Master internship from February to July 2023:

Post-Quantum Cryptography Key Establishment for constrained IoT nodes and networks

Keywords: Post-Quantum Cryptography, IoT, ARM Cortex-M3, Key Establishment

Context

There is a non-zero probability of usable large-scale Quantum Computers (QCs) in the next 50 years. A QC can break all widely used asymmetric cryptographic protocols and the systems that rely on them, like the Internet, banking systems, or cellular networks. To anticipate the existence of the QC, the cryptographic community has been working on Post-Quantum Cryptography (PQC): cryptography that can run on classical computers and that is secure against a QC. Since 2016, the U.S. National Institute of Standards and Technology (NIST) has started a procedure to standardize one or more quantum-resistant cryptographic algorithms [1]. However, current PQC proposals use more resources (e.g., ram, flash, cpu), in particular requiring larger key sizes, than non-quantum cryptography and the question of their usability for embedded systems and constrained networks – like Internet of Things (IoT) systems– remains unanswered [2,3].

Objectives

The internship objective will be to select, implement, and evaluate one or more of the NIST's Key-establishment/Key Encapsulation Mechanisms (KEM) PQC candidates (e.g., Kyber and Saber), on an IoT embedded device based on the ARM Cortex-M3 processor. We expect to re-use as much as possible existing open-source code implementations of required primitive operations [4,5]. Moreover, we will propose a compact representation of the KEM messages to exchange over constrained IoT networks and build a demonstrator showing a successful key establishment.

Work to accomplish

First, the intern will familiarize with the general IoT constraints, the exiting NIST-based PQC KEM protocols, programming for an embedded Cortex-M3 platform and the existing PQC implementations for Cortex-M [4,5]. This first phase, estimated at two months, will end with a justified selection of potential PQC KEM protocol(s) that will be implemented on a Cortex-M3.

Then, the second phase will be about implementing/adapting the KEM protocol(s) on a Cortex-M3 hardware platform like the OpenMoteB [6]. The focus of this phase is on the IoT node. Evaluation and benchmarking against non-constrained implementations (e.g., used resources like cycles, ram, flash) will be conducted. However, the main objective is to have a proof of concept, i.e., running code on a Cortex-M3.

Finally, the focus will be on the IoT network: we will take in account the constraints of the network (e.g., max. size of messages, unreliable messages), to propose a suitable and compact exchange for the KEM messages, we will leverage state-of-the-art standards like IETF's Concise Binary Object Representation (CBOR) [7]. We aim at implementing the proposal on the hardware platform to provide a fully functional demonstration of a PQC KEM mechanism on a constrained node (Cortex-M3) and a constrained wireless network.

Expected skills and knowledge

Candidates should master the essential concepts of computer security and computer networks. System and programming skills will be required to be able to implement/adapt cryptographic protocols on an embedded device. In particular, C language programming skills are expected.

Internship conditions

The internship takes place within the SRCD department of IMT Atlantique and falls within the scientific axis "Cyber-security". An office, shared by several internship students, will be allocated to the intern with a fixed computer for work.

Internship remuneration is around € 530 per month.

Contact

Renzo NAVAS: renzo.navas@imt-atlantique.fr -- https://cv.archives-ouvertes.fr/rnavas

Referennces

[1] “NIST: Post-Quantum Cryptography”. URL: https://csrc.nist.gov/projects/post-quantum-cryptography
[2] Khalid, Ayesha, Sarah McCarthy, Maire O’Neill, and Weiqiang Liu. "Lattice-based cryptography for IoT in a quantum world: Are we ready?." In *2019 IEEE 8th international workshop on advances in sensors and interfaces (IWASI)*, pp. 194-199. IEEE, 2019.
[3] Fernández-Caramés, Tiago M. "From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things." *IEEE Internet of Things Journal* 7, no. 7 (2019): 6457-6480.
[4] "pqm4: Post-quantum crypto library for the ARM Cortex-M4". URL: https://github.com/mupq/pqm4
[5] Greconici, Denisa OC, Matthias J. Kannwischer, and Daan Sprenkels. "Compact dilithium implementations on Cortex-M3 and Cortex-M4." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2021): 1-24.
[6] “OpenMoteB: FIT – IoT LAB” https://iot-lab.github.io/docs/boards/openmoteb/
[7] Carsten Bormann, & Paul E. Hoffman. (2020). RFC 8949 : Concise Binary Object Representation (CBOR) . URL: https://datatracker.ietf.org/doc/rfc8949/