March 7th 2019

Lightweight Cryptographic Group Key Management Protocols for the Internet of Things

Author licentiate thesis: Teklay Gebremichael
STC Research Centre
Mid Sweden University

Abstract

The Internet of Things (IoT) is increasingly becoming an integral component of many ap-plications in consumer, industrial and other areas. Notions such as smart industry, smart transport, and smart world are, in large part, enabled by IoT. At its core, the IoT is under-pinned by a group of devices, such as sensors and actuators, working collaboratively to provide a required service. One of the important requirements most IoT applications are expected to satisfy is ensuring the security and privacy of users. Security is an umbrella term that encompasses notions such as confidentiality, integrity and privacy, that are typically achieved using cryptographic encryption techniques.

A special form of communication common in many IoT applications is group communication, where there are two or more recipients of a given message. In order to encrypt a message broadcast to a group, it is required that the participating parties agree on a group key a priori.Establishing and managing a group key in IoT environments, where devices are resources constrained and groups are dynamic, is a non-trivial problem. The problem presents unique challenges with regard to constructing protocols from lightweight and secure primitives commensurate with the resource-constrained nature of devices and maintaining security as devices dynamically leave or join a group.

This thesis presents lightweight group key management protocols proposed to address the aforementioned problem, in a widely adopted model of a generic IoT network consisting of a gateway with reasonable computational power and a set of resource-constrained nodes. The aim of the group key management protocols is to enable the gateway and the set of resource constrained devices to establish and manage a group key, which is then used to encrypt group messages. The main problems the protocols attempt to solve are establishing a group key among participating IoT devices in a secure and computationally feasible manner; enabling addition or removal of a device to the group in a security preserving manner; and enabling generation of a group session key in an efficient manner without re-running the protocol from scratch.The main challenge in designing such protocols is ensuring that the computations that a given IoT device performs as part of participating in the protocol are computationally feasible during initial group establishment, group key update, and adding or removing a node from the group.

The work presented in this thesis shows that the challenge can be overcome by designing protocols from lightweight cryptographic primitives. Specifically, protocols that exploit the lightweight nature of crypto-systems based on elliptic curves and the perfect secrecy of the One Time Pad (OTP) are presented. The protocols are designed in such a way that a resource constrained member node performs a constant number of computationally easy computations during all stages of the group key management process.

To demonstrate that the protocols are practically feasible, implementation result of one of the protocols is also presented, showing that the protocol outperforms similar state-of-the-art protocols with regard to energy consumption, execution time, memory usage and number of messages generated.

Sensible Things that Communicate
PART OF MID SWEDEN UNIVERSITY