Title: Lightweight end-to-end secure group communication for the IoT with CoAP and Group OSCORE

Abstract:

IoT deployments can benefit from communication with multiple recipients simultaneously, for instance by relying on one-to-many group communication. Utilizing group communication can save battery and processing power on constrained devices, and save overhead on constrained networks.

The Constrained Application Protocol (CoAP) is a lightweight, application layer protocol based on the REST paradigm. It is similar to HTTP, but specifically designed to be suitable to use for resource-constrained devices and IoT networks.

CoAP supports group communication, for example over IP multicast, where one request can reach multiple recipients. Such communication can be protected end-to-end with the Group OSCORE protocol. Group OSCORE ensures source authentication, confidentiality, replay protection, and integrity of protected CoAP messages.

This work presents ongoing efforts in the Internet Engineering Task Force (IETF) on secure group communication with CoAP and Group OSCORE, focusing on three related specifications. Together, these specifications enable an administrator to create and configure groups at a Group Manager, allow authorized nodes to join groups and obtain keying material, and enable the nodes to communicate using secure group communication after having joined.

Authors: Rikard Höglund, Marco Tiloca