Implementing End-to-End Security in Internet of Things

Vishwas Lakkundi
Altiux Innovations Private Limited
Bengaluru, INDIA

1. Abstract
Security is fast emerging as a key area of focus in the Internet of Things. Lightweight implementations of the required security features are necessary considering the resource constrained nature of the underlying nodes and networks. At the same time, it is essential that such implementations are robust, reliable and efficient. Security can be provided at different layers of the underlying protocol stack. This poster addresses these requirements by providing an end-to-end security framework for implementing a lightweight version of the DTLS protocol in the CoAP-based Internet of Things. In addition, this lightweight security approach is illustrated with a real-world application scenario and its performance analysis. It also provides an overview of the ongoing standardization activities in the IoT security domain.

2. Internet of Things

3. Security in IoT

4. Security in IoT - Protocols

5. Lightweight DTLS
- Supports pre-shared key (PSK) based security
- Supports advanced encryption standard (AES)
- Supports HMAC-SHA2 base hashing algorithm
- IETF Class-1 compliant (~100 KB ROM, ~10 KB RAM)

6. Performance Analysis

7. Application Scenario

8. Standardization Activities
- DICE: DTLS In Constrained Environments
  - Currently being standardized by IETF
  - Propose a minimal DTLS profile for use in IoT scenarios
  - Enables DTLS record layer for secure multicast transmissions
  - Investigates practical issues around DTLS handshake
  - DICE does NOT intend to modify DTLS state machine
  - Out of scope: key management and multicast sessions
- ACE: Authentication and Authorization for Constrained Environments
  - Currently being standardized by IETF
  - Identifies authentication and authorization mechanisms suitable for resource access in constrained environments
  - Produces use cases and requirements

References