The Vital Role of Protected Confirmation

Approve Payments Through Dynamic Linking

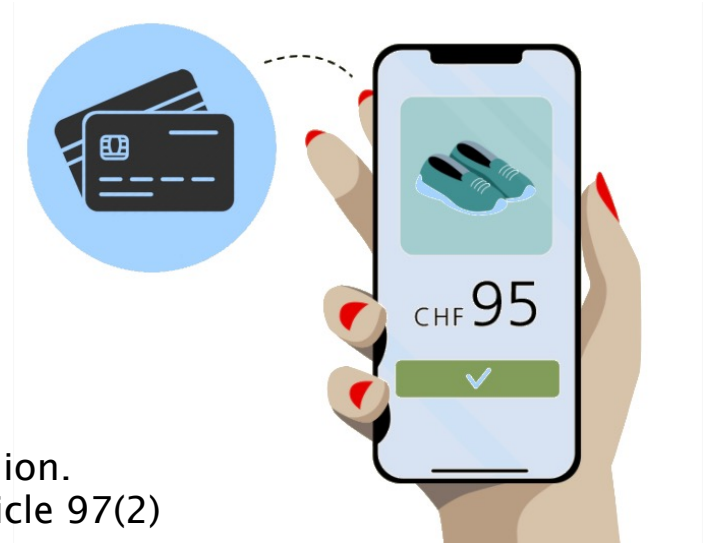
- Department TI, Institute for Cybersecurity and Engineering ICE

Protected Confirmation - Dynamic Linking

- EU Directive „Revised Payment Services Directive" (PSD2)[*] mandates that:

  payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.

- EMV Security Standard
- PCI SSC

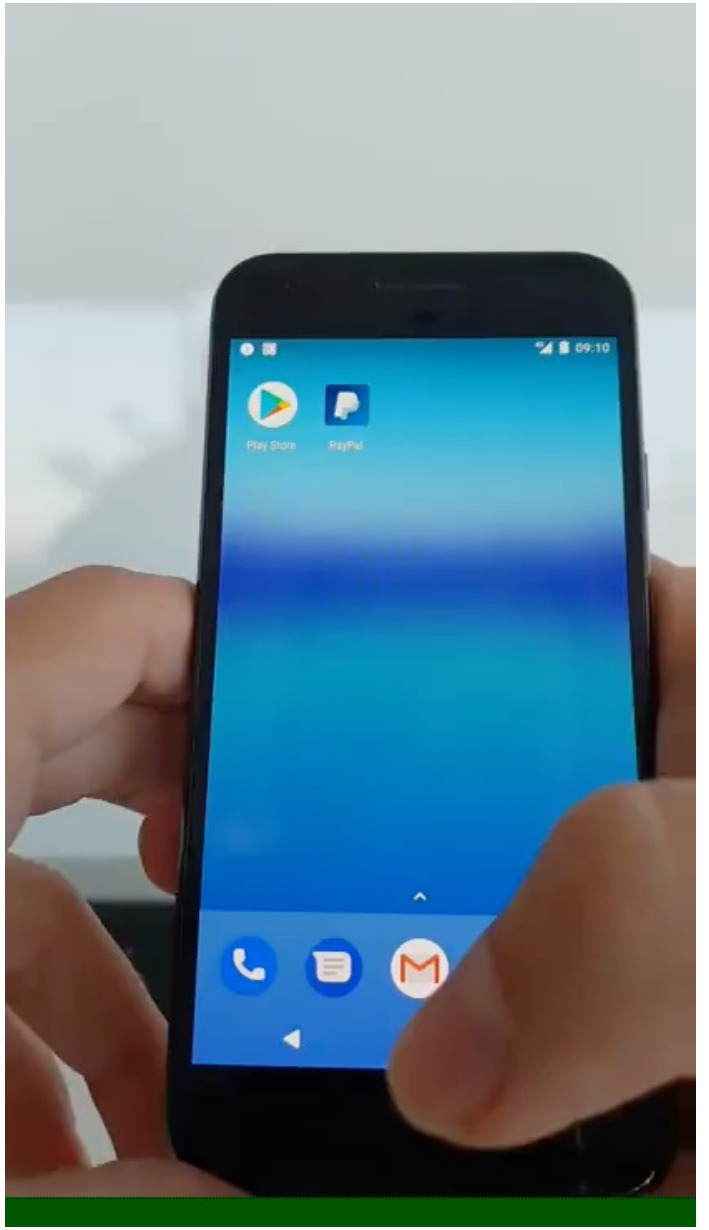


[*] The European Parliament and Regulation (EU) the Council of the European Union. Directive (eu) 2015/2366 on payment services in the internal market, 2015, Article 97(2)

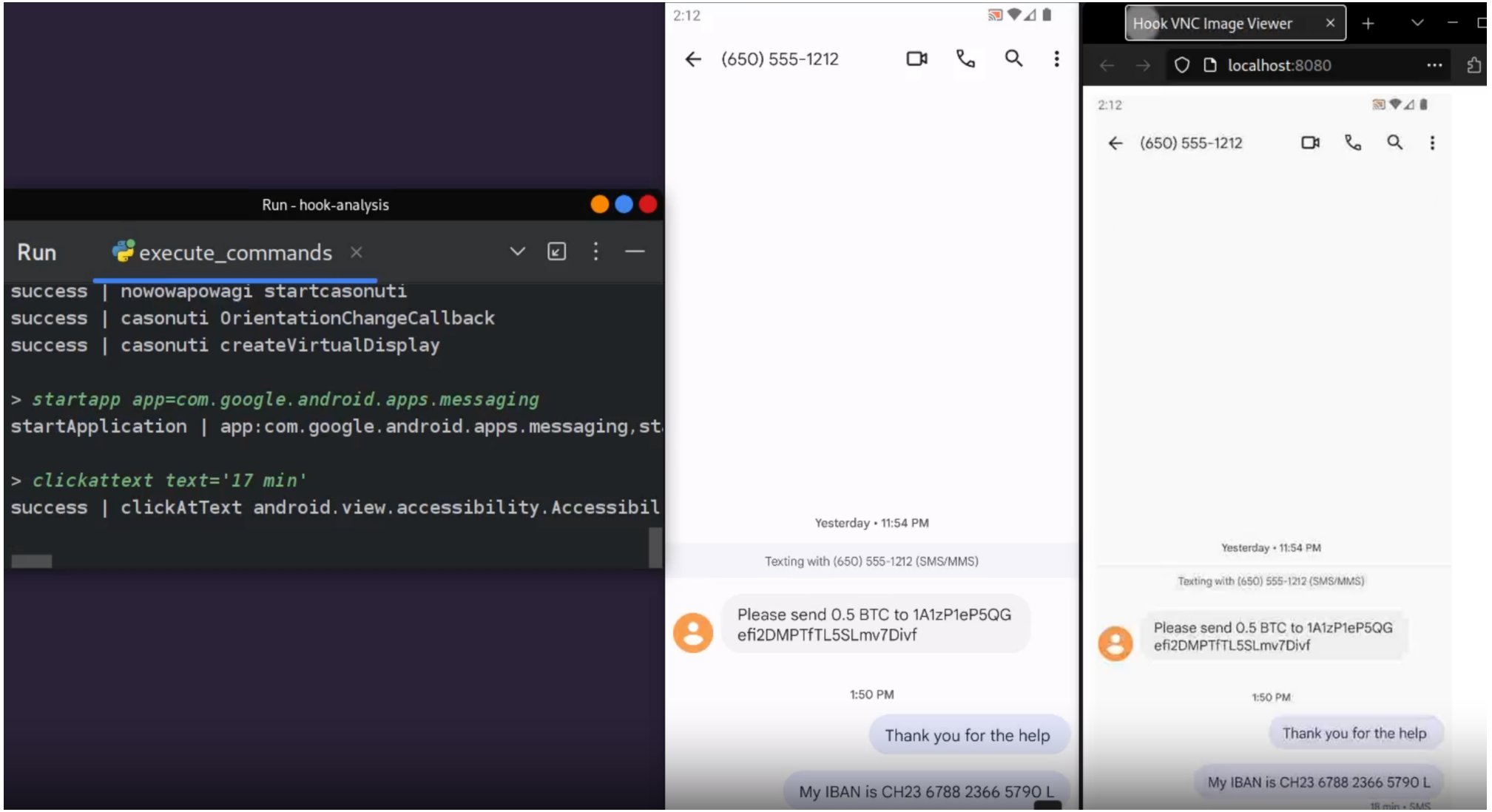
Banking Trojan: Remote Control Device

Automate Any User Interaction with ACCESSIBILITY

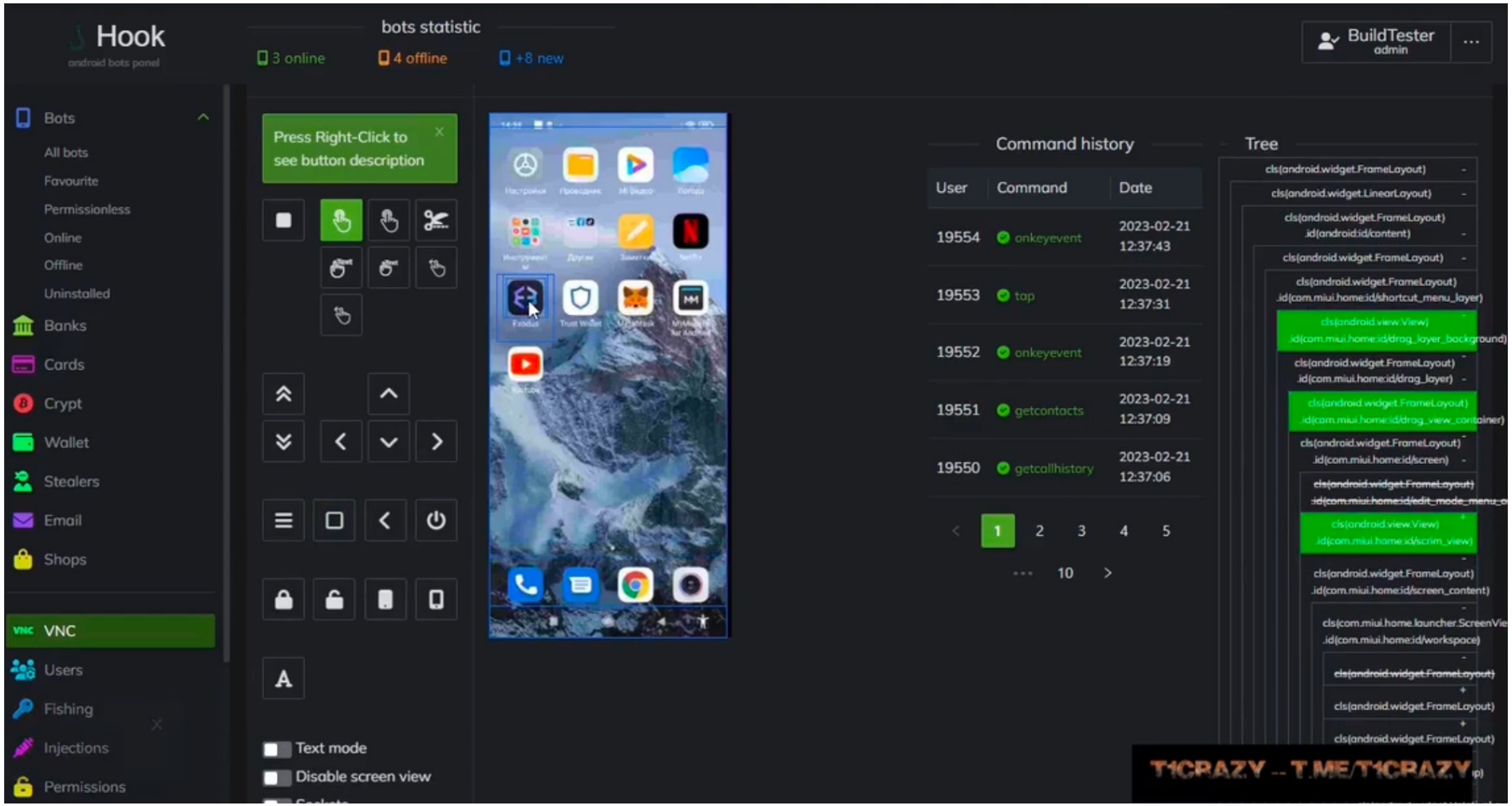
- Automate user input via Accessibility
- Attacker can sniff user input such as PINs, clicks, text input, voice input etc.
- Attacker can automate user input:
  - Auto-confirm granting privileges
  - Auto-confirm approving payments
  - Entering fraudulent payments
  - Prevent removing privileges
  -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



ACCESSIBILITY: Remote Control Device

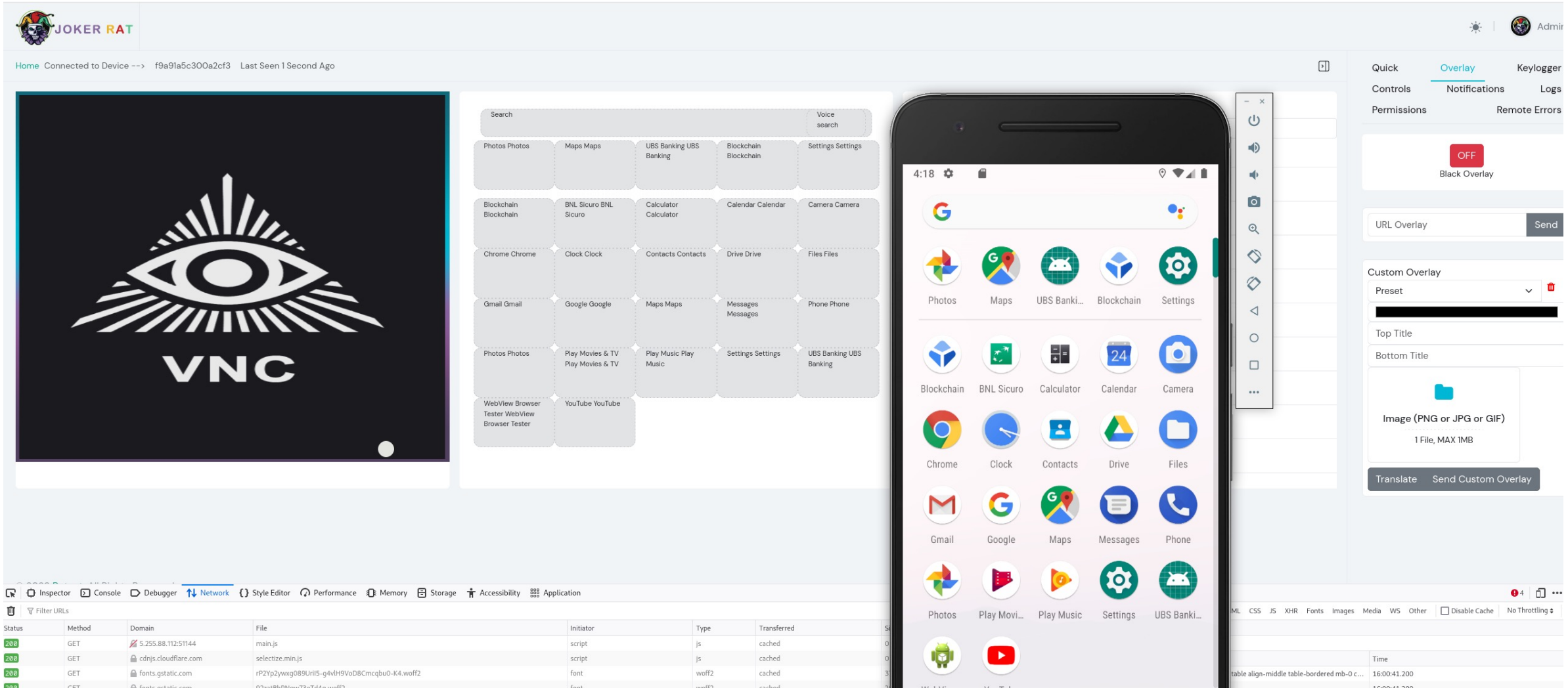


Hook VNC



- Convenient remote control via C2
- Similar to TeamViewer
- Any User Interaction can be logged
- Any Interaction can be invoked.

Copybara – Remote Control Hidden Under Overlay



Copybara – Typical Attack

- Lock Screen
- Login to Bank App
- Enter Payment
- Remove Banking App
- Cleanup

```
16:23:54↓  Command: Send_LockScreen_Overlay_CO Installazione in corso Attendere prego 1711548724
    051.png rgba(248, 247, 247, 1)
16:23:55↓  Command: Send_DeviceScreenShot_Permission
16:23:56↑  Notification: com.bnlsicuroappbnlapp.apkapp ->
16:23:59↓  Command: Send_Swipe_Action_ACS <pattern>
```

```
16:27:02↓  Command: clickbyid it.bnl.apps.banking:id/btn_eir_registrati Accedi con PIN
16:27:23↑  KeyLog: [] -pkg : it.bnl.apps.banking
16:27:35↓  Command: clickbyid None 0052093302
```

```
16:31:03↑  KeyLog: [IT79H                                                    072] -pkg : it.bnl.apps.banking
16:31:21↓  Command: Send_Text_FromPCToAndroidDevice IT79H
16:31:26↓  Command: Send_Swipe_Action_ACS <pattern>
16:31:34↓  Command: clickbyid it.bnl.apps.banking:id/et_state_money_item Importo
16:31:38↓  Command: Send_Text_FromPCToAndroidDevice 9800
16:31:40↓  Command: clickbyid None Prosegui
```

```
16:34:20↓  Command:      Send_Uninstall_CertainApp it.bnl.apps.tol.bnl
16:34:24↓  Command:      clickbyid android:id/button1 OK
16:34:25↓  Command:      Send_Swipe_Action_ACS <pattern>
16:34:26↑  Notification: com.google.android.packageinstaller ->  Disinstallazione di BNL
    …Trading
16:34:29↑  PhoneCalling: OFFHOOK
```

```
16:48:07↑  PhoneCalling: OFFHOOK 3475######
16:50:15↑  PhoneCalling: IDLE 3475######
16:50:22↓  Command:      FormatthisDevice
```

Mitigate Banking Trojan Attacks

- Hardware backed keys
- Strong 2 Factor Authentication 2FA
- Biometrics
- App Protection against Remote Control
- Protected Confirmation

Class 4 Reader – Evolution Of Strong Authentication

Class 1 Reader

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

Class 2 Reader

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

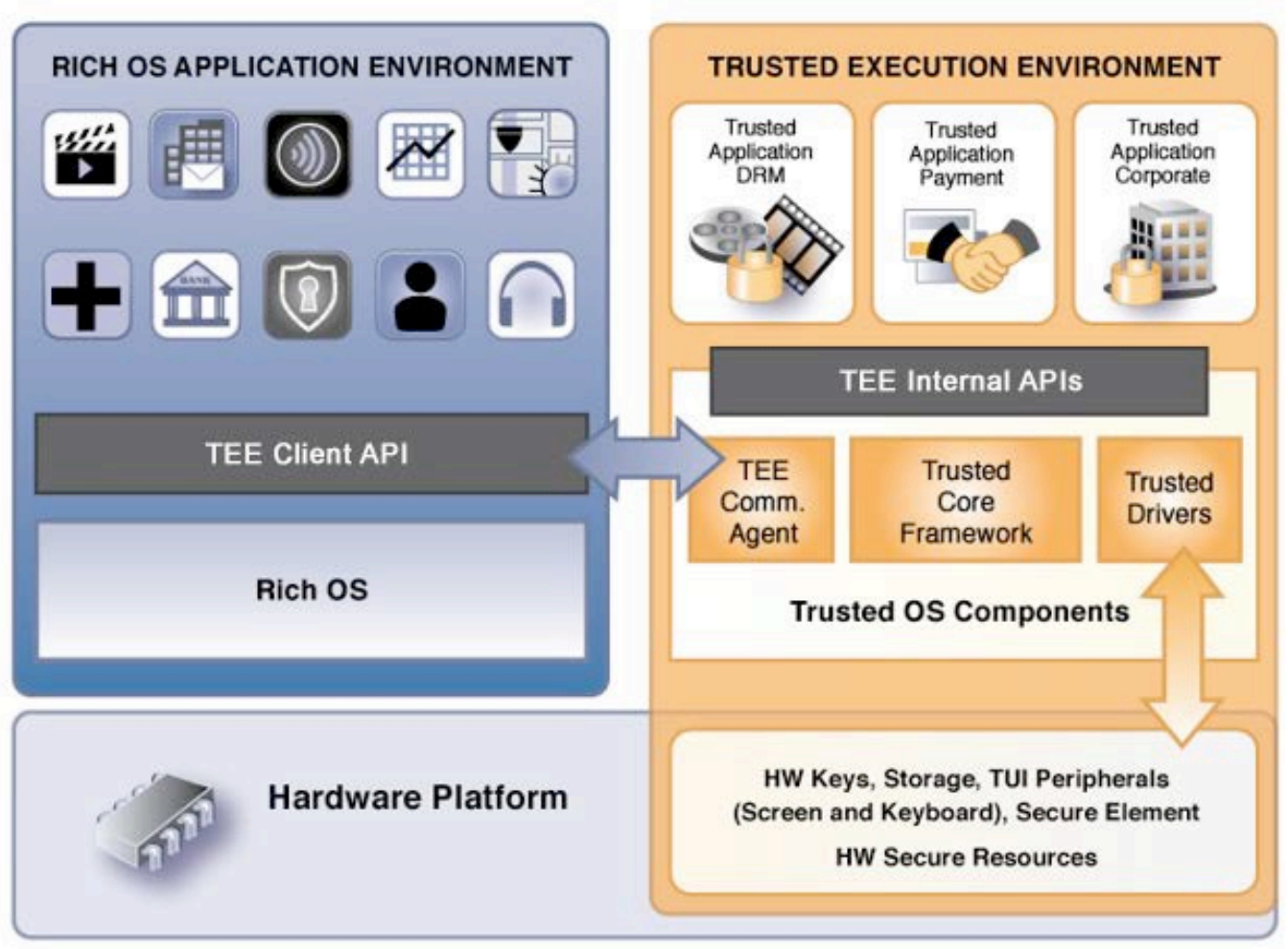
Class 3 Reader

- Trusted User Interface
- Prevents overlay attacks

Class 4 Reader

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

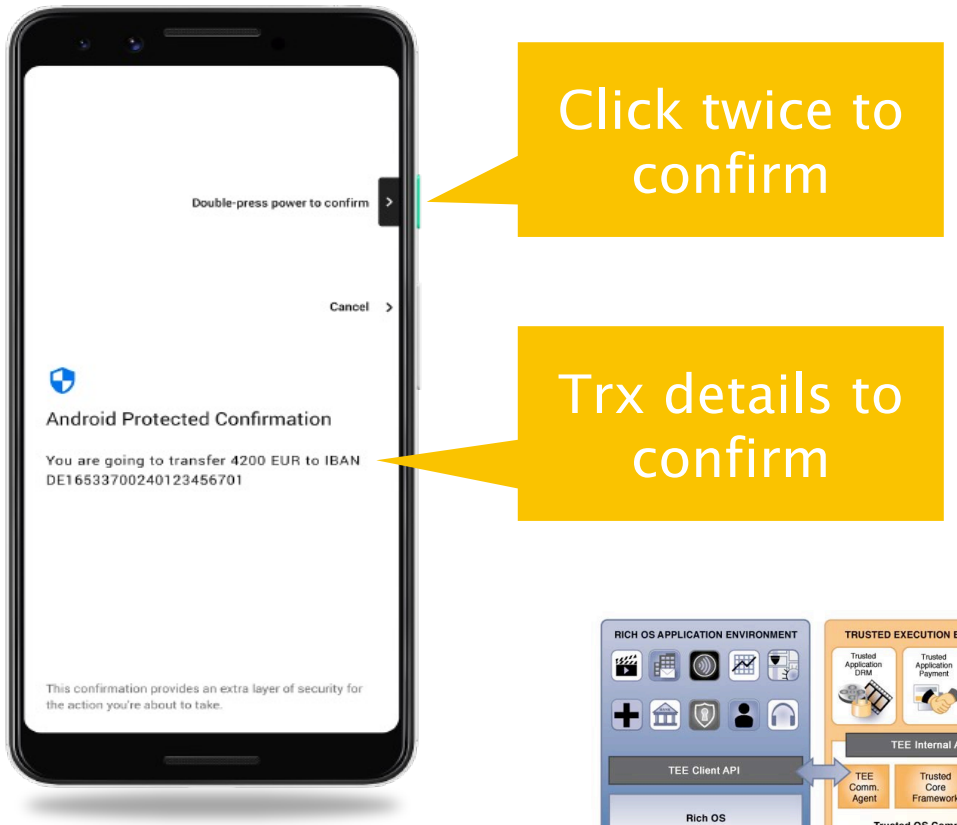
Target Security Architecture

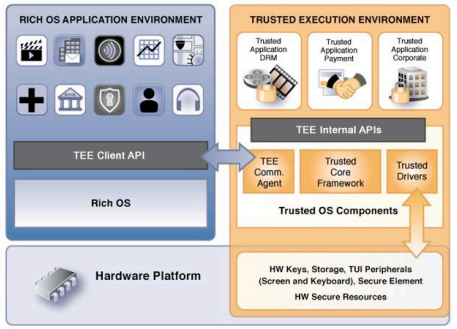


- Separation between 2 security domains
- Device attestation
- Hardware backed key on Hardware Storage Module (HSM) FIPS 140-3 (Level 3+) ,EAL4+ certified
- **Trusted UI**

Source: GlobalPlatform, The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market, February 2011.

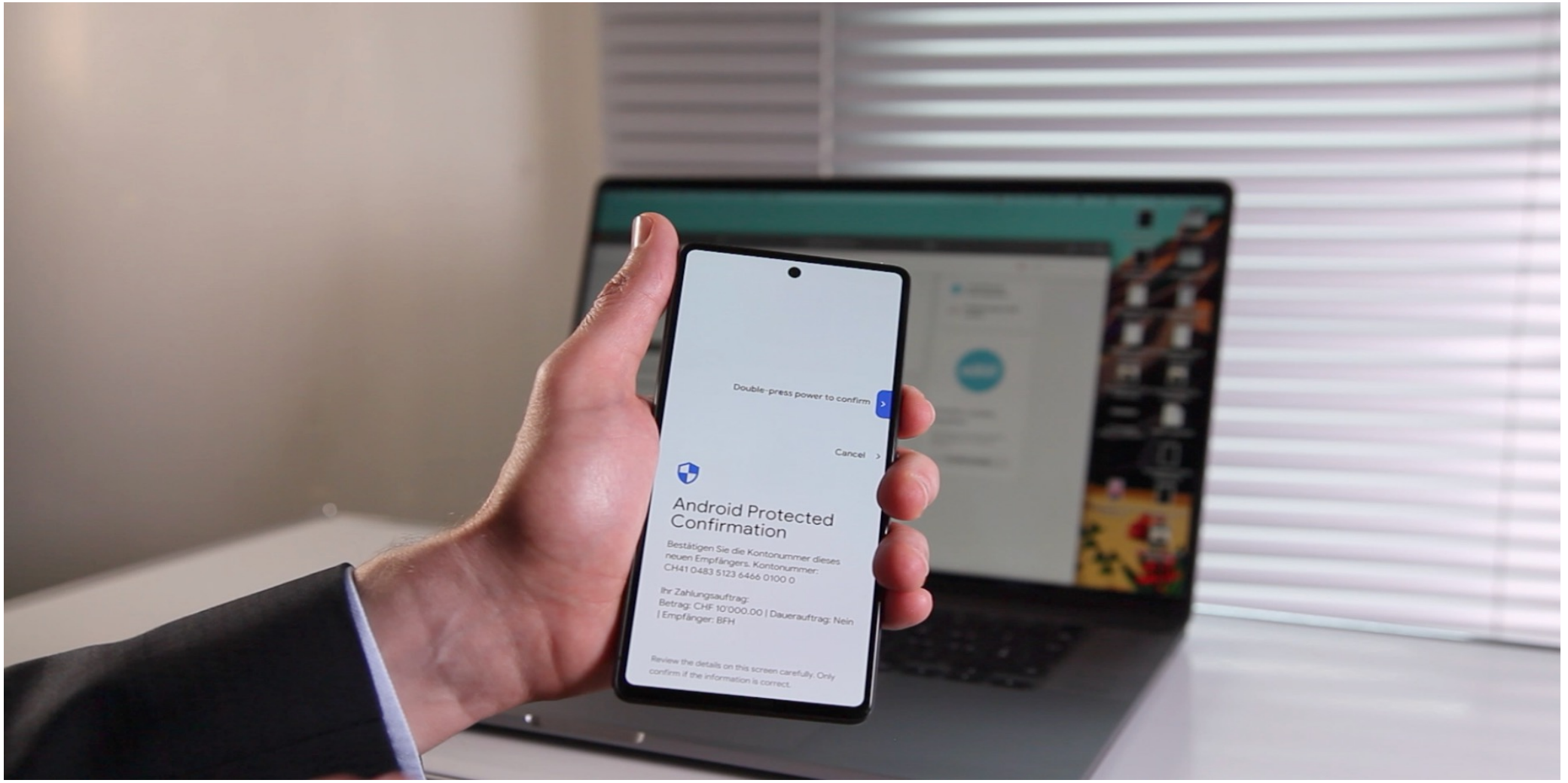
Android Protected Confirmation (APC)





- Confirmation data submitted from an app in the blue OS to APC running in the orange OS (TEE)
- Transaction details displayed by APC via Trusted User Interface (TUI), leveraging own drivers
- Physical user response collected by APC via TUI, directly connected power button or biometrics
- APC usage evidenced to the bank through a TEE-issued digital signature over the confirmation data
- Signed confirmation returned from APC in the orange OS to the app in the blue OS (REE)

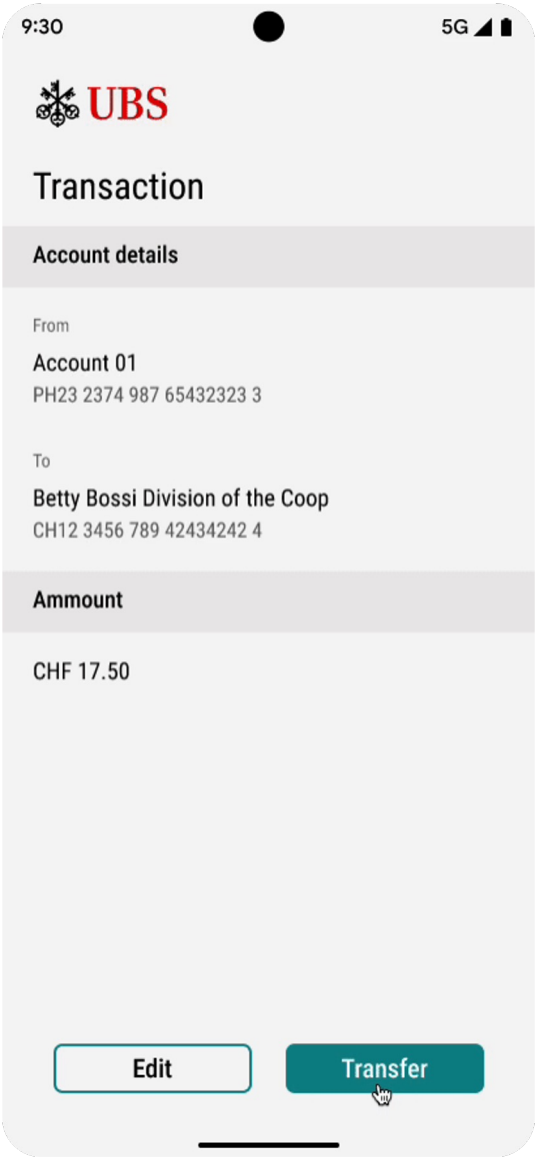
Science Fiction Or Reality – USB Pilot



https://www.ubs.com/ch/en/private/digital-banking/private/apc-pilot.html

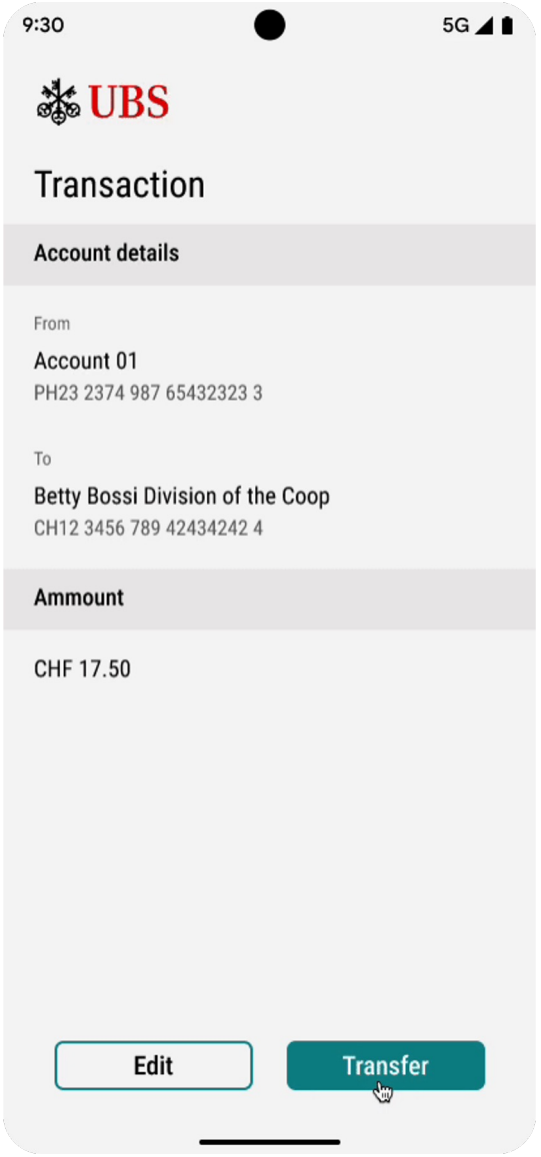
FIDO - Technology-Neutral International Standard

- In order to make "Protected Confirmation" widely accessible, the technology must be standardized in a technology-neutral, internationally accepted specification.
- FIDO is a broadly accepted international standard implemented by all major Software companies.



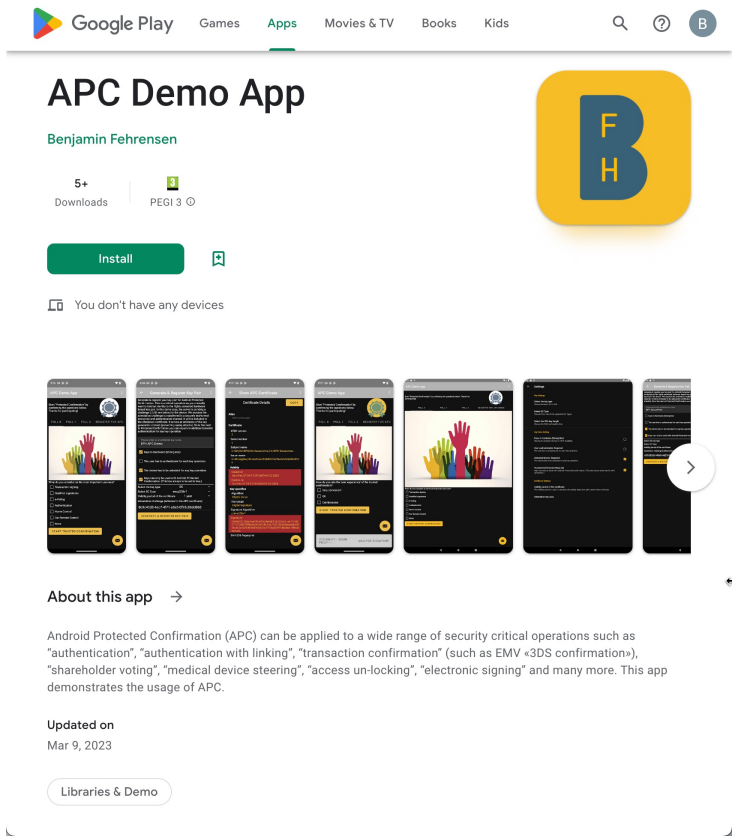
Thank you!

Questions?



APC Demo App – Try it

https://play.google.com/store/apps/details?id=ch.bfh.securevote



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