CARTES BANCAIRES CB

TEE Summit Europe 2017
2017-11-16

Cartes Bancaires is the most widely used card scheme (& payment method) **in France**

95% of domestic transactions

11 Bn card transactions in **2016**
for **€570 Bn total ***

2nd largest card scheme in Europe

* **+ 6% compared to 2015 /** Represents 40 % of total French household expenditure

istock.com/IakovKalinin

64,5 million CB cards

1.4 avg card per person

1.5 million PoS merchants

(almost 2 million attended / unattended terminals)

99% end-user satisfaction
(2015)

A fragmented mobile payment landscape

- Many different mobile payment solutions with different security models
  - Bar/QR-code-based (security relying on phone being online during payment)
  - Contactless (NFC-based) (should work without the phone being online), can be either:
    - ✓ SIM-based (in FR no more)
    - ✓ Embedded Secure Element based (e.g. Apple Pay)
    - ✓ HCE based (Host Card Emulation)

- **Host Card Emulation (HCE)** has significant traction
  - From **Google**: put HCE into Android and later developed Android Pay using it
  - From '**OEM-Pays**': easier integration, no additional hardware (eSE) needed
  - From issuing **banks**: single application for all Android platforms
    - ✓ no OEM fees
    - ✓ no technical partnership required (MNO, OEM)
    - ✓ no brand intermediation
    - ✓ transaction data does not get shared
  - Even from PoS vendors ('Host PoS Emulation') for contactless-only mobile acceptance

A fragmented mobile payment landscape

Reminder: Card schemes ‘certify’ all payment solutions to achieve a consistent security level across them (and thus maintain a sustainable issuer risk)

- Fraud / insecurity of any type of mobile payment solution will **jeopardize trust** in all of mobile payment
  - Consumer does not care about security models of HCE vs SE

- Payment security must not be a competitive issue for tech companies: issuing banks should be able to offer a **consistent security level** in this fragmented landscape of mobile payment platforms
  - Similar user experience (e. g. use of biometrics for authentication on any phone)
  - Similar risk management strategy

The HCE security challenge

- The HCE security model is currently not satisfactory, relying on:
  - Android phones being ‘secure’ (unrealistic since most of them are never getting patched)
  - ‘Defense in depth’ software security controls (anti-debug/tamper, obfuscation, whitebox cryptography…)
    - ✓ Individually weak
    - ✓ Altogether ‘raising the bar’ on the attacker
    - ✓ Requiring permanent security R&D with strong reaction capabilities to adjust security model faced to fraud

- Implementations slowly improving by relying on Android security features
  - TEE-based *Keystore*
  - *SafetyNet* attestation

The TEE opportunity for HCE

Objectives

- Reduce dependency on software-only security controls built on top of Android
  - ✓ Hardware-level security for the (service provider) masses!
- Achieve ‘OEM-pay’-like consistent integration of security layer
  - ✓ Payment assets + EMV cryptography + authentication within TEE
- Streamline security assurance
  - ✓ Rely on certified (GP, CC) platforms and security features

The TEE opportunity for HCE

Challenges

- Avoid fragmentation of TEE platforms and APIs
  - ✓ HCE supported by Android 4.4 onwards (Java + native code)
  - ✓ HCE vendors provide a single binary SDK, easy to integrate
- Be independent of OEM updates lifecycle for applications
  - ✓ Mobile payment specifications change
- Remaining cost-effective compared to other ‘security-enhanced’ solutions (e.g. eSE-based)
- Demonstrate added security in the long run
  - ✓ ARM TrustZone and TEE software currently under heavy ‘security researchers’ scrutiny

Thank you for your attention

INTÉGRATEUR D'INNOVATION