Ph.D. Offer : Design and Verification of Security Protocols for Heteregeneous 5G IoT Devices

January 19, 2019

Supervision: Pascal Lafourcade (LIMOS, UMR Université Clermont Auvergne) and Cristina Onete (XLIM, UMR 7252, Université de Limoges).

Location: LIMOS, Clermont Ferrand, France.

Research team: Olivier Blazy, Gérard Chalhoub, Pascal Lafourcade and Cristina Onete.

Starting date: October 2019.

Duration: 3 years (36 months).

Salary: 1500 € funded by the ANR project MOBIS5.

Contact: `pascal.lafourcade@uca.fr`, `cristina.onete@gmail.com`

Key words: Authenticated Key Exchange (AKE), Secure Delegation, Internet of Thing (IoT), 5G, Formal Verfication, Heteregenous Networks.

Context

For 30 years, 3rd and 4th generation mobile networks have allowed users to receive service anywhere, at any time. The dawning and visionary 5th generation mobile network (5G) aims to create a highly-decentralised architecture, including a massive Internet of Things (mIoT) and a non-federated core network, making telecommunications ubiquitous. The two of the most important cryptographic challenges for future mobile communications, unanswered by current 3G/4G solutions today [1, 2], are designing:

- a versatile secure-channel establishment protocol in 5G networks;
- secure and privacy-preserving protocols for resource-constrained IoT devices.

An important difference between current and future mobile architectures is, indeed the variety of devices for which security solutions must be found. Current mobile phones are vulnerable to many attacks, e.g., malware, Denial-of-Service (DoS), tracking, and cryptographic attacks. Future networks will include IoT devices, which are even more attack-prone, and can be used as "tools" in cyber-attacks. The transition to 5G networks is expected to not only combine, but to compound risks to all types of devices.

Moreover one of the most important threats to mobile security is that of *mass surveillance attacks* [5]. Following the revelations of Edward Snowden regarding mass-scale tracking of users and illicit decryption of data by large counterintelligence agencies, like GCHQ and the NSA, cryptographers have begun to develop countermeasures to large-scale espionage. One way of achieving this is by ensuring that strong end-to-end secure-channel establishment can be achieved between any two parties exchanging data. A further principle is that of putting as little trust as possible in any node, which implies – for 5G networks – that even if strong devices do help weaker devices handle sensitive data, the stronger devices should never have direct access to that data. Finally, one must be able to guarantee security even in the presence of semi-trusted parties, such as operators or intermediate nodes in the infrastructure. Promising points of departure in this setting could be the research on reverse firewalls by Dodis et al. [4], or the work on authentication in the presence of anonymizers of Sadeghi et al. [6].

Addressing these challenges is the aim of the ANR project MOBIS5 and also the goal of the Ph.D.

Ph.D. Goals

This thesis is funded by the ANR project MOBIS5 and aims to tackle the following two fundamental aspects in 5G networks:

IoT: Providing secure and privacy-preserving protocols that allow large 5G devices to aid resource-constrained IoT devices to securely handle functionalities such as: authentication, secure-channel establishment, and computing on sensitive data.

AKE: Providing a secure and versatile means of establishing a secure channel between any two 5G devices, whether they are resource-constrained or not, registered with the same operator or two different operators, or whether they be within a personal network or in a larger one.

In both cases, the explicit methodology adopted would be that of designing protocols and then proving the precise security and privacy they provide. The student will focus on *formal verification*, especially with the aid of adapted tools such as ProVerif, Tamarin, etc. Where appropriate, the results of the automated verification will also be supported by computational proofs of security.

Skills: We are looking for excellent candidates, in possession of a Master Degree (or equivalent) in Mathematics or Computer Science. The candidate must have some knowledge of cryptography (visible in courses taken at master level and potentially internship work in that field), an interest in research, and a good level of written and spoken English. Work in fields related to mobile networks, authenticated key-exchange, implementations on resource-constrained devices, or formal verification of cryptographic protocols/primitives is considered a very strong plus.

The candidate will spend three years in a dynamic team that favours academic excellence. You will have a fair amount of leeway to choose the direction in which you want to push your Ph.D. The thesis is part of a large-scale 4-year project, ANR MobiS5, which will give the candidate an opportunity to interact with the members of our consortium, including: Orange Labs, the University of Rennes 1, and EURECOM.

How to apply ? Prepare a 1-page letter of motivation, a 2-page CV, an extract of all your grades and subjects taken throughout your Master degree, and a 2 pages essay describing how you see your Ph.D. evolve within the topics presented above. Be sure to include any topics that interest you, any topics you would like to avoid, and what you would like to bring to the research team.

You have to send the required documents *in PDF format ONLY* to the email addresses: `pascal.lafourcade@uca.fr` and `cristina.onete@gmail.com` as soon as possible. We will receive applications until the post has been filled.

References

[1] S. Alt, P.A. Fouque, G. Macario-Rat, C. Onete and B. Richard. *A cryptographic analysis of the 3GPP AKA protocol.* In Proceedings of ACNS, pp. 18-35. (2016)

[2] P.A. Fouque, C. Onete and B. Richard. *Achieving better privacy for the 3GPP AKA protocol.* In PoPETS. vol. 2016/4, pp. 255-275. (2016)

[3] F. van den Broek, R. Verdult and J. de Ruiter. *Defeating IMSI catchers.* In: Proceedings of ACM SIGSAC. pp. 340-351, (2015)

[4] Y. Dodis, I. Mironov and N. Stephens-Davidowitz. *Message transmission with reverse firewalls ? Secure communication on corrupted machines.* In CRYPTO, pp. 341-372. (2016)

[5] M. Bellare, K.G. Paterson and P. Rogaway. *Security of symmetric encryption against mass surveillance.* In CRYPTO 2014, pp. 1-19. (2014)

[6] A.R.Sadeghi, I. Visconti and C. Wachsmann. *Anonymizer-Enabled Security and Privacy for RFID* In CANS 2009, (2009)