FutureTPM H2020 PROJECT: Secure Mobile Wallet and Payments

1st FutureTPM Workshop, 19th October 2018, Lisbon

Fanis Sklinos – fanis@indev.gr / Stratos Moros - stratos@indev.gr

Future Proofing the Connected World: A Quantum-Resistant Trusted Platform Module

The FutureTPM project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779391.

Mobile Wallet and Payment

- Offers convenience compared to traditional wallet
- Security Challenges
- Only 23% of security experts believe that mobile payments are currently sufficiently robust
- Need and proof for secure and trusted transactions

Security Challenges

- Existing Threats identified by ENISA:
  - **Mobile user threats** – installation of rogue and malware applications, phishing and social engineering
  - **Mobile device threats** – unauthorized access, lost or stolen device
  - **Mobile payment application and wallet threats** – reverse engineering, tampering with the payment application and the use of rootkits
  - Merchant threats – Point of Sale (POS) malware, Man-in-the-Middle (MiTM) and replay attacks
  - Payment service providers' and Acquirers threats – payment system compromise and data connectivity compromise
  - Payment Network Providers Threats – token service compromise and denial of service
  - Issuers Threats – payment authorization process compromise, token data compromise
  - Mobile Payment Applications Providers threats – compromise of sensitive data, compromise of user profile managed in the cloud, token compromise and denial of service attacks
- Threats arising form Quantum-Computing
  - Crypto-primitives are broken (TLS, asymmetric crypto in general)

“As-Is” Scenario

- Actively developed and highly ranked application
- Tens of thousands active users
- Social auth – verified phone number is required
- Token based auth with FreePOS service
- OAuth 2.0 with PCI compliant services
- Conducts actual monetary transactions
- Depends on OS level security (No TPM present)

Sensitive Data Stored

- **FreePOS token** that authenticates between the client and the service
- **Bearer token** required to authenticate with the PCI compliant services
- **Transaction metadata** in local DB

Testing infrastructure has been deployed

- Authorized accounts (along with phone numbers)
- Authorized credit card details
- Infrastructure mirrors the production
- Same tokens are generated, with the exact same methods

TPM Functional Requirements

- Confidentiality
  - TPC key storage persistency will be used for token storage (NVRAM)
  - Symmetric Encryption will be used for database (SQLite) encryption
- Integrity
  - HMAC digital signatures will be used

The above need to be considered in the QR Domain.

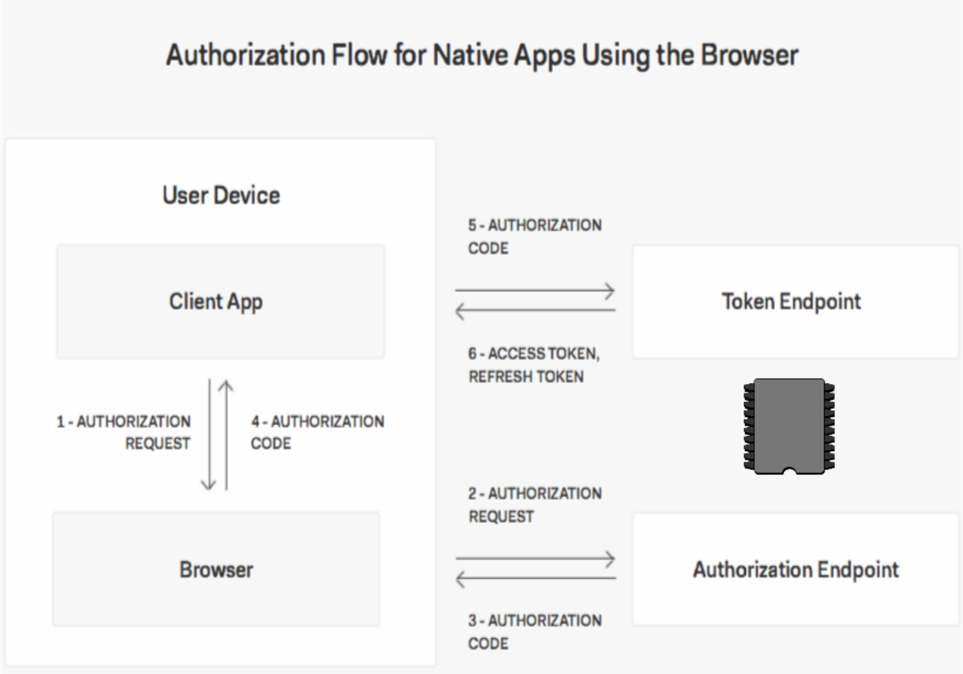
"To-Be" Reference Scenario

- **User Identification:**
  - The client is going to store all important credentials within the TPM:
    - OAuth Bearer tokens
    - FreePOS authentication tokens
- **Financial Data Confidentiality and Integrity**
  - Local storage metadata will utilize the TPM for encryption and signing

User Identification

- The application stores two discreet types of tokens on the device's main storage:
  - the FreePOS token that authenticates between the client and the business logic;
  - the bearer token required to authenticate with the PCI compliant services.
- Anyone with root privileges could gain access to the tokens

Authorization Flow



Financial Data Confidentiality and Integrity

- The application stores on an encrypted local SQLite DB
  - the users' past financial transactions,
  - along with any associated metadata.
- Keys stored on the device and the encryption is performed via third party libraries
  - Anyone with root privileges could gain access to the actual data
- TPM is necessary to store the keys

Qualitative Metrics

Id	Metric	Target Value	(M)andatory / (G)ood to Have / (O)ptional
1	Store OAuth bearer tokens in the QR TPM	Supported	M
2	Store Authentication tokens in the QR TPM	Supported	M
3	Encrypt the local database using keys generated by the QR TPM	Supported	M
4	Sign the local database using the QR TPM	Supported	M

Basic investigated TPM functionalities

- Key management
- Key hierarchy
- Encryption
- Key Derivation Function (KDF)
- HMAC signatures

QR Transition

- Symmetric Crypto
  - Encryption
    - AES128 → AES256
  - Key Derivation Function (KDF)
    - SHA256 → SHA512
  - HMAC signatures
    - HMAC/SHA256 → HMAC/SHA512/SHA3
    - qTESLA
- Asymmetric crypto
  - Key exchange protocols between device and service provider
    - QR New Hope key exchange protocol or
    - Hybrid key exchange protocol
      - QR New Hope – device side
      - Traditional crypto – service side

FutureTPM Grant Agreement No. 779391

"The FutureTPM project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779391."

If you need further information, please contact the coordinator:

TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55 Fax: +43 4242 233 55 77
E-Mail: coordination@futuretpm.eu