The Use of Smartphone in the Chain of Security
When all Becomes Electronically ---except the User

Who
Berne University of Applied Sciences (BFH)
Research Institute for Security In the Information Society (RISIS)
E-Voting Group
Eric Dubuis, Rolf Haenni, Reto E. Koenig
IoT Group
Andreas Danuser, Franz Meyer, Reto E. Koenig

Why
Experts In Remote Voting Over the Internet (E-Voting)
Demonstration of Vulnerabilities in E-Voting System (2013)
Demonstration of Vulnerability in E-Banking Solution (2014)

Quest
Stop using Smartphones as Part of the Security Chain
Start using Secure Hardware Tokens Instead

What is It All About?

<Diagram: Transaction Substitution Exploit On a Current Secure E-Banking Solution>

History of E-Banking and Security: From Past to Future

<Diagram: Introduction of Smartphone Into the Chain of Security>

Introduction of a Dedicated Secure Hardware Token* Into the Chain of Security

* Provided by FIDO Alliance

How to Infect General Purpose Device*

<Diagram: An Infected Browser is All It Needs>

How Infected Devices Communicate

<Diagram: There is no Air Gap>
The Use of Smartphone in the Chain of Security
When all Becomes Electronically ---except the User

Who  Berne University of Applied Sciences (BFH)
      Research Institute for Security in the Information Society (RISIS)
      E-Voting Group
      Eric Dubuis, Rolf Haenni, Reto E. Koenig
      IoT Group
      Andreas Danuser, Franz Meyer, Reto E. Koenig

Why  Experts in Remote Voting Over the Internet (E-Voting)
      Demonstration of Vulnerabilities in E-Voting System (2013)
      Demonstration of Vulnerability in E-Banking Solution (2014)

Quest  Stop using Smartphones as Part of the Security Chain
        Start using Secure Hardware Tokens instead
What is It All About?

"This client option provides a secure cost-effective mobile tool for strong transaction authentication anywhere, anytime, without the need of an extra device."

Demo Transaction Substitution Exploit On a Current Secure E-Banking Solution
History of E-Banking and Security: From Past to Future

Introduction of Smartphone Into the Chain of Security

Introduction of a Dedicated Secure Hardware Token* Into the Chain of Security

* Provided by Trustworthy Site
  Secure Channel to Trusted Site
  Non Reprogrammable
  Secure Keyboard
  Secure Display
# Personal contact with trust-institute

<table>
<thead>
<tr>
<th>Objective</th>
<th>Subjective</th>
<th>Security</th>
<th>Subjective</th>
<th>Privacy</th>
<th>Subjective</th>
<th>Attack Price</th>
<th>Subjective</th>
<th>Privacy</th>
<th>Subjective</th>
<th>Attack Price</th>
<th>Subjective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Objective</td>
<td>Subjective</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Usability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Objective</td>
<td>Subjective</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>Hidden Session</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack Price</td>
<td>Hidden Transaction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transaction Substitution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Dedicated software or browser
No Threat
<table>
<thead>
<tr>
<th>Usability</th>
<th>Objective</th>
<th>Subjective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Objective</td>
<td>Subjective</td>
</tr>
<tr>
<td>Privacy</td>
<td>Hidden Session</td>
<td>Hidden Transaction</td>
</tr>
</tbody>
</table>

Dedicated software or browser
Threat unbeknownst by parties
Session initiation by One-Time-Password list
<table>
<thead>
<tr>
<th>Usability</th>
<th>Objective</th>
<th>Subjective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Objective</td>
<td>Subjective</td>
</tr>
<tr>
<td>Privacy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack Price</td>
<td>Hidden Session</td>
<td>Hidden Transaction</td>
</tr>
</tbody>
</table>

Session initiation by One-Time-Password list
Transaction authentication via SMS on mobile phone
<table>
<thead>
<tr>
<th>Feature</th>
<th>Objective</th>
<th>Subjective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack Price</td>
<td>Hidden Session</td>
<td>Transaction Substitution</td>
</tr>
<tr>
<td>Price</td>
<td>Hidden Transaction</td>
<td></td>
</tr>
</tbody>
</table>

Session initiation & transaction authentication via SMS on mobile phone
Introduction of Smartphone Into the Chain of Security
Session Initiation & Transaction authentication via SMS on smart-phone
Dedicated software or browser
Threat unbeknownst by parties

Session initiation by One-Time-Password list

Session Initiation & Transaction authentication via SMS on smart-phone
Dedicated App for Session Initiation & Transaction authentication
Dedicated App for Session Initiation & Transaction authentication Alternative: via SMS on smart-phone
Introduction of a Dedicated Secure Hardware Token
Into the Chain of Security

* Provided by Trustworthy Site
  Secure Channel to Trusted Site
  Non Reprogrammable
  Secure Keyboard
  Secure Display
Dedicated secure hardware from trust-institute for
Session Initiation & Transaction authentication
Secure Hardware Token

* Provided by Trustworthy Site
* Secure Channel to Trusted Site
* Non Reprogrammable
* Secure Keyboard
* Secure Display
How to Infect *General Purpose Device*

* Uncontrolled Provider
  Connected to the Internet
  Freely Reprogrammable

An Infected Browser is All It Needs

1. User is seduced to install a shady software.
2. Infected Browser is enough to do the rest without the need of a user.
3. Infected Browserfects nearby devices via the Cloud (e.g., Phone/Apple iOS)
General Purpose Device*

* Uncontrolled Provider
  Connected to the Internet
  Freely Reprogrammable

An Infected Browser is All It Needs

1. User is seduced to install a faulty software.
2. Infected Browser is enough to do the rest without the need of a user.
3. Infected Browser infects remaining devices via the Cloud (e.g. Playstore, Appstore)
User is seduced to install a faulty software.
Infected Browser infects remaining devices via the Cloud (e.g. Playstore, Appstore)
How Infected Devices Communicate

There is no Air Gap
There is no Air Gap

Cloud
Internet
Wireless LAN
Bluetooth

Suppressed SMS
Ultra-Sound
...

Live Demo