Mit dem Handy das Auto aufschliessen? Hardware Protected Confirmation macht es möglich
Prof. Dr. Benjamin Fehrensen, Institute for Cybersecurity and Engineering ICE, BFH-TI
Class 4 Reader

- Keys generated on Hardware, non-extractable
- Keys are protected against cloning

Class 1 Reader

- PIN entry on dedicated HW
- Credentials cannot easily be sniffed

Class 2 Reader

- Trusted User Interface
- Prevents overlay attacks

Class 3 Reader

- Device attestation
- The integrity of the device / environment can be verified.
Remote Control Device

- Automate user input via Accessibility
- Attacker can sniff user input such as clicks, text input, voice input etc.
- Attacker can automate user input:
  - Auto-confirm granting privileges
  - Auto-confirm approving payments
  - Entering fraudulent payments
  - Prevent removing privileges
  - Prevent removing malware

EventBot Sample
Our Vision: Global «Protected Confirmation» API

Joint InnoSuisse Project: University of Applied Science Bern & UBS Business Solutions AG

Practical Business Use Cases
Payments, Signing, Voting, Remote Control, …
Our Goals

Put end users back into sole control

- Put end users back into **sole control** over their mobile-device
  - Leverage TUI for protected confirmation
  - Leverage TEE signatures for legally-binding evidence
  - Consider biometrics for stronger user binding

- Liaise with int’ card schemes, int’ banking regulators to strengthen the **demand** for a global protected confirmation API
  - Implement compelling payment business cases (3DS payment confirmation, PSD2 authentication with linking, …)
  - Motivate OEMs to implement the API **optional** standard set by Android
Our Implementation Security Architecture

Trusted Execution Environment – Prerequisites at our fingertips

- Separation between 2 security domains
- Device attestation
- Hardware backed key on Hardware Storage Module (HSM) FIPS 140-3 (Level 3+) certified
- Trusted UI

Implementation Standard

Trusted User Interface

- Click twice to confirm

Android Protected Confirmation

- Transaction details displayed on a Trusted User Interface (TUI)
- Physical presence enforced via power button
- Protected confirmation evidenced through a TEE electronic signature
- Security context & device integrity proven by TEE key attestation
- Enhancement with device biometrics enforced via TEE
Attestation - Also Used By OEM Checks

The integrity of the environment is certified by attestation.

«Attested APC key pair»: Can only be used for the attested purpose. Provides comprehensive information about the environment and the possible use of the key-pair.

One or multiple intermediate device key(s) identifying the keystore such as «StrongBox», «TEE», etc.

Attestation root key (Trust Anchor) injected into the hardware-backed keystore by the device manufacturer.
## Attestation Attributes

<table>
<thead>
<tr>
<th>Root Of Trust</th>
<th>TEE Enforced Authorization</th>
<th>Attestation Application</th>
<th>Global Attestation Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Locked</td>
<td>Purpose(s)</td>
<td>Package Infos</td>
<td>KeyStore</td>
</tr>
<tr>
<td>Verified Boot State</td>
<td>User Auth Type</td>
<td>Signature Digests</td>
<td>Attestation Challenge</td>
</tr>
<tr>
<td>OS Version</td>
<td>Trusted Confirmation Required</td>
<td>Attestation Application ID Bytes</td>
<td>Attestation Version</td>
</tr>
<tr>
<td>OS Patch Level</td>
<td>Trusted User Presence Required</td>
<td>Attestation ID Brand</td>
<td>Keymaster Version</td>
</tr>
<tr>
<td>Boot Patch Level</td>
<td>Unlocked Device Required</td>
<td>Attestation ID Device</td>
<td>Unique ID</td>
</tr>
<tr>
<td>Brand</td>
<td>Rollback Resistance</td>
<td>Attestation ID Product</td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>Creation DateTime</td>
<td>Attestation ID Serial</td>
<td></td>
</tr>
<tr>
<td>Product</td>
<td>Algorithm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial Number</td>
<td>Digest(s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMEI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manufacturer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APC Demo App – Try it


Android Protected Confirmation (APC) is basically a Class-4-Reader. The message is displayed on a Trusted User Interface. The confirmation and authentication take place on a Trusted Execution Environment (TEE). The keys are generated and stored on hardware. The state of the trusted environment is certified by attestation. I.e. APC meets security requirements that are set for POS (Point Of Sales) terminals.

Try it.

Motivation

https://apc.ti.bfh.ch/

Bern University of Applied Sciences / APC Project / APC - Get started

Android Protected Confirmation: Confirm and sign messages displayed on a Trusted User Interface

Put end users back into sole control over their mobile-device.
Project Lead

UBS

Dr. Alain Hiltgen
Executive Director
Head Business Security Advice
UBS Business Solutions AG

alain.hiltgen@ubs.com
www.ubs.com

BFH

Prof. Dr. Benjamin Fehrensen
Department TI
ICE
University of Applied Science Bern

benjamin.fehrensen@bfh.ch
www.bfh.ch
Nächste Seminare

Biel / Bienne
Quellgasse 21, Aula

6.4.2023 | Von der Laborbank zum Patienten – Erste klinische Resultate zur selektiven Netzhauttherapie Christian Burri, Institute for Human Centered Engineering HuCE, BFH-TI

13.4.2023 | Intégration d’un ensemble complet de logiciels pour la conduite autonome Ahmed Hanachi, Institut pour la recherche sur l’énergie et la mobilité IEM, BFH-TI

27.4.2023 | Die digitale Transformation des Exportgeschäfts Prof. Dr. Paul Ammann, Institute for Data Applications and Security IDAS, BFH-TI

11.5.2023 | The Relevance and Hands-on Application of Biomedical Record Linkage in the Big Data Era Prof. Dr. Murat Sariyar, Institute for Medical Informatics I4MI, BFH-TI

1.6.2023 | Averaging Model for Feedback Control of Ultrasonic Transducers Diego Stutzer, Institute for Human Centered Engineering HuCE, BFH-TI

Burgdorf / Berthoud
Pestalozzistrasse 20, E013

20.4.2023 | How Data Analysis Can Help to Better Understand the Degradation in PV Modules Prof. Dr. Jasmin Wandel, Institute for Optimisation and Data Analysis IODA, BFH-TI and Sara El Hassani, Institute for Energy and Mobility Research IEM, BFH-TI

4.5.2023 | TPV 5000 – Beitrag zur Defossilisierung des Verkehrs Dr. Albrecht Tribukait, CEO ad int., Silent-Power AG

25.5.2023 am Jcogew 1 | What is High Voltage Engineering about? Prof. Dr. Roman Grinberg, Institute for Energy and Mobility Research IEM, BFH-TI

8.6.2023 | Waghalsige Holzkonstruktionen unter Anwendung moderner Technologie neu denken Matias Penroz, Institut für digitale Bau- und Holzwirtschaft IdBH, BFH-AHB