Netzwerke und Sicherheit auf mobilen Geräten

Univ.-Prof. Priv.-Doz. DI Dr. René Mayrhofer
Antrittsvorlesung
Johannes Kepler Universität Linz
Repräsentationsräume 1. Stock (Uni-Center)
19.1.2015, 16:00
Mobile devices proliferate
Problems

- Wireless communication
- No (capable) user interfaces
- Scalability of user attention

- cryptography
- no passwords
- unobtrusive, intuitive
One approach for D2D authentication: Shaking
Accelerometer data

Data analysis

Split acceleration into n overlapping slices

Coherence per pair of slices

Average over coherences

### Protocol

<table>
<thead>
<tr>
<th>A</th>
<th>Message</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Choose DH key</strong></td>
<td></td>
</tr>
<tr>
<td>$x \in {1 \ldots q - 1}$</td>
<td>$X := g^x$</td>
<td>$y \in {1 \ldots q - 1}$</td>
</tr>
<tr>
<td>$K_a^{Sess} := H(Y^x)$</td>
<td></td>
<td>$K_b^{Sess} := H(X^y)$</td>
</tr>
<tr>
<td>$K_a^{Auth} := H(Y^x</td>
<td>C)$</td>
<td>$Y := g^y$</td>
</tr>
</tbody>
</table>

| | **Split and encrypt signal** | |
| | $A_1 = c_0[0 : 63] \ldots | c_n[0 : 63]$ | $B_1 = d_0[0 : 63] \ldots | d_m[0 : 63]$ |
| $(i = 0 : n - 1, \quad j = 1 : n)$: | | $(i = 0 : m - 1, \quad j = 1 : m)$: |
| $a_i := a[128i : 128i + 127]$ | | $b_i := b[128i : 128i + 127]$ |
| $c_0 \in \{0, ..., 2^{128} - 1\}$ | $B_i := d_i[0 : 63] \ldots | d_m[0 : 63]$ | $d_0 \in \{0, ..., 2^{128} - 1\}$ |
| $c_j := E(K_a^{Auth}, c_{j-1} \oplus a_{j-1})$ | | $d_j := E(K_b^{Auth}, d_{j-1} \oplus b_{j-1})$ |

| | **Interlock and reassemble** | |
| | $A_2 = c_0[64 : 127] \ldots | c_n[64 : 127]$ | $B_2 = d_0[64 : 127] \ldots | d_n[64 : 127]$ |
| $(i = 0 : m - 1)$: | | $(i = 0 : n - 1)$: |
| $\tilde{a}_i := \tilde{B}_1[128i : 128i + 63]$ | $\tilde{c}_i := \tilde{A}_1[128i : 128i + 63]$ | $\tilde{A}_2[128i : 128i + 63]$ |
| $\tilde{B}_2[128i : 128i + 63]$ | $\tilde{B}_2[128i : 128i + 63]$ | $\tilde{a}_i := D(K_b^{Auth}, \tilde{c}_{i+1} \oplus \tilde{c}_i)$ |
| $\tilde{b}_i := D(K_a^{Auth}, \tilde{a}_{i+1} \oplus \tilde{a}_i)$ | $\tilde{b} := \tilde{b}_0| \ldots | \tilde{b}_m$ | $\tilde{a} := \tilde{a}_0| \ldots | \tilde{a}_n$ |

| | **Compare** | |
| if $a \sim \tilde{b}$ | if $b \sim \tilde{a}$ |
| then $K := K_a^{Sess}$ | then $K := K_b^{Sess}$ |
| else $K := null$ | else $K := null$ |

---


Netzwerke und Sicherheit auf mobilen Geräten – Univ.-Prof. René Mayrhofer
Results: Security vs. usability

Mobile devices and users
Problems

http://www.telemed.no/new-opportunities-present-new-challenges.552290-80451.html
Mobile devices and users
Biometric authentication: 3D Face


Mobile devices and users
Biometric authentication:
Iris
Biometric authentication: Gait


http://www.homelandsecuritynewswire.com/gait-biometrics-shows-promise
Data analysis

Walk separation

Data analysis

Cycle length estimation

Data analysis

Walk cycle comparison

Results

Gait is not enough for high security

- 7.05% equal error rate on same day
- 18.97% equal error rate when trained on one day and tested on another → research still ongoing

Will require library of biometric methods

Mobile devices and users
Open security problem: Secure user interaction

Networks and Security

Security
- Hardware
- Virtualisation
- Reliable code

Privacy

Networks
- High latency
- Self healing
- Wireless
- Ad-hoc
- P2P

Cryptography

VPN

Authentication
Mobile communication
Communication protocol layers

Communication protocol layers diagram:

- **Web browser**
- **Internet protocols (TCP, IP)**
  - **IEEE 802.11**
  - **UMTS /GSM**
  - **Ethernet**
- **Web server**
- **Internet protocols (TCP, IP)**
  - **Ethernet**
Communication protocol layers

- Web browser
- Internet protocols (TCP, IP)
  - IEEE 802.11
  - UMTS /GSM
- Web server
- Internet protocols (TCP, IP)
- Ethernet

https://www.ins.jku.at
Communication protocol layers

- Web browser
- Internet protocols (TCP, IP)
- IEEE 802.11
- UMTS /GSM
- Web server
- Internet protocols (TCP, IP)
- Ethernet

- PRISM

https://www.ins.jku.at
Encryption layer

Internet protocols (TCP, IP)

TLS / HTTPS

Web browser

Web server

TLS / HTTPS

Internet protocols (TCP, IP)

IEEE 802.11

UMTS / GSM

Ethernet
Problem: re-connect
Problem: re-connect

Internet protocols (TCP, IP)

Web browser

Web server

TLS / HTTPS

IEEE 802.11

UMTS /GSM

Ethernet

Internet protocols (TCP, IP)

TLS / HTTPS

https://www.ins.jku.at
Next steps: long-range communication latency

https://www.flickr.com/photos/58068110@N00/394840906/
Future: How far can the (secure) Internet go?