Securing IoT

Oscar Garcia-Morchon
ETSI Security Week
June 14th 2016
Internet of Things
Some use cases and features

- Constrained links
- Device to device
- Large network
- Low power
- Long-term

- Identify devices
- Low power
- Robust
- Speed

- Robust architecture
- Small packets
- Private data
- Low power
Abstracting
Many Requirements

Energy efficiency

Small and real-time

Device lifecycle
- Manufacturing
- Distribution
- Installation
- Operation
- Re-configuration
- End-of-life

Simple operation

Quantum secure
Many Requirements

Energy efficiency

Small and real-time

Device lifecycle

Manufacturing

Distribution

Installation

Operation

Re-configuration

End-of-life

Simple operation

Quantum secure

Challenge: Efficient and scalable management of keys/_credentials of devices
Device Lifecycle and Security Needs
Device Lifecycle and Security Needs

Security infrastructure

Root of trust

Root of trust

Device 1
Manufacturing

Server 1

Server s

Network access

Device 2

Device d

Device 3

Operation
Device Lifecycle and Security Needs

**Infrastructure**
- Out-of-band (secure manufacturing) and in-band (Internet) provisioning
- Efficient resistance to root capture
- Long term security
- Key escrow

**Diagram**
- Device 1: Manufacturing
- Root of trust
- Server 1
- Server s
- Network access
- Operation
- Device 2
- Device d
- Device 3
Device Lifecycle and Security Needs

Infrastructure
- Out-of-band (secure manufacturing) and in-band (Internet) provisioning
- Efficient resistance to root capture
- Long term security
- Key escrow

Network access
- Backend authentication/authorization
- Device authentication/authorization
- Device identification/blacklisting
- DoS prevention
Device Lifecycle and Security Needs

Infrastructure
- Out-of-band (secure manufacturing) and in-band (Internet) provisioning
- Efficient resistance to root capture
- Long term security
- Key escrow

Network access
- Backend authentication/authorization
- Device authentication/authorization
- Device identification/blacklisting
- DoS prevention

Operation
- Key agreement
- Collusion resistance
- Quantum resistance
- Easy protocol integration
- Forward security and key escrow
- Credential verification, e.g., public-keys
Options

**Online Key Distribution Center**
- KDC

**PKI**
- CA

**IBE**
- PGK

**Key Pre-Distribution Scheme**
- TTP
Options

Online Key Distribution Center

KDC

IBE

PGK

PKI

Key Pre-Distribution Scheme

Configuration

Operation
# HIMMO

Efficient Collusion- and Quantum-Resistant Key Pre-Distribution Scheme

<table>
<thead>
<tr>
<th>1) Setup</th>
<th>2) Keying material extraction</th>
<th>3) Operational protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTP</td>
<td>TTP</td>
<td>TTP</td>
</tr>
<tr>
<td>Secret $R(x, y)$</td>
<td>$ID$</td>
<td>$K_{A,B}$</td>
</tr>
<tr>
<td>Configuration parameters</td>
<td>$G_{ID}(x)$</td>
<td>$E_{K_{A,B}}(m)$</td>
</tr>
</tbody>
</table>

The diagrams illustrate the process:

1. **Setup**: TTP generates a secret $R(x, y)$ and distributes it to all parties.
2. **Keying material extraction**: TTP extracts the identity $ID$ and a function $G_{ID}(x)$.
3. **Operational protocol**: Party $A$ encrypts a message $m$ with the key $K_{A,B}$ and sends it to party $B$. Party $B$ decrypts it with their key $K_{B,A}$. 
HIMMO

- Efficient collusion- and quantum- resistant

- Easy protocol integration (TLS, MAC-layer level protocols, etc)

- Features
  - Identity-based
  - Multiple TTP support
  - Credential certification and verification
  - One-way key exchange and authentication in 30 Bytes

- Advantages
  - Very low overhead
  - Blacklisting feasible
  - Resilient TTP infrastructure
  - Out-of-the-box secure by factory configuration
  - Architectures able to support both forward secrecy and key escrow
Information and Contest for Open Verification

www.himmo-scheme.com

HIMMO
Efficient, authenticated, and quantum-resistant communications

Learn more »
Conclusions

• The IoT covers a plethora of use cases with very diverse needs

• The key challenge: efficient and scalable management of keys/credentials of devices through their lifecycle

• HIMMO is an efficient collusion- and quantum-resistant key pre-distribution scheme overcoming this problem
Literature


HI and MMO Problems

• Hiding Information (HI) problem [2]:
  Let \( f \in \mathbb{Z}[x] \) of degree at most \( \alpha \), \( x_i \in \mathbb{Z} \) and \( y_i = \langle f(x_i) \rangle_N \) for \( 0 \leq i \leq c \). Given \( \alpha, N, r, (x_1, y_1), \ldots, (x_c, y_c) \) and \( x_0 \), find \( y_0 \).

• Mixing Modular Operations (MMO) problem [3]:
  Let \( m \geq 2 \) and \( g_1, \ldots, g_m \in \mathbb{Z}[x] \), all of degree at most \( \alpha \), let \( x_i \in \mathbb{Z} \) and \( y_i = \sum_{j=1}^{m} \langle g_j(x_i) \rangle_{q_j} \) for \( 0 \leq i \leq c \). Given \( \alpha, m(x_1, y_1), \ldots, (x_c, y_c) \) and \( x_0 \), find \( y_0 \).
## Performance

<table>
<thead>
<tr>
<th>Target security level (bits)</th>
<th>Classical</th>
<th>Quantum</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>Identity size (B)</td>
<td>10</td>
<td>32</td>
</tr>
<tr>
<td>“Signature size” (B)</td>
<td>10</td>
<td>32</td>
</tr>
<tr>
<td>One-way key exchange (B)</td>
<td>20</td>
<td>75</td>
</tr>
<tr>
<td>One-way key exchange &amp; entity authentication (B)</td>
<td>30</td>
<td>107</td>
</tr>
<tr>
<td>PC time (ms)</td>
<td>0.29</td>
<td>0.68</td>
</tr>
<tr>
<td>NXP 120 MHz time (ms)</td>
<td>18.45</td>
<td>41.37</td>
</tr>
<tr>
<td>Required Root Hermite factor</td>
<td>1.008</td>
<td>1.0056</td>
</tr>
<tr>
<td>Pre-processing running time for LLL (years)</td>
<td>75</td>
<td>639.65</td>
</tr>
</tbody>
</table>
Certification and verification of information

1) Certification

\[ \text{TTP} \leftarrow \{Alice, 1982\} \rightarrow \text{A} \]
\[ G_{\text{Hash}(Alice, 1982)}(x) \]

2) Verification

\[ \text{A} \rightarrow \text{B} \]
\[ \text{Hash}(Alice, 1982), \ AE_{K_{A,B}}(m|\{Alice, 1982\}) \]

- \( K_{B,A} = G_B(\text{Hash}(Alice, 1982)) \)
- Decrypt and verify \( m \) (and implicitly, information)
Supporting multiple TTPs

- **Trusted**: never rely on a single authority, what if hacked or monitoring
- **Efficient**: same overhead as a single TTP scheme
- **Key escrow**: IFF agreement by all TTPs
Secure Device-to-Device Communication

- Problems
  - Whole system/network depends on a single master key
  - Credential management for millions of devices

- HIMMO key shares instead of a common secret
  - Quantum- and collusion-resistant
  - No overhead
  - Straightforward integration
  - Blacklisting feasible
  - Out-of-the-box secure by factory configuration
End-to-end secure communication

• Problems in (D)TLS
  – Non-PSK modes are resource-hungry and PSK does not scale
  – All cipher suites in (D)TLS (except PSK) are not quantum-resistant
  – Certification authority compromised → huge problem

• HIMMO can be easily integrated into (D)TLS-PSK mode by exchanging HIMMO identities in two parameters of DTLS-PSK

```
Client  | Server
---|---
HIMMO key  | HIMMO key
HIMMO credential verification | HIMMO key credential verification

*ServerKeyExchange (PSK identity hint = HIMMO fields)  
  ClientKeyExchange (Key hint = HIMMO fields), Finish
  Finish
```
HIMMO-based trust infrastructure
(IoT and beyond)

• We can even
  – Use HIMMO to authenticate public-keys: Public-keys are “signed” by several TTPs
  – Use public-key to securely distribute HIMMO keying material to a node

• Features
  – Extremely efficient public-key verification
  – Resilient TTP infrastructure
  – Supports forward secrecy and key escrow
  – Excellent **performance independent of TTP number**
  – Handshake modification enables **encrypted exchange of credentials**