Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

Cryptography and Public-Key Infrastructures (PKIs)

Author(s): André Schaller (TUD)

CC RG-11, CC RG-13, CC RG-85 and CT RG-8, CT RG-12, CT RG-76 - Strong and efficient cryptographic primitives for low-end embedded devices and sensors
CC RG-15, CC RG-25, CC RG-26 and CT RG-25, CT RG-26 - Simple and efficient key distribution mechanisms and Public-Key Infrastructures
CC RG-66, CC RG-03 and CT RG-61, CT RG-83 - Preserving future resilience of encryption and authentication schemes

ABSTRACT

This document summarizes main research gaps regarding cryptographic protocols as well as key distribution and management schemes in order to ensure appropriate levels of security in future technologies. In particular, due to the massive deployment of low-end devices, either in the form of 'smart' Internet-of-Things technology or as sensors to make up Industry 4.0 infrastructure, a new class of lightweight crypto primitives is required. They must adhere to new requirements such as low energy consumption, minimal hardware footprint and easy synthetization in hardware. Securing vastly deployed devices is of utmost importance as they are considered as the building blocks of upcoming technological trends such as smart city, car-to-X scenarios and more. Furthermore, technologies to distribute and manage cryptographic keys in a way that allows for efficient scaling and preserves the security of the overall system are required for secure interaction with distributed devices. Lastly, those schemes and cryptographic primitives must provide sufficient usability for the end-user and further must remain resilient against attacks in the future. Thus, post-quantum secure encryption and authentication schemes must be considered.

RESEARCH ACTION #1

Development and security analysis of lightweight encryption and authentication schemes as well as hash functions for low-end mobile devices.

DISTANCE TO THE MARKET: **TRL 6**
COST OF THE TOPIC: **2 STREPs + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **18 months**
ACTORS: **Research Institutions, Industry, Policy-makers**

New lightweight cryptographic primitives must be found, including encryption schemes, hash functions as well as authentication schemes that are optimized towards area, energy consumption, throughput as well as latency.
With mobile devices becoming smaller, the importance of minimized area consumption on the silicon (usually measured in Gate Equivalents, GEs) is growing. If future cryptographic primitives do not meet the requirements of industry and the markets, security levels of mobile devices will decrease or cryptographic means will not be implemented at all.
Considering the vast amount of mobile devices that will be embedded in various elements of everyday life, energy consumption of each individual device will become a critical factor. Thus, it is reasonable to consider the energy consumption imposed by cryptographic elements and subsequently optimize them towards low-energy.
With low-end devices being used as sensors and actuators in industrial facilities, the importance of low latency in the context of real-time operations is increasing.
While some candidates exist for block ciphers, i.e. PRINCE, KATAN, SIMON and SPECK that are optimized towards area and speed, there is a lack of comparative studies as those block ciphers have been implemented using different technologies. Thus, common test cases with identical interfaces must be established, as already proposed by the ECRYPT project. Further, although there are first efforts towards proving security of lightweight ciphers, it is an open question to what extent they are vulnerable against side-channel analysis. Especially in the case of using low-end devices (such as sensor node in the context of smart cities), these devices will be likely much more physically exposed compared to current device classes, which makes them more vulnerable against side-channel attacks. Also, considering that devices are sending sensor measurements in order to control parts of the infrastructure of a smart city, integrity and authentication of the sensor values will become an important security objective. Thus, authenticated encryption (i.e. AES-GCM/ AES-GCC) must be examined towards its compatibility with resource-constrained devices. Subsequently, the implementation of secure and lightweight cryptographic primitives in mission-critical low-end devices must be guaranteed by defining standards, policies and/or laws.

RESEARCH ACTION #2

Scalable key distribution and management schemes for secret-key based cryptosystems and networks with highly dynamic topologies.

DISTANCE TO THE MARKET: **TRL 7**
COST OF THE TOPIC: **2 STREPs**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **12 months**
ACTORS: **Research Institutions, Industry**

Considering the vastly growing numbers of embedded devices, that will be part of smart cities, the smart metering grid of the future and industrial facilities as well as those which will be used as wearables and in the context of the quantify-yourself trend, a critical point in maintaining security of those devices is whether one would be able to efficiently distribute and maintain cryptographic keys and certificates. From the perspective of the end-user, complex systems like PKIs must be made transparent and understandable. Nowadays, most often PKI-based errors are ignored which corrupts the PKI and its security properties as a whole. Thus, the PKI must be appropriately used and trusted by all users in order to make it work. Additionally, maintenance of Registration Authorities must be made easy enough for human operators. Interesting questions arise when considering the scenario where a hardware device (i.e., smart grid) must be rekeyed due to compromise of the private key, such as how to choose a methodology or standard according to which the party that revokes or re-certifies the device can be authorized. Also, there remain open questions regarding large-scale revocation, i.e., in case of a compromise of a CA that is responsible for a complex PKI.
Furthermore, with mobile devices forming networks with highly dynamic topologies, i.e. Vehicular Ad-Hoc Networks (VANETS) or mesh networks, new approaches to distributing, updating or revoking keys are required. Additionally, considering the autonomous sensor networks which lack a central coordinating instance, traditional PKI-based approaches or hierarchical Key Management Systems in general are not applicable.
Regarding highly resource-constrained devices that usually only support symmetric key cryptography, there are open research challenges with respect to key distribution approaches that scale sufficiently.

RESEARCH ACTION #3

Development and evaluation of (lightweight) quantum-resistant encryption and authentication schemes as well as digital signatures.

DISTANCE TO THE MARKET: **TRL 4**
COST OF THE TOPIC: **2 STREPs + 2 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **48 months**
ACTORS: **Research Institutions, National Institutions**

In order to preserve security provided by encryption schemes in the future, it is not sufficient to rely on encryption schemes whose security is based on hardness assumptions. Rather, the (currently theoretical) construction of a quantum-computer must be considered, as its realization would make obsolete any cryptosystem that bases security on the hardness of factoring integers or the discrete-log problem. Thus, finding post-quantum secure (PQS) encryption and authentication schemes as well as hash functions are subject to current research.
Numerous subsequent questions arise, such as whether potential PQS cryptosystems are efficient enough to be used by highly-occupied systems (i.e., webserver or resource-constrained devices such as IoT platforms or wireless scenarios. Currently the public keys of PQS systems are rather large. Generally, as for any cryptosystem, trust must be established in potential PQS candidates by providing security proofs or conducting extensive cryptanalysis. The same holds for other cryptographic primitives such as digital signatures. This challenge also asks for new security models and exhaustive studies of the underlying algorithmic problems in general. Furthermore, there is a lack of knowledge regarding the resistance of PQS schemes against side-channel attacks due to the limited number of actual implementations, in software as well as hardware.
Another important aspect with respect to PQS schemes is the complexity of their implementation. As many crypto-related security incidents of the past suggested, the secure implementation of a theoretically secure cryptographic system often is the weak point. Finally, in order to make actual usage of quantum-resistant cryptosystems they must provide sufficient usability such that the average end-user is able to interact with it conveniently. Without broad user adaption such algorithms will remain theoretical concepts that do not contribute to actual security in our digital communication.