Application Layer Security for the Internet of Things

CASTOR Software Days 15-10-2019
Francesca Palombini, Ericsson Research
HTTP
TCP
TLS
IP
QUIC
... and many more
The IoT is happening

Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020
The “T” in “IoT”

- maximum code complexity (ROM/Flash)
- size of state and buffers (RAM),
- amount of computation feasible in a period of time ("processing power"),
- available power
- user interface and accessibility in deployment (ability to set keys, update software, etc.).

---

<table>
<thead>
<tr>
<th>Name</th>
<th>data size (e.g., RAM)</th>
<th>code size (e.g., Flash)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 0, C0</td>
<td>&lt;&lt; 10 KiB</td>
<td>&lt;&lt; 100 KiB</td>
</tr>
<tr>
<td>Class 1, C1</td>
<td>~ 10 KiB</td>
<td>~ 100 KiB</td>
</tr>
<tr>
<td>Class 2, C2</td>
<td>~ 50 KiB</td>
<td>~ 250 KiB</td>
</tr>
</tbody>
</table>

Terminology for Constrained-Node Networks, RFC7228

---

Example: LoRaWAN architecture

Francesca Palombini - Ericsson Research
The “I” in “IoT” – Internet Protocol Stack

Constrained Application Protocol – RFC7252
Maps to HTTP, optimized for constrained
TCP is too expensive for constrained node networks, UDP is used instead. DTLS is developed to run over UDP.

Including an adaptation layer protocol such as 6LoWPAN, 6TiSCH, IPv6 over BLE
LoRaWAN, Zigbee (over IEEE802.15.4), Bluetooth LE, NB-IoT …
The “s” in IoT stands for “security”

**Strong coupling to physical assets**
- Intrinsic safety and privacy risks

**The number of things**
- Distributed Denial-of-Service

**The hype and low security incentives**
- Common insecure deployments

**Power constrained and sleepy devices**
- Security overhead challenges

**Gateways and proxies**
- End-to-end security challenges

---

*Need for end-to-end security in constrained environments*
Example scenario

**End-to-end aspects**
- Endpoints
- Transport layer protocols
- Application layer protocols
- Intermediaries

**Constrainedness**
- Message overhead
- Round-trips
- Public-key operations

**Security aspects**
- Encryption
- Integrity and replay protection
- Authentication
- Authorization

Diagram:
- Control/Aggregation
  - HTTP
  - TCP
  - IP
- HC Proxy
  - CoAP
  - UDP
  - IP
- Capillary GW
  - CoAP
  - NB-IoT
- Constrained Device
Application Layer Security for the IoT

Requirements

• Independence of transport layer
• Support for proxy operations
• Protection of REST operations (HTTP/CoAP)
• Optimized for constrained devices
• Standardized
• Wide applicability

Security layer?

REST method unprotected

Proxies cannot read

New IoT security protocols

ACE, EDHOC

OSCORE, Group OSCORE

Application

HTTP/CoAP

TCP/UDP

IP

Link
New IoT Security Protocols

• COSE (CBOR Object Signing and Encryption): Secure message format based on binary data format CBOR (small)

• OSCORE: Lightweight communication security protocol (once keys are in place)

• Group OSCORE: OSCORE in groups, adds signature

• EDHOC: Lightweight Diffie-Hellman key exchange
  To securely develop shared secrets to derive keys for OSCORE

• ACE: Lightweight authorization and access control
  A delegation protocol to convey authorization, enables a client to obtain scoped access to a resource
Object Security for Constrained Restful Environments - OSCORE

Application layer communication security protocol

- Object Security for Constrained RESTful Environments
- Protecting CoAP, HTTP, LwM2M
- End-to-end encryption, integrity and replay protection

Designed for constrained IoT deployments

- Low overhead (minimum 10-15 bytes)
- Low footprint in addition to CoAP
- Independent of transport layer
- Supports multicast and group communication

Developed by Ericsson Research in collaboration with RISE SICS

- Standardized in the IETF
- Adopted by LwM2M, OCF, Fairhair Alliance
- Open source Eclipse implementation in progress
- To be included in Ericsson IoT Accelerator
OSCORE Processing

- Addition to CoAP
- Uses Authenticated Encryption with Additional Data (AEAD)
- AES-128-CCM-8 mandatory to implement
- Protection of CoAP messages using the COSE format
- Replay protection
- Handling partial loss of security context
### OSCORE Message Overhead

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Overhead (B) for Sequence Number = '05'</th>
<th>Overhead (B) for Sequence Number = '1005'</th>
<th>Overhead (B) for Sequence Number = '100005'</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTLS 1.2</td>
<td>29</td>
<td>29</td>
<td>29</td>
</tr>
<tr>
<td>DTLS 1.3 (work in progress)</td>
<td>11</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>TLS 1.2</td>
<td>21</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>TLS 1.3</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td>DTLS 1.2 (GHC)</td>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>DTLS 1.3 (GHC) (wip)</td>
<td>12</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>TLS 1.2 (GHC)</td>
<td>17</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>TLS 1.3 (GHC) (wip)</td>
<td>15</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>OSCORE Request</td>
<td>13</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>OSCORE Response</td>
<td>11</td>
<td>11</td>
<td>11</td>
</tr>
</tbody>
</table>

EDHOC
Lightweight Key Exchange on Application Layer

Status

- Formal review by Univ. of Copenhagen
- Constrained implementation by Univ. of Murcia
- Significant reduction of overhead
- Mature specification
- Good support in the IoT community (6tisch, NB-IoT, LoRaWAN)

<table>
<thead>
<tr>
<th>Flight</th>
<th>#1</th>
<th>#2</th>
<th>#3</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTLS 1.3 RPK + ECDHE</td>
<td>149</td>
<td>373</td>
<td>213</td>
<td>735</td>
</tr>
<tr>
<td>DTLS 1.3 PSK + ECDHE</td>
<td>186</td>
<td>190</td>
<td>57</td>
<td>433</td>
</tr>
<tr>
<td>DTLS 1.3 PSK</td>
<td>136</td>
<td>150</td>
<td>57</td>
<td>343</td>
</tr>
<tr>
<td>EDHOC RPK + ECDHE</td>
<td>38</td>
<td>121</td>
<td>86</td>
<td>245</td>
</tr>
<tr>
<td>EDHOC PSK + ECDHE</td>
<td>43</td>
<td>47</td>
<td>12</td>
<td>102</td>
</tr>
</tbody>
</table>

Francesca Palombini - Ericsson Research
Authentication and Authorization for Constrained Environments (ACE)

ACE: Lightweight authorization and access control
A profile of OAuth 2.0 using CBOR and COSE secure objects, runs over CoAP

1. Client acquires Access Token from Authorization Server

1. Client presents Access Token to Resource Server to get access
Standardization and Implementation Status

- OSCORE is an IETF standard: RFC8613
- Several implementations exist, for several CoAP libraries: C, C#, Java, Python
- Interoperability tests have been run

- OSCORE group communication is in progress, and implementations are being developed

- EDHOC is a work in progress at IETF
- Partial implementations exist, formal verification has been done

- ACE is soon to be published as RFC
- A couple of implementations exist and have run interoperability tests
Key takeaways

- IoT is happening
- Security is important
- Former security solutions are not optimized
- We are working on it!