MITIGATING SECURITY RISKS IN USSD-BASED MOBILE PAYMENT APPLICATIONS

By Suhas Desai
Executive Summary

According to Gartner, 2014 there will be over 3 billion mobile users in the world. One of the hottest mobile technology applications will be mobile payments and financial services. However, the wide acceptance of mobile technology will lead to major security concerns among banks, telecom companies and service providers.

Mobile payment applications use various communications channels which are not secure, including SMS, USSD and IP-based communications. As usage of these communications channels by payment applications increases, security flaws are becoming prime concerns for service providers.

Critical threats such as fraudulent transactions, request/response manipulations, weak encryption, and insecure message communications are directly triggering revenue loss for mobile payment service providers. Fraudulent transactions, mobile application request/response tampering/dropping, sensitive information disclosure due to weak cryptographic implementation, improper account management, and modification of sensitive information can also cause security breaches and loss of sensitive data in USSD-based mobile payment applications.

In light of these threats, application development and integration companies, telecoms, and banks providing payment services need to assess USSD-based apps and ensure that secure coding practices have been followed during USSD-based applications software development.

In this white paper, critical threats for USSD-based mobile payment applications and Aujas approach to mitigate identified mobile application threats have been discussed in detail. The Aujas Security Lab recommended comprehensive framework is also presented to address mobile payment applications security and risks in mobile payment applications. Best practices to mitigate these risks are also presented.
THE NEED FOR MOBILE APPLICATION SECURITY

2014 will witness over 3 billion mobile users worldwide, according to Gartner’s research. Mobiles phones will become the preferred and most commonly used web device globally by 2013. They will be considered the most convenient device for almost everything that PCs are doing today. As a result, a large number of mobile applications will be built for multiple platforms (Android, J2ME, Symbian, etc.) and domains (mobile payments, mobile commerce, mobile VAS, etc.).

As more and more transactions are made over mobile phones, hackers are perpetrating more fraud and attacks. Experts believe more security breaches are inevitable as mobile usage grows. What makes mobile phones vulnerable is the speed and advancement of technology, along with continued business demand for newer mobile products and services. Proper security controls must become an intrinsic part of mobile phones and mobile applications.

Major business impacts in case of mobile application security breach are:

- Fraudulent transactions (Revenue Loss) through mobile applications
- Confidentiality (Users sensitive data- Credit/Debit Card Data, PIN, user credentials)
- Revenue loss through communications services misuse
- Brand value degradation through SIM card cloning related attacks
- Misuse of Enterprises Data through personal handheld devices
- Fraudulent transactions through USSD (Unstructured Supplementary Service Data) and DST (Dynamic SIM Toolkit) Applications

While telecoms and the rest of the service chain are becoming more motivated to deploy secure, reliable and robust products, the task is challenging. There are multiple mobile operating systems platforms, various telecom providers; banking services dependencies, and a complex network infrastructure to consider.

The Aujas Mobile Security Research Lab has designed a security framework which addresses Unstructured Supplementary Service Data (USSD) based mobile payment applications security in the application and network communications layers, local and server data storage, cryptography, and data transmission.

USSD-BASED MOBILE PAYMENT APPLICATION OVERVIEW

The Unstructured Supplementary Service Data communication protocol is widely used to provide mobile communication services, location-based services, mapping services, recharge/booking services, and mobile payment services along with banking services. USSD is preferred over the SMS communication channel. In USSD channels, STORE-FORWARD model is not used. The service provider’s SMS gateways and other infra-components are used in STORE-FORWARD model.

In USSD, direct communication between sender and recipients is established and this promotes faster data transmission. USSD communication is session-oriented and it is easily implementable while being more user-friendly. The developer community prefers USSD channels for development of mobile payment application because of these powerful features.

In this white paper, we look at USSD-based mobile payment application for performing a fund transfer and related payment services. This USSD-based mobile application can be installed on any mobile platform and supports all the mobile operating systems. The customer can use USSD applications for various transactions such as prepaid recharge, fund transfers, bill pay, and reservations. The customer can use his prepaid balance available in his account and also funds from his bank account.

The USSD application is connected as an interface between the customer’s telecom provider and his bank account. The customer can transact through both, handheld devices and web-based applications (USSD in IP mode). The customer can perform transactions through his mobile payment account and has the flexibility to perform the same transactions through his bank account.
CRITICAL THREATS – USSD-BASED MOBILE PAYMENT APPLICATIONS

This section details some of the critical threats for USSD-based mobile payment applications. These attack vectors were used in Aujas Security Lab to perform attacks against a sample mobile payment application.

**USSD Commands Request/Response Tampering**
A malicious user can tamper with USSD command requests and responses. This may cause confusion for the legitimate user and can also lead to fraudulent transactions. This request and response tampering is possible through hardware and software interceptors. Weak encrypted request and response messages are prime concerns in such threat vectors.

**USSD Request/Response Message Replay Attacks**
When a phone is lost, an adversary may perform fraudulent transactions through an installed USSD application. An application must authenticate USSD request originator (authentication through combination of MSISDN, IMEI, PIN and unique Message Tracking ID). If this USSD application server or application is unable to authenticate the USSD request originator, then it can perform fraudulent transactions.

**USSD Application Prepaid Roaming Access Test**
An adversary may get unauthorized access to USSD application prepaid roaming services. He may misuse chargeable roaming services with the help of roaming access parameters manipulation. This may lead to direct revenue loss for service providers.

**Local Data and USSD Server - Data Storage Security Tests**
An adversary may use clear text or weak encrypted data to perform fraudulent transactions. Clear text or weak encrypted data may reveal sensitive data (e.g., balance, customer number, PIN, account details, etc.). Using this sensitive data, an adversary may perform fraudulent transactions.

**USSD Server Response Tests**
The USSD application server should respond properly upon valid requests generated by an authenticated user. Weak encrypted response message, response delay and response exception handling (in case of buffer overrun, delivery notification) are the prime concerns in USSD application server response mechanism.

**Verify Strong Cryptographic Implementation**
Weak implementation of cryptography for critical data (customer number, credit/debit card numbers, PIN, passwords, beneficiary details – account numbers, balance summary) can be tampered. This can lead to fraudulent transactions.

**USSD Content Error Tests**
Improper USSD content error-handling may reveal sensitive information about customer data, USSD application and the service provider’s sensitive data.

**USSD Response Time Tests**
Improper USSD response time implementation may result in delay or tampering delivery notifications, transaction success messages and alerts.

**Improper Session Management**
In this case, an adversary gets physical access to a victim’s phone which has a USSD application installed on it. The adversary may perform any malicious activity on financial transaction modules (e.g., send money) due to improper session time-out implementation. It is also applicable to all financial transactions modules.

**Improper Data Validation (USSD IP Mode Applications)**
Improper data validation in USSD IP mode application can lead to SQL injection, cross site scripting attacks. An adversary may purposely insert specifically crafted scripts in user input. Once successfully inserted in the database, the attacker may try to use the same to perform malicious actions at the database or at other user’s active session.

SECURING USSD-BASED MOBILE PAYMENT APPLICATIONS

Aujas recommends a four phase approach to securing the mobile application:

**Phase 1 – Information Gathering**
The first phase is to conduct a detailed security assessment of the USSD-based mobile payment applications, its mobile validation layer and other infra-components involved in payment services. This provides a list of critical vulnerabilities in the application. The next step is to determine remediation measures and controls needed to mitigate identified vulnerabilities and implement secure interfaces. Mobile validation layer and application’s vulnerabilities fixing should also be covered in this phase.

The next step is to gather information for the USSD application architecture, mobile validation layer, USSD application server architecture, USSD application server logs, and USSD application server request-response mechanism.
Phase 2 – USSD Application Security Assessment

Security tests need to be performed against USSD applications and other involved components. Almost all the critical threats should be covered in this assessment. Individual components and security assessment with black box, gray box and white box approaches provides in-depth assessment. This approach identifies vulnerabilities from the attacker’s perspective. It should not be considered as a comprehensive assessment of vulnerabilities that may exist in the target assets.

The comprehensive black/gray/white box application testing consists of the following steps:

a) Zero Knowledge Testing

USSD applications should be tested for all the common application-level vulnerabilities and attacks.

b) Testing with user credentials and given role(s)

The applications should be checked for vulnerabilities that allows authorized users (for any role as provided) to escalate privileges and access restricted data or information. This phase of testing is performed after receiving a legitimate user account with appropriate rights from the client.

In the White box approach, detailed source code review should be performed with respect to secure coding best practices. There are manual and automated tool to find vulnerabilities in the source code of applications.

Phase 3 – Mobile Access Layer Security Assessment

In this phase, mobile validation layer components should be assessed manually and by automated techniques and tools.

Secure financial transactions through payment gateways, banks infrastructure components, payment service provider’s interfaces should be assessed as well. Major assessment tests should involve strong encryption, secure transmission over the network layer, secure payment transactions through interfaces and communications channels (USSD/IP based channel), and session management.

Phase 4 – Mitigating USSD Application Security Threats

In this final phase, the remediation needs to be done for the identified USSD-based application security threats, mobile validation layer threats, payment service provider’s interfaces vulnerabilities and the bank’s interface threats. It could mean implementing secure interfaces, writing secure code for entire USSD-based application and verifying it against secure coding best practices.

Best Practices to Secure USSD-based Mobile Payment Application

1. Validate all trusted (local data storage or server data storage) and not trusted (invalid user inputs e.g., special characters) inputs in the application.
2. Secure the interface between payment gateways and mobile payment application
3. Secure data transmission from handheld devices to the application server
4. Secure data storage on local handheld devices
5. Implement proper session management in the application
6. Implement a strong encryption mechanism to store sensitive data
7. Employ a strong authentication mechanism in the application
8. Use two-way authentication while performing critical financial transactions
9. Employ response and request messages encryption
10. Implement a proper message authentication mechanism to validate that requests/responses are generated through authenticated users
11. Use secure USSD communication channels with a strong encryption mechanism.
SUMMARY
A systematic approach to assessing and remediating vulnerabilities in mobile applications and is critical to ensuring secure payment transactions. Aujas recommends adopting a 4-phase security assessment:

• Detailed and proactive security assessment helps the client ensure secure financial transactions through mobile payment client applications

• Mobile client application and mobile validation layers security are enhanced through a proactive approach during entire SDLC

• Detailed analysis of the security gaps against the security best practices benchmarks

• Threat modeling activity using STRIDE/DREAD approach helps in identifying the application’s vulnerable

• Mapping identified vulnerabilities to threats brings about a clear understanding of the security issues in the application and how they may be exploited

• Mapping vulnerabilities to flaws at the architecture and design level helps prepare a comprehensive remediation plan

• Identifies vulnerabilities in financial transactions, application residing on mobile device and sensitive data transmission over wireless network which automated tools may not detect
ABOUT THE AUTHOR
Suhas Desai
A Senior Consultant of Aujas, working in Mobile Security Services. At Aujas, he is working in Mobile Apps, USSD Apps, Mobile VAS, SIM card and Mobile Payment’s Security. Prior to joining Aujas Networks, he has worked with Tech Mahindra.

Suhas has delivered noted sessions at OSSPAC’09, Singapore; INTEROP 2009, Mumbai; SteP-IN 2010 Bangalore; MOSC 2010, Kuala Lumpur; O5BizConference 2010, Malaysia; ‘Mobile VAS in Growth Markets summit’, 2010, Dubai and at ‘4th Mobile Commerce Summit ASIA’, 2011, Kuala Lumpur.

A frequent speaker at prominent industry and customer forums, Desai has been on technical advisory committees for prestigious National and International conferences. He has delivered over 350 conference talks on software & mobile security across the globe.

Suhas is a contributing writer for Linux for You, Linux+ and Linux Journal magazines.

ABOUT AUJAS
Aujas (www.aujas.com) is a global Information Risk Management services company and an IDG Ventures funded company. Aujas consultants work with the client’s management teams to align information risk with business initiatives, so that security becomes a business driver and competitive advantage. Aujas helps clients manage emerging technologies – mobile devices, social media, cloud computing – that are transforming the business environment and posing increasing security challenges.

The company offers global clients:
- Information risk advisory services
- Secure development life-cycle services
- Identity and access management services
- Managed information risk services
- Vulnerability management services
- Mobile, social media and cloud security services

For more information about mobile security services, please contact Karl Kispert, Aujas Vice President, Business Development at karl.kispert@aujas.com or (973) 229-5566.