Considerations (and solutions) for a lightweight, usable, and quantum-secure IoT

Oscar Garcia-Morchon
and Ronald Rietman, Ludo Tolhuizen, Sauvik Bhattacharya, Jose Luis Torre-Arce

Philips Research
Agenda

- Use cases and requirements
- Challenges
- Architectural options and HIMMO
- HIMMO directions
- Conclusions
Use cases and requirements
Internet of Things

Some use cases and features

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

- Robust architecture
- Small packets
- Private data
- Low power
- Long term
Abstracting

- Low energy (battery or harvesting)
- Small (100s bytes) packet
- Low (100s Kbps) data rate
- Long term (>10 years)
- Relatively slow CPU (10s MHz)
- Limited RAM (<10 KB)
- Limited memory (256 – 1024 KB)
Why Security in IoT?

Your privacy & safety

Company image and IPR

National security

Economy
Challenges
Why is Security Challenging in IoT?

Main reasons
• Business case $\rightarrow$ budget constrains $\rightarrow$ tight resources
• Application lifecycle $\rightarrow$ operational constrains

Many technical challenges (from www.ietf.org/id/draft-irtf-t2trg-iot-seccons-00.txt)
• DoS resistance
• Protocol translation
• End-to-end security
• Bootstrapping security
• Network access control (IP networks)
• Group membership and security
• IP network dynamics
• Long term security
• Software upgrade
• Intrusion detection
• Penetration testing
• Fine grained access control
• Re-selling devices
• System heritage
• Crypto agility (limited resources)
• Quantum-resistance
Why is Security Challenging in IoT?

Main reasons

• Business case → budget constrains → tight resources
• Application lifecycle → operational constrains

Many technical challenges (from www.ietf.org/id/draft-irtf-t2trg-iot-seccons-00.txt)

• DoS resistance
• Protocol translation
• End-to-end security
• Bootstrapping security
• Network access control (IP networks)
• Group membership and security
• IP network dynamics
• Long term security

• Software upgrade
• Intrusion detection
• Penetration testing
• Fine grained access control
• Re-selling devices
• System heritage
• Crypto agility (limited resources)
• Quantum-resistance

Challenge: efficient and scalable management of keys/credentials of devices
Why this challenge?

Challenge: efficient and scalable management of keys/credentials of devices
Why is Security Challenging in IoT?

Main reasons

- Business case → budget constrains → tight resources
- Application lifecycle → operational constrains

Many technical challenges (from www.ietf.org/id/draft-irtf-t2trg-iot-seccons-00.txt)

- DoS resistance
- Protocol translation
- End-to-end security
- Bootstrapping security
- Network access control (IP networks)
- Group membership and security
- IP network dynamics
- Long term security
  - Software upgrade
  - Intrusion detection
  - Penetration testing
  - Fine grained access control
  - Re-selling devices
  - System heritage
  - Crypto agility (limited resources)
- Quantum-resistance
Why is Security Challenging in IoT?

Main reasons
• Business case \(\rightarrow\) budget constrains \(\rightarrow\) tight resources
• Application lifecycle \(\rightarrow\) operational constrains

Many technical challenges (from [www.ietf.org/id/draft-irtf-t2trg-iot-seccons-00.txt](http://www.ietf.org/id/draft-irtf-t2trg-iot-seccons-00.txt))
• DoS resistance
• Protocol translation
• End-to-end security
• Bootstrapping security
• Network access control (IP networks)
• Group membership and security
• IP network dynamics
• **Long term security**

• Software upgrade
• Intrusion detection
• Penetration testing
• Fine grained access control
• Re-selling devices
• System heritage
• Crypto agility (limited resources)
• **Quantum-resistance**

Challenge: **Long term** efficient and scalable management of keys/credentials of devices
Why is Security Challenging in IoT?

Main reasons
• Business case → budget constrains → tight resources
• Application lifecycle → operational constrains

Many technical challenges (from www.ietf.org/id/draft-irtf-t2trg-iot-seccons-00.txt)
• DoS resistance
• Protocol translation
• End-to-end security
• Bootstrapping security
• Network access control (IP networks)
• Group membership and security
• IP network dynamics
• Long term security

• Software upgrade
• Intrusion detection
• Penetration testing
• Fine grained access control
• Re-selling devices
• System heritage
• Crypto agility (limited resources)
• Quantum-resistance

Challenge: Long term efficient and scalable management of keys/credentials of devices
Why is long-term security a challenge?

The construction of a large scale fault tolerant quantum computer would mean:

<table>
<thead>
<tr>
<th>Symmetric primitive</th>
<th>Security level</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES128</td>
<td>64</td>
</tr>
<tr>
<td>AES256</td>
<td>128</td>
</tr>
<tr>
<td>ECC</td>
<td>0</td>
</tr>
<tr>
<td>RSA</td>
<td>0</td>
</tr>
</tbody>
</table>

Challenge: Long term efficient and scalable management of keys/credentials of devices
Why is long-term security a challenge?

There are some proposed public-key primitives, but there are performance challenges:

<table>
<thead>
<tr>
<th>Primitive</th>
<th>Communication overhead</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMSS</td>
<td>(~39000 \text{ bits} (w = 4))</td>
<td>Scheme with short signatures?</td>
</tr>
<tr>
<td>New Hope</td>
<td>(~3800 \text{ bits})</td>
<td>Efficient key exchange?</td>
</tr>
<tr>
<td>Frodo</td>
<td>(~22500 \text{ bits})</td>
<td>How to upgrade deployed hardware?</td>
</tr>
<tr>
<td>AES128</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Challenge: **Long term efficient** and scalable management of keys/credentials of devices
Architecture options
Architectural Options
Architectural Options

Online Key Distribution Center

KDC

PGK

IBE

CA

PKI

TTP

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><img src="TTP.png" alt="" /></td>
<td><img src="TTP.png" alt="" /></td>
<td>![](Identity-based key exchange with implicit authentication.png)</td>
</tr>
</tbody>
</table>

- **Configuration parameters**
  - **TTP**: $\text{Secret}_R$
  - **$a$**
  - **$S_a(x)$**
  - **$E_{K_{a,b}}(m)$**
  - **$K_{a,b}$**
  - **$K_{b,a}$**

Identity-based key exchange with implicit authentication
HIMMO

www.himmo-scheme.com

- Efficient collusion- and quantum- resistant
- Easy protocol integration (TLS, MAC-layer level protocols, etc)
- Features
  - Key exchange
  - 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
HIMMO directions
HIMMO directions

• Running challenge with HIMMO design according to https://eprint.iacr.org/2016/152.pdf

• We have kept analyzing HIMMO and also ways of optimizing design
Current HIMMO design (online challenges)

Setup

Keying material extraction

Operation

\[ s_a = \left( \sum_{i=0}^{m-1} \langle aR_i \rangle_{q_i} \right)_N \]

\[ \mathbf{R}_i \text{ be a random symmetric } t \times t \text{ matrix over } \mathbb{Z}_{q_i}, \text{ for } 0 \leq i \leq m - 1 \]

\[ s_a, b = \left( \langle s_a b^T \rangle_N \right)_{2^b} \]

\[ k_{a,b} = \left[ \frac{s_{a,b}}{2^u} \right] \]

\[ h = \langle s_{a,b} \rangle_{2^u} \]

\[ E_{K_{a,b}}(m), h \]

\[ s_{b,a} = \langle s_b a^T \rangle_N \]

\[ s_{a,b} = f(s_{b,a}, h) \]

\[ k_{a,b} = \left[ \frac{s_{a,b}}{2^u} \right] \]

As in https://eprint.iacr.org/2016/152.pdf but with different notation
Simplifying the HIMMO design

\[ s_a = \langle aR + \epsilon_a \rangle_N \]

\[ a, b, \epsilon_a, \epsilon_b \in [0, 2^b - 1]^t \]

\[ s_b \]

\[ N \text{ be an integer of bit length } 3b \]

\[ R \text{ be a random symmetric } t \times t \text{ matrix over } Z_N \]

\[ s_{a,b} = \langle sb^T \rangle_N \]

\[ k_{a,b} = \left\lfloor \frac{s_{a,b}}{2^{2b+u}} \right\rfloor \]

\[ h = \left\lfloor \frac{s_{a,b}}{2^{2b}} \right\rfloor_2 \]

\[ s_{b,a} = \langle sb^T \rangle_N \]

\[ s_{a,b} = f(s_{b,a}, h) \]

\[ k_{a,b} = \left\lfloor \frac{s_{a,b}}{2^{2b+u}} \right\rfloor \]

Note: Before \( \epsilon_a \) determined by \( \beta_i, R_i \) and \( a \). Now random
About the simplified design

• Operationally equivalent to existing HIMMO design (eprint 2016/152)

• For work done so far, same attacks and security parameters seem to apply.

• It shares some similarities with LWE, but it is not LWE.
  
  – Key difference: identity vector is not evenly distributed in $\mathbb{Z}_N$ since it is short.
  
  – The fact that the identities are shorter implies that a larger value of $t$ is required to deal with existing attacks

• Further simplifications are feasible.
Parameters and performance

- **Security notion**
  - **Information-theoretically secure:** attacker needs $c > 3t/2$ nodes to attack a system. In a small network with $d$ devices, we can use small $t = 2d/3$
  - **Computational security:** for $b$ parameter (e.g., 16) and a relatively large $t$ (e.g., 2000) a high quality (slow) lattice reduction algorithm is needed to obtain a lattice basis with a small enough root Hermit factor (e.g., < 1.005)

- **Estimated performance**

<table>
<thead>
<tr>
<th>Parameters (t/b)</th>
<th>Inf.-theor. Security</th>
<th>Computational security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters (t/b)</td>
<td>200/32</td>
<td>2000/16</td>
</tr>
<tr>
<td>Network size</td>
<td>e.g., $d = 300$</td>
<td>Any</td>
</tr>
<tr>
<td>Communication overhead</td>
<td>48 $B$</td>
<td>96 $B$</td>
</tr>
<tr>
<td>Keying material size</td>
<td>6.25 $KB$</td>
<td>30 – 60 $KB$</td>
</tr>
<tr>
<td>Code / RAM size</td>
<td>&lt; 500 $B$, ~ 40 $B$</td>
<td></td>
</tr>
<tr>
<td>Security level</td>
<td>128 bits long key</td>
<td>Up to 256 bit long key</td>
</tr>
</tbody>
</table>
Conclusions

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

• IoT has many security challenges ahead; many more in the advent of quantum computers: efficiency, transition, key/credential management

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

• HIMMO (www.himmo-scheme.com) is an efficient collusion- and quantum-resistant scheme overcoming this problem
Many Requirements

- Energy efficiency
- Small and real-time

Simple operation

- Device lifecycle
- Long term security
Attacks Paths and Security Analysis

- Eve has any set of $c$ compromised keying materials $s_{x_1}, ..., s_{x_c}$. Eve’s goal is to find the key shared between Alice and Bob, $k_{a,b}$.

- Attack paths:
  - Try to recover $k_{a,b}$ by attacking the TTP: recovers $R$, $s_x$, and any $k_{x,y}$.
  - Try to recover $k_{a,b}$ by attacking Alice’s $s_a$ (or Bob): recovers $s_a$, and any $k_{a,y}$.
  - Try to recover $k_{a,b}$ only.

- Security analysis for the above attack paths is described here

About the HIMMO Contest

- No time limit, you can take as much time as you need
- Five challenges for $b = 32$
- 1000 Euros per solved challenge

<table>
<thead>
<tr>
<th>Challenge</th>
<th>$t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIMMO1</td>
<td>2000</td>
</tr>
<tr>
<td>HIMMO2</td>
<td>4000</td>
</tr>
<tr>
<td>HIMMO3</td>
<td>8000</td>
</tr>
<tr>
<td>HIMMO4</td>
<td>16000</td>
</tr>
<tr>
<td>HIMMO5</td>
<td>32000</td>
</tr>
</tbody>
</table>
+ Information and Contest for Open Verification

www.himmo-scheme.com

HIMMO

Efficient, authenticated, and quantum-resistant communications

Learn more »
Key Pre-Distribution Scheme

A key pre-distribution scheme involves a trusted third party TTP and nodes $N_1, \ldots, N_l$ and consists of the following three components.

• **Setup.** An algorithm run by TTP for generating secret root keying material $R$ and public system parameter $P$, given a security parameter.

• **Extract.** An algorithm run by TTP for generating secret keying material $s_x$ for a given node $N_x$, given root keying material $R$ and system parameter $P$.

• **Key establishment.** A protocol run by node $N_x$ and $N_y$ for generating shared key $k_{x,y}$, given secret keying material $s_x$ and $s_y$, and system parameter $P$. 
Rationale

Features of KPS
✓ Efficient
✓ Any node can directly obtain a pairwise key with any other any node
✓ Based on identities so that it is possible to verify them
✓ Multiple TTP support so that a single TTP does not have access to all keys
X KPS collusion resistance

Our goal with HIMMO was to achieve collusion resistance while keeping the rest of nice features
HIMMO in Practice

Extraction

\[ R_i^l \quad q_i^l \]

TTP I

\[ S_x \]

\[ x, S_x \]
HIMMO in Practice

One-way key exchange and entity authentication
HIMMO in Practice
Implicit certification and verification of parameters

\[ R_i^I, q_i^I \]

\text{TTP I}

\[ x, s_x \rightarrow A_{E_{k_{x,y}}}\{M\}, h \rightarrow y, s_y \]

\[ k_{x,y}, k_{y,x} \]

x (and any parameters (e.g., access roles) in it) is implicitly verified
HIMMO in Practice

Multiple TTP support

Single TTP does not have access to communication

x (and any parameters (e.g., access roles) in it) is implicitly verified

HIMMO in Practice

HIMMO for certification of public-keys

Single TTP cannot fake the MAC that verifies x’s public key ($pu_x$)

Device Lifecycle and Security Needs

Root of trust

Device 1

Root of trust

Server 1

Device 2

Server s

Device d

Device 3
Device Lifecycle and Security Needs
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
- Manufacturing
- Operation

Root of trust
- Server 1
- Server s
- Device 1
- 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