PRESERVE: Privacy-preserving Communication for Lightweight Applications

Open position for research associate with duration 6 months

Summary

With the widespread use of resource-constrained devices such as RFID sensors, IoT, etc. the area of lightweight cryptography has become increasingly important. For evidence we can look to the current standardisation effort by the US National Institute of Standards and Technology (NIST) aimed at selecting the new world standard/s in lightweight cryptography (LC) [1].

In the world of anonymous Internet communication the onion routing network Tor [4] has established itself as the standard for private and anonymous communication. Unfortunately Tor is not a viable solution for networks of small highly constrained devices such as sensor networks, smart homes and smart cities. Furthermore, the threat model for Tor admits a global passive adversary, meaning that Tor is not a viable solution in smart home and city scenarios where a global eaves dropping capabilities are not beyond the reach of real world actors.

In this project we propose to research the application of privacy- preserving technologies such as secret sharing, differential privacy, and authenticated connections for lightweight devices. The goal is to design an efficient privacy-preserving communication network that will make use of future standards in LC with the privacy-preserving properties available on the Internet of today

Objectives

- Design an efficient framework for privacy-preserving communication using latest standards in lightweight cryptography.
- Survey and evaluate the current state of the art and future directions
- Identify the most promising cryptographic primitives that we may use for the purpose

Candidate requirements

Looking for a candidate fitting one of the following profiles:

*** Profile 1 (Research-oriented)**

- Has research experience as evidenced by publications in any of the following areas: privacy, security, applied cryptography, cryptographic implementations

Note: Also suitable for a last-year PhD student

*** Profile 2 (Implementation-oriented)**

At least one of the following is required:

- Experience with programming for embedded devices (e.g. IoT, LoRaWAN)
- Experience with hardware implementations

Desired, but not required:

- Knowledge of cryptography and cryptographic implementations (software and/or hardware)

More info

- https://www.rephrain.ac.uk/preserve/
- Contact: Vesselin Velichkov at vvelichk@ed.ac.uk