Security Assessment of HCE-NFC enabled E-Wallet Banking Android Apps

Ratinder Kaur, Yan Li, Junaid Iqbal, Hugo Gonzalez, Natalia Stakhanova

Canadian Institute for Cybersecurity (CIC), University of new Brunswick (UNB)

ABSTRACT

E-wallets have started to grow in popularity, reaching to a tipping point in some countries. This can be attributed to the worldwide use of payment-enabled devices and ubiquity of e-wallet acceptance by larger and smaller retailers. As more customers adopt e-wallets they may also become a big target of cybercrime. E-wallets facilitates financial transactions via smartphones which is a lucrative opportunity for cybercriminals. This work presents a security assessment of the Android e-wallet apps provided by the Canada's leading banks. We performed security analysis of the mobile apps only and testing on the cloud infrastructure, payment network, NFC communication technology was out of the scope.

Introduction

- E-Wallet apps allows the user to store multiple payment information in the phone and pay for goods and services just by tapping the phone over the payment terminal.
- The tap and pay functionality is facilitated by Near Field Communication (NFC) technology which enables a smartphone to emulate smart card using e-wallets apps. There are two ways to do emulation:
  - Secure Element (SE)
  - Host Card Emulation (HCE)

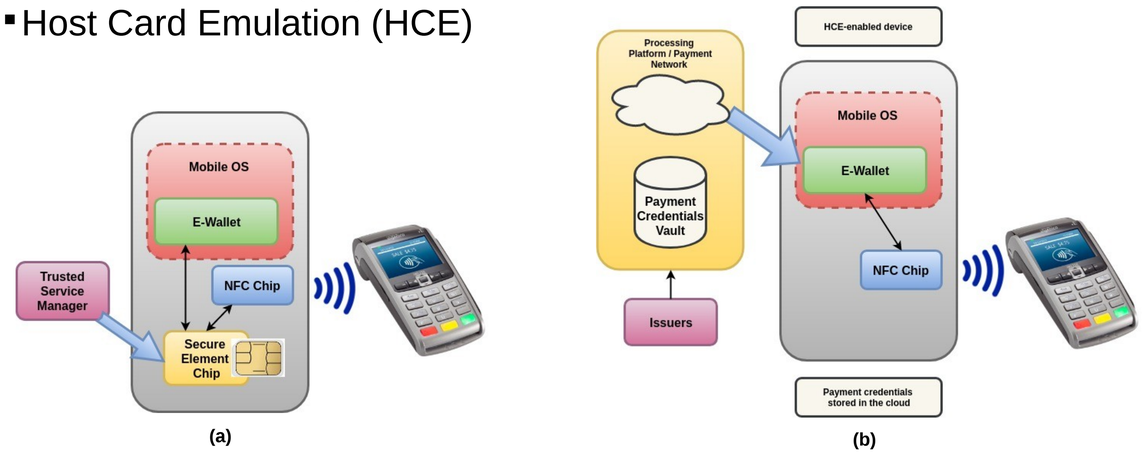


Figure1: (a) Card Emulation with a Secure Element (b) Host-based Card Emulation

Testing Android Apps

- Test set comprises of e-wallet apps from large and leading banks in Canada. These are security critical apps with large user base and motivated attackers. Often have additional security feature such as two-factor authentication and unlike other apps, are thoroughly tested before being distributed.
- Rules to assess security of apps are derived from **OWASP Mobile Security Project's Top Ten** Mobile Risks (M1 to M10) and the security recommendations provided by **Canadian Bankers Association (CBA)**.

RBC	RBC-Wallet App is pure e-wallet app for tap and pay at NFC POS terminals. RBC Bank has a separate app solely for mobile banking. This e-wallet app is only for RBC Bank account holders.
TD	TD Bank App combines e-wallet tap and pay functionality in its mobile banking app and is only for TD Bank account holders.
	ScotiaBank App also combines e-wallet tap and pay functionality in its mobile banking app. It is only for Scotia Bank account holders.
pay	Android Pay (now GooglePay) is a pure e-wallet app that accepts credit cards from any banks.

Figure2: Test Set

Table1: Security Rules to Assess an E-Wallet App

Set	Derived Security Rules
Minimal: This set of rules define an app as a possible e-wallet.	• Android 4.4 or higher • Use of NFC-HCE permission • No third-party ads libraries
Device security: This set of rules assures if a device is compromised or not.	• No rooted devices • No emulator
Application security: This set certifies whether the app is be trusted or not.	• Self-verification integrity {M8} • Protected app (obfuscated or packed) • No debuggable flag • No open intents {M1} • No legacy versions
Communication security and Dynamic data: This set of rules ensures the confidentiality of app data in transit.	• HTTPS enforced {M3} • Proper certificate pinned • No weak cryptography (no md5) {M5} • Proper key management process {M9}, {M10}
Device Storage: This set of rules covers unintended data leakage.	• No sensitive information in backups {M2}
Memory: This rule checks for the data leak during runtime.	• No sensitive information on the memory

Analysis Process

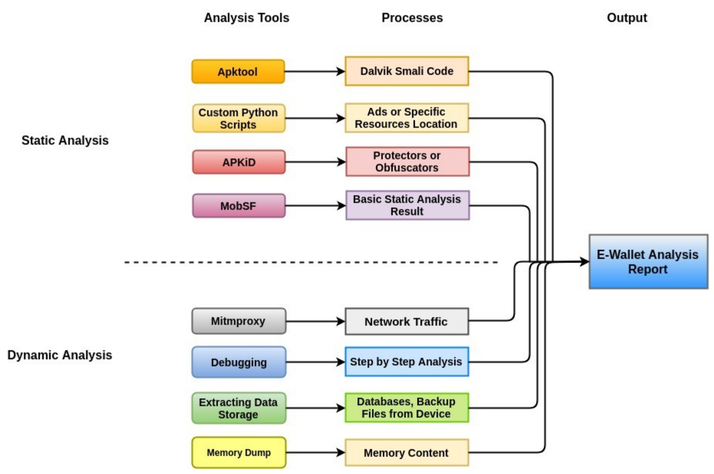
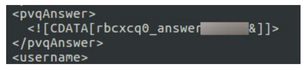


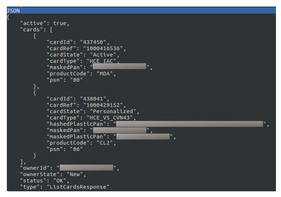
Figure3: Analysis Tools and Processes Applied for Assessment

Findings

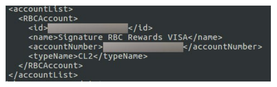
(a) Login Details



(b) Security Answer



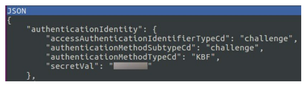
(d) Card Details



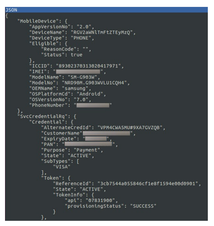
(c) Account Number

Figure4 (a-d): Data Leak RBC-Wallet App

(d) Login Details



(e) Security Answer



(f) Device and Card Details

Figure5 (d-f): Data Leak TD Bank App

Table2: Security Assessment Results

Rules	RBC-Wallet	TD Bank	ScotiaBank	Android Pay
No third-party ads libraries	√	√	√	√
No rooted devices	√, bypassed	X	X	√
No emulator	√, bypassed	X	X	√
Self-verification integrity	√, bypassed	X	X	√
Obfuscated or packed	√	√	√	√
Not debuggable	√	X	X	√
No legacy app versions	X	√	√	√
HTTPS enforced	X	X	√	√
Proper certificate pinned	X	X	√	√
No weak cryptography	X	X	√	√
No sensitive information in backups	√	√	√	√

Conclusions

This poster presents the security assessment of e-wallet apps of some leading banks in Canadian market. We performed manually analysis on three apps and compared with the Android Pay, which is the most popular and quite secure e-wallet app. Our analysis targets basic device, application and communication security. It was found that e-wallet apps in the Canadian market are not well secured.