HIMMO

Oscar Garcia-Morchon, Ronald Rietman, Ludo Tolhuizen

July 2016
Aims of the presentation

• To share work done at Philips Research
• To discuss rationale of HIMMO
• To get feedback on our work
Contents

• Key Pre-Distribution Schemes
• HIMMO
• The HIMMO Contest
• Performance
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
\( \langle x \rangle_m \) is the integer in \([0, x)\) such that \( x \equiv \langle x \rangle_m \pmod{m} \)

**HIMMO**

- **Setup.**
  - Determine positive integers \( b, m, u, t \) for a given security parameter
  - Let \( N \) be an odd integer of bit length \( 3b \)
  - Let \( q_i = N - \beta_i 2^b \) for \( \beta_i \) being a secret \( b \) bit positive integer, for \( 0 \leq i \leq m - 1 \)
  - Let \( R_i \) be a random symmetric \( t \times t \) matrix over \( \mathbb{Z}_{q_i} \), for \( 0 \leq i \leq m - 1 \)

- **Extract.**
  - Associate node \( N_x \) with a public random vector identifier \( x \in [1, 2^b]^t \)
  - TTP provides node \( N_x \) with secret key generating vector \( s_x = \langle \sum_{i=0}^{m-1} \langle xR_i \rangle_{q_i} \rangle_N \)

- **Key establishment.**
  - \( N_x \) computes \( s_{x,y} = \langle \langle s_y x \rangle^T \rangle_N \) and determines \( k_{x,y} = \left\lfloor \frac{s_{x,y}}{2^u} \right\rfloor \) and \( h = \langle s_{x,y} \rangle_{2^u} \)
  - \( N_x \) sends \( h \) to \( N_y \)
  - \( N_y \) computes \( k_{x,y} \) from \( k_{y,x} \) and \( h \) as \( \left\lfloor \frac{\langle K_{y,x} + \lambda N \rangle_{2^b}}{2^u} \right\rfloor \) where \( \lambda = \left\lfloor \frac{N^{-1}(h - k_{y,x})}{2^u} \right\rfloor \)

---


\( \langle x \rangle_m \) is the integer in \([0, x)\) such that \( x \equiv \langle x \rangle_m \pmod{m} \)

**HIMMO**

- **Setup.**
  - Determine positive integers \( b, m, u, t \) for a given security parameter
  - Let \( N \) be an odd integer of bit length \( 3b \)
  - Let \( q_i = N - \beta_i 2^b \) for \( \beta_i \) being a secret \( b \) bit positive integer, for \( 0 \leq i \leq m - 1 \)
  - Let \( R_i \) be a random symmetric \( t \times t \) matrix over \( \mathbb{Z}_{q_i} \), for \( 0 \leq i \leq m - 1 \)
- **Extract.**
  - Associate node \( N_x \) with a public random vector identifier \( x \in [1, 2^b]^t \)
  - TTP provides node \( N_x \) with secret key generating vector \( s_x = \langle \sum_{i=0}^{m-1} \langle xR_i \rangle_{q_i} \rangle_N \)
- **Key establishment.**
  - \( N_x \) computes \( s_{x,y} = \langle \langle s_x y^T \rangle_N \rangle_{2^b} \) and determines \( k_{x,y} = \left[ \frac{s_{x,y}}{2^u} \right] \) and \( h = \langle s_{x,y} \rangle_{2^u} \)
  - \( N_x \) sends \( h \) to \( N_y \)
  - \( N_y \) computes \( k_{x,y} \) from \( k_{y,x} \) and \( h \) as \( \left[ \frac{\langle k_{y,x} + \lambda N \rangle_{2^b}}{2^u} \right] \) where \( \lambda = \left[ \frac{N^{-1}(h - k_{y,x})}{2^u} \right] \)

---

HIMMO in practice

Extraction

$R_i^l$, $q_i^l$

TTP I

$s_x$

$x, s_x$
HIMMO in practice
One-way key exchange and entity authentication

\[ k_{x,y} \xrightarrow{AE_{k_{x,y}}\{M\}, h} y, s_y \]

\[ x, s_x \]
HIMMO in practice
Implicit certification and verification of parameters

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

$k_{x,y} \rightarrow x, S_x \rightarrow \text{AE}_{k_{x,y}} \{M\}, h \rightarrow y, S_y \rightarrow k_{y,x}$
HIMMO in practice

Multiple TTP support

\[ R_i^I \quad q_i^I \]
TTP I

\[ R_i^{II} \quad q_i^{II} \]
TTP II

\[ R_i^{III} \quad q_i^{III} \]
TTP III

x (and any parameters (e.g., access roles) in it) is implicitly verified
Single TTP does not have access to communication

\[ k_{x,y} \]

\[ x, s_x \]

\[ y, s_y \]

\[ AE_{k_{x,y}} \{M\}, h \]

HIMMO in practice

HIMMO for certification of public-keys

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

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 $R_i, q_i, s_x$, 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

HIMMO

Security analysis relies on the HI and MMO problems

**HI [1]:** given arbitrarily many keys and corresponding reconciliation data, recovering the keying material of a node or the key of another pair is computationally infeasible

\[ s_{x,y} = \left\langle s_{x y^T} \right\rangle_N^{2b} \]

**MMO [2]:** given the keying materials of arbitrarily many nodes, recovering the root keying material or estimating the keying material of another node is computationally infeasible

\[ s_x = \left\langle \sum_{i=0}^{m-1} (x R_i) q_i \right\rangle_N \]


HIMMO Contest

www.himmo-scheme.com
Public verification and the HIMMO Contest

• Since 2012 we have tried to get as much public feedback as feasible talking and receiving feedback during crypto-colloquiums: Leuven, TU/e, Bochum, Darmstadt, DTU, MIT, Saarland, Paris, NIST, and many others.

• We announced the contest during NIST Workshop on PQ crypto (early 2015) – ~ 34 times downloaded

• So far HIMMO has received attention (review) not only from academia, but also several national security agencies (at least 2) and several industrial corporations have reviewed/worked on it or are reviewing/working on it now.

• Software implementation for research purposes available
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>
### Performance

- **Size of the generated key (bits)**
  - Classical: 80, Quantum: 256
- **Target security level (bits)**
  - Classical: 80, Quantum: 128
- **m (bits)**
  - Classical: 10, Quantum: 21
- **b (bits)**
  - Classical: 32, Quantum: 32
- **t**
  - Classical: 2750, Quantum: 4000
- **Number of HIMMO instances**
  - Classical: 5, Quantum: 19
- **Identity size (Bytes)**
  - Classical: 10, Quantum: 32
- **“Signature size” (Bytes)**
  - Classical: 10, Quantum: 32
- **One-way key exchange (Bytes)**
  - Classical: 20, Quantum: 75
- **One-way key exchange & entity authentication (Bytes)**
  - Classical: 30, Quantum: 107
- **PC time (ms)**
  - Classical: 0.29, Quantum: 0.68
- **NXP 120 MHz time (ms)**
  - Classical: 18.45, Quantum: 41.37
- **Required Root Hermite factor (best attack)**
  - Classical: 1.008, Quantum: 1.0056
- **Pre-processing running time for LLL (years)**
  - Classical: 75, Quantum: 639.65
Thanks!!

Q&A
Two Applications

• Integration of HIMMO into (D)TLS-PSK
  – Low communication overhead
  – Mutual authentication
  – Capabilities of digital certificates

• HIMMO as trust infrastructure for verifying public-keys
  – Public-keys are HIMMO identities
  – Implicit verification of public-keys relying on multiple TTPs
  – Does not require the exchange of certificates
