MOBILE PAYMENT APPLICATIONS:RISKS AND POSSIBILITIES

Trishla Shah, Raghav Sampangi, Angela Siegel

Department of Computer Science, Dalhousie University

Overview

- Mobile payment applications have become more popular and, in many cases, have replaced traditional wallets due to their ease of use, convenience, and compatibility with financial sources like banks [1].
- The security concerns with these applications remain incredibly important, especially for a product having a huge consumer market.
- In our work, we analyze mobile payment applications and discuss the threats associated with them.
- We classify the deployment stages of a mobile payment application and identify the risk associated with it. It opens up research direction in building threat models and appropriate risk assessment methods for mobile payment applications.

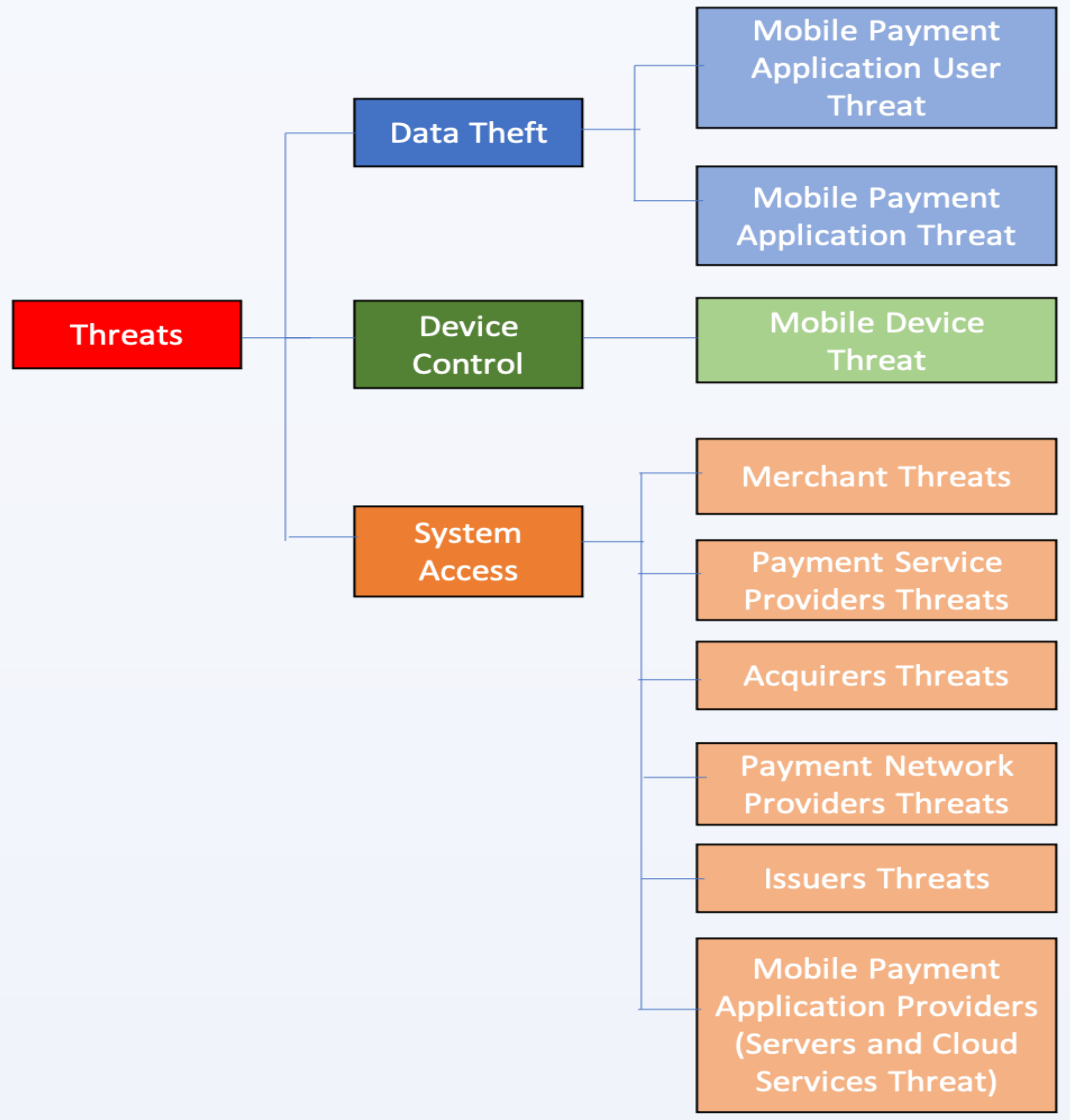
Threats in mobile payment ecosystem

We studied the leading payment applications – Samsung pay, Apple pay and Android pay and identified threats in these applications. Table 1 shows the comparison of leading payment applications.

Features	Samsung pay	Apple pay	Google pay
Compatible devices	Samsung devices	Apple devices	Android devices
Authentication	Fingerprint, PIN or iris	FaceID or fingerprint	Fingerprint, PIN, pattern or password
Cards	Credit, debit, loyalty and gift cards	Credit, debit and loyalty cards	Credit, debit, loyalty and gift cards
Technology	NFC and MST	NFC	NFC
Offline payments	Supported	Supported	
Security mechanism	Tokenization	Fingerprint authentication	Storae of users' sensitive information using HCE
Authentication before a payment can go through	Iris scan, fingerprint, or PIN	Fingerprint, FaceID, or PIN.	Fingerprint, password, pattern, or PIN
When stolen	Remotely wipe the device	Remotely wipe the device	Remotely wipe the device

Table 1: Comparison of leading payment applications

- Based on the guidelines from Payment Card Industry Data Security Standard (PCI DSS) [2] , we evaluated the threats at various stages in the mobile payment cycle.
- These threats were divided at the data level, device level, and system level. These threats are as shown in Fig1.



Threats

Data Theft

Mobile Payment Application User Threat

Mobile Payment Application Threat

Device Control

Mobile Device Threat

System Access

Merchant Threats

Payment Service Providers Threats

Acquirers Threats

Payment Network Providers Threats

Issuers Threats

Mobile Payment Application Providers (Servers and Cloud Services Threat)

Fig.1. Threats in mobile payment ecosystem

Risk assessment

- Several methods and systems have been proposed from various perspectives for solving the issue of mobile security [3].
- However, none have explored the risk level of each process within the payment applications.
- The proposed risk assessment model is constructed separately for the **Payment phase** (Fig 2) and the **Card enrolment phase** (Fig 3).
- The model focuses on decision points at each stage of the process. These decision points act like diagnostic checks for raising alerts.

Proposed risk assessment model

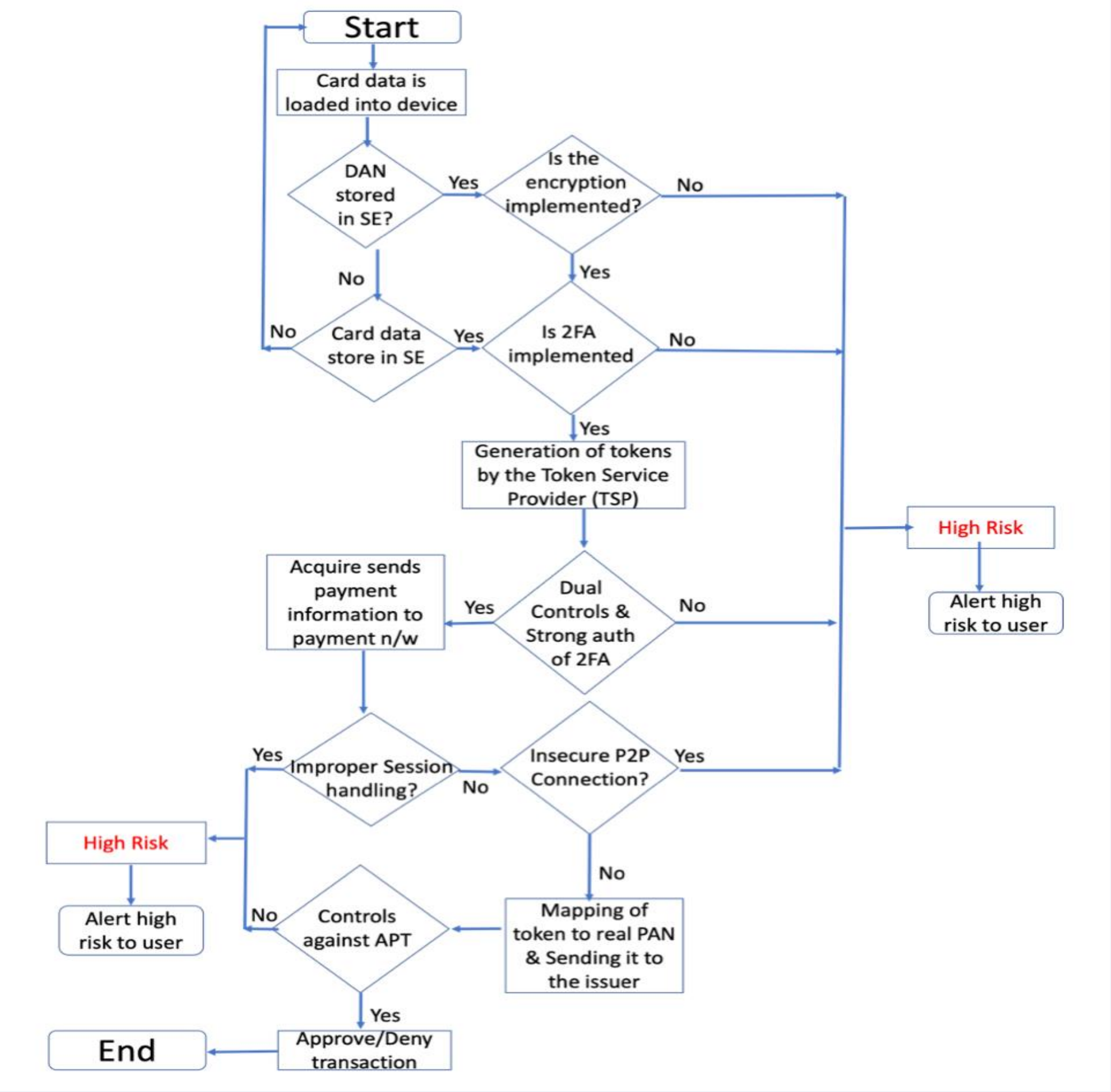

Start
Card data is loaded into device
DAN stored in SE?
Yes
No
Is the encryption implemented?
No
Yes
No
Card data store in SE
Yes
Is 2FA implemented
No
Yes
Generation of tokens by the Token Service Provider (TSP)
High Risk
Alert high risk to user
Acquire sends payment information to payment n/w
Yes
Dual Controls & Strong auth of 2FA
No
Yes
Improper Session handling?
No
Insecure P2P Connection?
Yes
High Risk
Alert high risk to user
No
No
Controls against APT
Mapping of token to real PAN & Sending it to the issuer
Yes
End
Approve/Deny transaction

Fig.2 Risk assessment model - payment phase

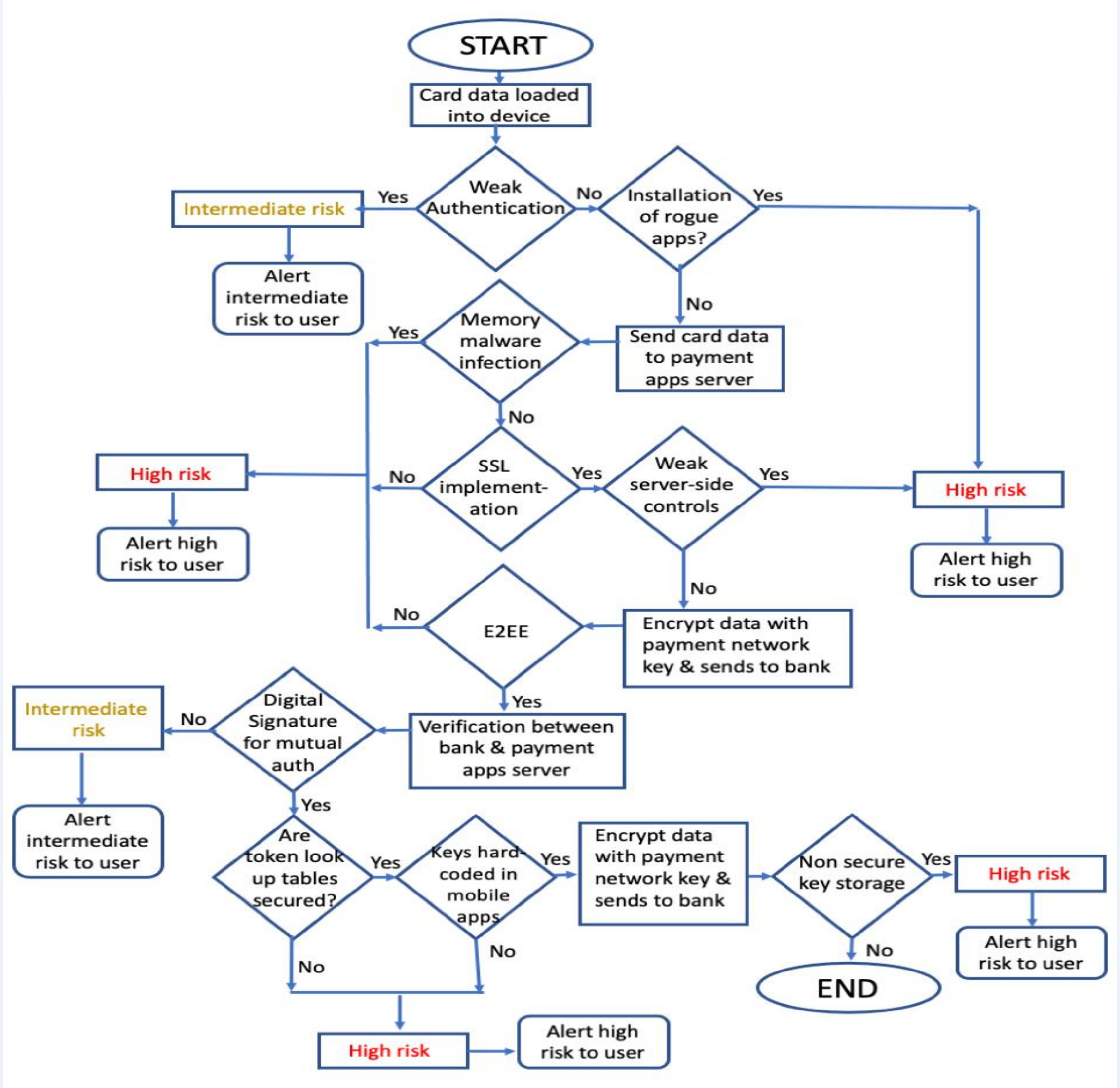

START
Card data loaded into device
Intermediate risk
Yes
Weak Authentication
No
Installation of rogue apps?
Yes
Alert intermediate risk to user
No
Yes
Memory malware infection
Send card data to payment apps server
No
High risk
No
SSL implement-ation
Yes
Weak server-side controls
Yes
High risk
Alert high risk to user
No
Alert high risk to user
No
E2EE
Encrypt data with payment network key & sends to bank
Yes
Intermediate risk
No
Digital Signature for mutual auth
Verification between bank & payment apps server
Yes
Alert intermediate risk to user
Are token look up tables secured?
Yes
Keys hard-coded in mobile apps
Yes
Encrypt data with payment network key & sends to bank
Non secure key storage
Yes
High risk
No
No
No
END
Alert high risk to user
High risk
Alert high risk to user

Fig.3 Risk assessment model - card enrolment phase

`

Future direction

- The components at each level have two patterns: A few of them were static and did not update their value throughout the payment cycle.
- While most of them were volatile whose value changed in every transaction e.g., token numbers. Hence, while designing a risk mitigation system both these type of components needs to be treated independently.
- In addition to these two aspects, we explore the impact of various categories of threats and vulnerabilities on such a risk assessment and mitigation system.
- We also explore dynamic user data and its impact on risk assessment and mitigation in real-time payment scenarios.

References

1. Mobile wallets accepted by merchants worldwide,"Statista, 2018.[Online].
2. J. Seaman, "Pci dss applicability," in PCI DSS. Springer, 2020, pp.195–211
3. T. Lederm and N. L. Clarke, "Risk assessment for mobile devices,"inInternational Conference on Trust, Privacy and Security in Digital Business. Springer, 2011, pp. 210–221
4. M. Theoharidou, A. Mylonas, and D. Gritzalis, "A risk assessment method for smartphones," in IFIP International Information Security Conference.Springer, 2012, pp. 443–456.
5. A. Mylonas, M. Theoharidou, and D. Gritzalis, "Assessing privacy risks in android: A user-centric approach," in International Workshop on Risk Assessment and Risk-driven Testing. Springer, 2013, pp. 21–37.
6. H. Verkasalo, "Analysis of smartphone user behavior," in 2010 Ninth International Conference on Mobile Business and 2010 Ninth Global Mobility Round table (ICMB-GMR). IEEE, 2010, pp. 258–263.