The Long and Winding Path to Secure Implementation of GlobalPlatform SCP10

Daniel De Almeida Braga
Pierre-Alain Fouque
Mohamed Sabt
CHES 2020, 14-18 September 2020
Secure Communication Protocols

- Establish a secure session between a card and an Off-Card Entity
- 2-steps protocol: Initialization + Communication
Establish a secure session between a card and an Off-Card Entity

2-steps protocol: Initialization + Communication

SCP10 relies on a Public Key Infrastructure:
- Both the card and off-card entity have a key pair
- They use each other public key to encrypt/verify messages
Our contributions:

1. Two full session key recovery attacks
   - About 0.35s for the first attack
   - On average 2h30 for the second

2. Exploit a design flaw to forge a certificate, signed by the card

3. Secure implementation, with an estimation of the overhead

\[1\text{https://github.com/ddealmei/SCP10-attack} \]
Our contributions:

1. Two full session key recovery attacks
   - About 0.35s for the first attack
   - On average 2h30 for the second

2. Exploit a design flaw to forge a certificate, signed by the card

3. Secure implementation, with an estimation of the overhead

Attacker’s position

https://github.com/ddealmei/SCP10-attack
Key Exchange Modes

Key Transport mode

- Applet Selection
- Manage Security Environment
- Certificate exchange

OCE → Card

Key Exchange Modes

- RSA with PKCS#1 v1.5
- Like padding
- Padding with 0002FF..FF00
- Known to be prone to format oracle attack
- Same key for confidentiality and authentication
Key Exchange Modes

Key Transport mode

OCE

Card

Applet Selection
Manage Security Environment
Certificate exchange
Perform Security Operation (dec)

Key Exchange Modes

RSA with PKCS#1 v1.5

- Padding with 0002FF..FF00
- Known to be prone to format oracle attack
- Same key for confidentiality and authentication
Key Exchange Modes

Key Transport mode

OCE
- Applet Selection
- Manage Security Environment
- Certificate exchange
- Perform Security Operation (dec)
- Get challenge
- External authentication

Card

• Padding with 0002FF..FF00
• Known to be prone to format oracle attack
• Same key for confidentiality and authentication
Key Exchange Modes

Key Transport mode

OCE

Card

Applet Selection

Manage Security Environment

Certificate exchange

Perform Security Operation (dec)

Get challenge

External authentication

Internal authentication

Key Exchange Modes

Card

OCE

- Internal authentication
- External authentication
- Get challenge
- Perform Security Operation (dec)
- Certificate exchange
- Manage Security Environment
- Applet Selection

Key Transport mode

RSA with PKCS#1 v1.5

- Padding with 0002FF..FF00
- Known to be prone to format oracle attack
- Same key for confidentiality and authentication
Key Exchange Modes

Key Transport mode

RSA with PKCS#1_v1.5-like padding
Key Exchange Modes

Key Transport mode

- RSA with PKCS#1v1.5-like padding
  - Padding with 0002FF..FF00
Key Exchange Modes

Key Transport mode

← RSA with PKCS#1v1.5-like padding
  • Padding with 0002FF..FF00
  • Known to be prone to format oracle attack
Key Exchange Modes

<table>
<thead>
<tr>
<th>OCE</th>
<th>Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applet Selection</td>
<td></td>
</tr>
<tr>
<td>Manage Security Environment</td>
<td></td>
</tr>
<tr>
<td>Certificate exchange</td>
<td></td>
</tr>
<tr>
<td>Perform Security Operation (dec)</td>
<td></td>
</tr>
<tr>
<td>Get challenge</td>
<td></td>
</tr>
<tr>
<td>External authentication</td>
<td></td>
</tr>
<tr>
<td>Internal authentication</td>
<td></td>
</tr>
</tbody>
</table>

Key Transport mode

← RSA with PKCS#1\textbf{1.5-like} padding

- Padding with 0002FF..FF00
- Known to be prone to format oracle attack
- Same key for confidentiality and authentication
## Secure Implementation Overhead

<table>
<thead>
<tr>
<th>Key Transport, (mutual authentication)</th>
<th>Original</th>
<th>Secure</th>
<th>Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cert. verification (card)</td>
<td>0.92</td>
<td>2.06</td>
<td>+124%</td>
</tr>
<tr>
<td>Cert. verification (OCE)</td>
<td>0.15</td>
<td>0.24</td>
<td>+60%</td>
</tr>
<tr>
<td>PSO (decipher)</td>
<td>0.15</td>
<td>0.16</td>
<td>+6%</td>
</tr>
<tr>
<td>External authentication</td>
<td>0.68</td>
<td>0.8</td>
<td>+18%</td>
</tr>
<tr>
<td>Internal authentication</td>
<td>0.73</td>
<td>0.71</td>
<td>-3%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>2.76</strong></td>
<td><strong>4.11</strong></td>
<td><strong>+49%</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key Transport, (external authentication only)</th>
<th>Original</th>
<th>Secure</th>
<th>Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cert. verification (card)</td>
<td>1.13</td>
<td>2.44</td>
<td>+116%</td>
</tr>
<tr>
<td>Cert. verification (OCE)</td>
<td>0.15</td>
<td>0.24</td>
<td>+60%</td>
</tr>
<tr>
<td>PSO (decipher)</td>
<td>0.15</td>
<td>0.16</td>
<td>+6%</td>
</tr>
<tr>
<td>External authentication</td>
<td>0.72</td>
<td>0.82</td>
<td>+14%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>2.31</strong></td>
<td><strong>3.81</strong></td>
<td><strong>+65%</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key Agreement</th>
<th>Original</th>
<th>Secure</th>
<th>Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cert. verification (card)</td>
<td>1.18</td>
<td>2.12</td>
<td>+80%</td>
</tr>
<tr>
<td>Cert. verification (OCE)</td>
<td>0.15</td>
<td>0.24</td>
<td>+60%</td>
</tr>
<tr>
<td>PSO (decipher)</td>
<td>0.15</td>
<td>0.16</td>
<td>+6%</td>
</tr>
<tr>
<td>External authentication</td>
<td>1.61</td>
<td>1.43</td>
<td>-11%</td>
</tr>
<tr>
<td>Internal authentication</td>
<td>0.85</td>
<td>0.80</td>
<td>-6%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>4.09</strong></td>
<td><strong>4.90</strong></td>
<td><strong>+20%</strong></td>
</tr>
</tbody>
</table>
## Secure Implementation Overhead

<table>
<thead>
<tr>
<th>Category</th>
<th>Original</th>
<th>Secure</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Transport (mutual authentication)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSO (decipher)</td>
<td>0.15</td>
<td>0.16</td>
<td>+6%</td>
</tr>
<tr>
<td>External authentication</td>
<td>0.68</td>
<td>0.8</td>
<td>+18%</td>
</tr>
<tr>
<td>Internal authentication</td>
<td>0.73</td>
<td>0.71</td>
<td>-3%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>1.56</td>
<td>1.67</td>
<td>+7%</td>
</tr>
<tr>
<td><strong>Key Transport (external authentication only)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSO (decipher)</td>
<td>0.15</td>
<td>0.16</td>
<td>+6%</td>
</tr>
<tr>
<td>External authentication</td>
<td>0.72</td>
<td>0.82</td>
<td>+14%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>0.87</td>
<td>0.98</td>
<td>+13%</td>
</tr>
<tr>
<td><strong>Key Agreement</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSO (decipher)</td>
<td>0.15</td>
<td>0.16</td>
<td>+6%</td>
</tr>
<tr>
<td>External authentication</td>
<td>1.61</td>
<td>1.43</td>
<td>-11%</td>
</tr>
<tr>
<td>Internal authentication</td>
<td>0.85</td>
<td>0.80</td>
<td>-6%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>2.61</td>
<td>2.39</td>
<td>-10%</td>
</tr>
</tbody>
</table>
Sum-up

- We tried to apply well known attack to the smart cards world
- Successfully performed two attacks speculating on the implementation
  - We believe our assumption to be reasonable giving past attacks
  - Lack of key isolation is not implementation dependent
- Suggest mitigations:
  - Easy to add in the specification
  - Reasonable overhead
- GlobalPlatform released an amendment based on our recommendations (work in progress)
Thank you for your attention!

https://github.com/ddealmei/SCP10-attack