with increased cooperation between vehicles and infrastructures (V2X) and with the introduction of intelligence. A number of communication and security protocols are being standardized for this Cooperative Intelligent Transport Systems (C-ITS). However, in current C-ITS standards, security of individual devices, both tightly integrated devices (ECUs, cameras, etc.) and smart external sensors (e.g. a temperature sensor in an attached container) terminates at the edge/gateway of a vehicle. Most existing vehicles are system of systems where individual system providers leak sensitive data across vendors.*

In this paper, we proposed an end-to-end security architecture between C-ITS devices and back-end server where sensitive data from different individual devices can be shared with the communication back-ends without trusting third-parties. The proposed solution is standard-based integrated system that exploits recent IoT security standards and ensures interoperability between C-ITS protocols and conventional Internet protocols, without leaking sensitive data to proxy gateways and routers. We perform a formal analysis of our architecture using the Tamarin Prover and show that it guarantees the secrecy and authenticity of the communications under adversarial settings."

Current status: Will be submitted to the ACM 4th Computer Science in Cars Symposium (CSCS 2020) on September 11th

III – ATTENDED SEMINARS, WORKSHOPS, CONFERENCES

Seminar: RISE-SICS and Ericsson Security Day – October 2nd 2019, Stockholm, Sweden
Workshop: Workshop on Product Security for Cross Domain Reliable Dependable Automated Systems – October 9-10 2019, Graz, Austria
Seminar: 19th Seminar within the Framework of a Swedish IT Security Network (SWITS) – on June 3-4 2019, Karlstad, Sweden

IV – RESEARCH EXCHANGE PROGRAMME (REP)

As discussed with the ERCIM office in our mail exchange from May 15th 2020, it has been difficult to organize an exchange visit during the COVID pandemic with travel bans in place over most of Europe. Instead, we started remote collaborations with researchers from NTNU Systems Security Group, Norway (https://www.ntnu.edu/iik/s2g). We also scheduled a series of video conference meetings and lectures in September, where I will present the topics I worked on at RISE to the NTNU Group. Our NTNU contact is Prof. Stewart James Kowalski (stewart.kowalski@ntnu.edu), who is currently on a sabbatical visit at RISE. I will send a follow-up report after those meetings.