CMSGu2016-04

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Mobile Payment Security

CERT-MU

National Computer Board
Mauritius

Version 1.0

September 2016

Issue No. 4

Table of Contents

1.0 Introduction 4
1.1 Purpose and Scope 4
1.2 Audience 4
1.3 Document Structure 4
2.0 Background 5
3.0 Risks Associated with Mobile Payments 7
4.0 Guidelines for risks and controls when using mobile devices for payment 8
4.1 Prevent unauthorized logical device access 8
4.2 Create server-side controls and report unauthorized access 8
4.3 Prevent escalation of privileges 8
4.4 Create the ability to remotely disable the payment application 9
4.5 Detect theft or loss 9
4.6 Harden supporting systems 9
4.7 Prefer online transactions 9
4.8 Conform to secure coding, engineering, and testing 9
4.9 Protect against known vulnerabilities 10
4.10 Protect the mobile device from unauthorized applications 10
4.11 Protect the mobile device from malware 11
4.12 Protect the mobile device from unauthorized attachments 11
4.13 Create instructional materials for implementation and use 11
4.14 Support secure merchant receipts 11
4.15 Provide an indication of secure state 11
4.16 Mitigating Risks Associated with Mobile Payments 12
5.0 Conclusion 13
6.0 References 14
Appendix A 15
MCB Juice 15

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this document is to educate users on the secure use of mobile devices when using such devices for payment.

1.2 Audience

The target audience for this guideline includes all users of mobile devices for payment.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 gives a background on the current state of mobile payments.

Section 3 lists the risks associated with mobile payments.

Section 4 provides the precautions to take when using mobile devices for payment.

Section 5 concludes the document.

Section 6 contains a list of references that have been used in this document.

Appendix A illustrates the login and registration processes for MCB Juice users.

2.0 Background

The proliferation of mobile devices such as smartphones and tablets not only gives consumers more choice, it also has the potential to dramatically expand the payments ecosystem, bringing new players such as mobile operators and handset manufacturers into the mix. Multiple payment advocates are competing for attention, with each party advancing a different vision for where the consumer's electronic wallet (the trusted source of credentials) should reside: on a card, on a phone, or in the Cloud. These various approaches create new challenges and in some cases have the potential to establish new business models. The traditional role of banks in issuing physical cards that are mailed to users could be replaced by new classes of intermediaries such as Trusted Service Managers (TSMs) that provide over-the-air provisioning capabilities to mobile devices.

While new mobility for the customer continues to inspire innovation, these changes also create new data protection challenges. Whether organizations are issuing payment credentials and applications, accepting payments, or processing payments on the back end, they must keep stored customer and account information secure. Mobile transactions must be protected, whether they occur via Near Field Communication (NFC) in a store, on a tablet computer, or using a mobile phone over a wireless network. And every organization involved must continue to comply with an evolving set of industry mandates.

With the market in flux and plenty of innovation still to come, organizations are challenged to:

- Remain flexible, prepared to support a range of mobile payment scenarios and business models as they evolve.
- Be alert to disruptive change that can disturb existing revenue streams.
- Run traditional and mobile payments processes in parallel, while avoiding as much as possible the need for duplication of processing infrastructure and creation of unnecessary silos.
- Keep abreast of emerging technologies and standards for issuing credentials and applications, making payments, and accepting payments (and the business opportunities and risks they create).
- Accommodate peer-to-peer payments as they expand the market beyond the world of retail. Even in developing countries, the need to exchange funds has already triggered innovation beyond the traditional banking model.

- Accelerate the transition to a cashless society by embracing micropayments for parking meters, vending machines, highway tolls, and other purchases that otherwise involve the unnecessary costs and inconvenience of handling cash.
- Build relationships with new players, including mobile device suppliers, peer-to-peer payment services, wallet providers, TSM services, loyalty applications, consumer credit scoring agencies, and others.

3.0 Risks Associated with Mobile Payments

- Inability to adapt to mobile payments can put your company at a competitive disadvantage.
- New processes create new security vulnerabilities. Over-the-air provisioning of payment credentials and applications, for example, potentially creates new attack vectors for eavesdroppers to steal and misuse customer data.
- Attackers can steal and misuse data, leading to painful disclosures, adverse publicity, and fines.
- Failure to understand exactly where and how sensitive account data is stored and transmitted can prevent organizations from clearly defining and implementing data protection solutions.
- Rising transaction volumes can lead to performance bottlenecks as inefficient processing limits capacity and degrades the customer experience.
- Overly cumbersome and costly security schemes can hinder an organization's ability to adapt quickly to new opportunities or to scale its business processes to meet rising service demand.

Figure 1 Top 4 Vulnerabilities of Mobile Payment

4.0 Guidelines for risks and controls when using mobile devices for payment

This section addresses security measures essential to the integrity of the mobile platform and associated application environment.

4.1 Prevent unauthorized logical device access

Protect mobile device from unauthorized logical access. Include design features that prevent unauthorized use. For example, include in the design one of the more secure lock screens: “Face Unlock,” “Password,” “Pattern,” or “PIN.” Do not rely on “Slide,” since it does not add security. Include a feature that would force the user to re-authenticate to the device after a specified amount of time. Bypassing of the lock screen may be prevented by enabling full disk encryption and/or disabling USB debugging.

The mobile app developer should include the capability for the mobile app to determine whether USB debugging is disabled and whether full disk encryption is enabled. In addition, the operating-system developer should include controls that can prevent the user from enabling USB debugging or disabling full disk encryption.

4.2 Create server-side controls and report unauthorized access

Develop the overall payment-acceptance solution to include capabilities for preventing and reporting unauthorized access attempts, identifying and reporting abnormal activity, and discontinuing access (i.e., the payment-acceptance solution would prevent further access by the mobile payment-acceptance app on that device until an administrator restores access). Controls include, but are not limited to:

- Support for authorized access (e.g., access control list)
- Ability to monitor events and to distinguish normal from abnormal events
- Ability to report events (e.g., via a log, message, or signal) including cryptographic key changes, escalation of privileges, invalid login attempts exceeding a threshold, updates to application software or firmware, and similar actions

4.3 Prevent escalation of privileges

Controls should exist to prevent the escalation of privileges on the device (e.g., root or group privileges). Bypassing permissions can allow untrusted security decisions to be made, thus

increasing the number of possible attack vectors. Controls should include but are not limited to:

- Providing the capability for the device to produce an alarm or warning if there is an attempt to "root" or "jail-break" the device;
- Providing the capability within the payment-acceptance solution for identifying authorized objects[6] and designing controls to limit access to only those objects.

4.4 Create the ability to remotely disable the payment application

The payment application should support a mechanism that permits it to be disabled by the merchant or solution provider responsible for the payment system application. The feature should not interfere with other, non-payment functions of the mobile device.

4.5 Detect theft or loss

A process should exist for the detection and reporting of the theft or loss of the mobile device. Inherent to such a process should be a means for testing and for confirming that it remains active. Examples include the use of Global Positioning System (GPS) or other location technology with the ability to set geographic boundaries, periodic re-authentication of the user, and periodic re-authentication of the device.

4.6 Harden supporting systems

Supporting systems that either provide management for mobile devices or receive payment card data should be hardened to prevent unintended access or exposure of a mobile payment transaction. Therefore, any system used to support the mobile payment-acceptance solution should be compliant with the Payment Card Industry Data Security Standard (PCI DSS).

4.7 Prefer online transactions

When the mobile payment-acceptance application on the host is not accessible, the mobile device should neither authorize transactions offline nor store transactions for later transmission.

4.8 Conform to secure coding, engineering, and testing

Mobile payment-acceptance applications should conform to secure coding, engineering, and testing conventions, such as the requirements and testing procedures outlined in the Payment Application Data Security Standard (PA-DSS). Other examples include Institute for Security

and Open Methodologies (ISECOM)'s Open Source Security Testing Methodology Manual (OSSTMM), or International Systems Security Engineering Association (ISSEA)'s Systems Security Engineering Capability Maturity Model (SSE-CMM – ISO/IEC 21827).

Developers should be trained on PCI standards. Secure-coding best practices should cover prevention of common coding vulnerabilities in software development processes to include but not be limited to injection flaws, buffer overflow, insecure cryptographic storage, insecure communications, improper error handling, and improper access control.

Developers should also document their implementation and create a formal response plan to identify and mitigate new risk. Developers should establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities and to test their applications for vulnerabilities. Any underlying software or systems that are provided with or required by the application should be included in this process.

4.9 Protect against known vulnerabilities

Provide a secure means for keeping mobile device software and all applications up-to-date through patch management and other means to prevent compromise of the mobile device due to vulnerable software. Controls should include but are not limited to:

- Evaluate updates prior to implementing them.
- Ensure that updates are received from a trusted source.
- Apply updates in a timely manner.

4.10 Protect the mobile device from unauthorized applications

All authorized mobile apps, drivers and other software that form part of the payment solution should have a mechanism that permits authentication of the source and integrity of the executable file. The system should prevent the loading and subsequent execution of applications that cannot be authenticated. Developers should ensure that a process exists for the secure distribution of their software such that an end user can determine that the software came from a trusted source before installing it. For instance, it may not be permissible to download apps from an online store whose security cannot be validated.

4.11 Protect the mobile device from malware

Enhance current capabilities to protect mobile device from malware. Deploy anti-malware products on all systems including antivirus, antispyware, and software-authentication products to protect systems from current and evolving malicious software threats.

Mechanisms (such as a displayed icon) should exist to demonstrate that persistent protection is active and that it is from a trusted source.

4.12 Protect the mobile device from unauthorized attachments

If an entry device is attached to the mobile device (e.g., card reader), whether the connection is physical or wireless, it needs to identify itself uniquely to the mobile payment-acceptance app to ensure that the correct entry device is paired to the correct mobile device. Mutual authentication between the entry device and the mobile device provides the best integrity assurance for the path. When the entry device is attached, the mobile payment-acceptance app validates the account data entry device via serial number or other unique identifier.

4.13 Create instructional materials for implementation and use

Documentation should exist specifically to address the proper, secure use of mobile devices in the merchant environment, including instructional material on the hardware, operating system, and application software.

4.14 Support secure merchant receipts

Regardless of the method used for producing receipts (e.g., e-mail, SMS, or attached printer), the method should mask the Primary Account Number (PAN) in support of applicable laws, regulations, and payment-card brand policies. Insecure channels such as e-mail and Short Message Service (SMS) should not be used to send banking details.

4.15 Provide an indication of secure state

A trusted execution environment (or equivalent) should include a mechanism for indicating to the mobile-device user that the payment-acceptance mobile app is executing in a secure state. This would be similar to the indication that a Secure Socket Layer (SSL) session is active in a browser.

4.16 Mitigating Risks Associated with Mobile Payments

There are various measures that can be taken to address the security challenges of mobile banking and payments. As a summary, the table below lists the major risks and the suggested mitigation.

Risk	Suggested Mitigation
Mobile more susceptible to loss or theft	• Customer Education • Implementation of remote wipe, passcode and automatic lock out
Users more likely to store personal and sensitive information on mobile device	• Customer education • Device encryption • Ensure applications do not store customer sensitive data locally
Malware	• Mobile malware protection • Do not jailbreak your device
Malicious applications	• Customer education • Use only reputable sites to download apps • Ensure that apps for tested for security
Privacy violations	• Customer education • Security testing applications and data handling
Wireless carrier infrastructure	• Vet the security if the carrier infrastructure and services through targeted questions
Payment systems infrastructure	• Ensure the point of sale device vulnerabilities and addressed • Make use of Europay, MasterCard, and Visa (EMV) where possible
SMS vulnerabilities	• SMS should not be used as a channel for money movement and other high risk transactions
Hardware and OS vulnerabilities	• Ensure that software updates are being pushed to devices
Complex supply chain and new entrants in the mobile ecosystem	• Implement a third party vendor security program
Lack of maturity in fraud tools and controls	• Extend current online fraud tools and controls to the mobile channel • Secure provisioning/de-provisioning

Table 1 Mitigating Risks Associated with Mobile Payments

5.0 Conclusion

Mobile payments have become quite popular nowadays with the proliferation of mobile connected devices and ease of access. With this come new risks and attacks, so users should exercise caution and secure their devices when effecting payment to mitigate, if not eradicate the risks.

6.0 References

- **www.thales-esecurity.com**
- **www.ecb.europa.eu**
- **www.isaca.org**
- **www.pcisecuritystandards.org**
- **www.juice.mu**

Appendix A

MCB Juice

The sections below explains how to login as a Juice user and register as a new Juice user.

Existing Juice users:

1. Log in to Juice using your Internet Banking Username & Password
2. Acknowledge the revised 'Terms and Conditions'
3. Confirm your 'Mobile Phone' number which will be used for future communications
4. Enter the six-digit 'Verification Code' sent to you by SMS to validate your registration to Juice
5. Select your four-digit mPIN (non-consecutive and non-repetitive numbers) which will enable you to access Juice and complete your transactions instantly and securely. The mPIN adds more security to your Juice account as it can be used uniquely on your phone
6. Confirm your mPin
7. Registration successful. You can now log in to Juice using your mPin to discover a new world of lifestyle banking at your fingertips

New Juice users:

1. Get the application from App Store (iOS/Apple), Google Play (Android), **https://juice.mcb.mu**
2. Create your Juice account
3. Select your Juice registration method, via Internet Banking, Debit card or Credit card details
4. Acknowledge the 'Terms and Conditions'
5. Select your daily funds transfer limit
6. Confirm your 'Mobile Phone' number which will be used for future communications
7. Enter the six-digit code 'Verification Code' sent to you by SMS to validate your registration to Juice
8. Select your four-digit mPIN (non-consecutive & non-repetitive numbers) which will enable you to access Juice and complete your transactions instantly and securely. The mPIN adds more security to your Juice account as it can be used uniquely on your phone.
9. Confirm your mPin

10. Registration successful. You can now log in to Juice using your mPin to discover a new world of lifestyle banking at your fingertips

Security Measure:

- Keep your username/password secure in case you forget your mPIN or use another phone. In such cases, you will have to go again through registration steps highlighted above.