International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

Risk Management in Mobile Banking

Dr. K V D Kiran
Department of Computer Science and Engineering
KLUniversity, Guntur, Andhra Pradesh, India

M V R Srivatsava, K Gayathri Devi
Department of Computer Science and Engineering
KLUniversity, Guntur, Andhra Pradesh, India

***Abstract*— In the current era of competition, the use of computers and allied technologies has become inevitable and it has been well recognized that Information Systems plays different roles in different industries. This paper makes an attempt to explore empirically the difference in the role of Information Systems in the banking sector. The study indicates that the future impact of Information Systems does not vary significantly with the banking groups. Today information security plays a vital role in different fields. Information security compresses of risk management and risk assessment, which plays a vital role in identifying risks, threats and vulnerabilities. Different tools like OCTAVE, MAGERIT, MEHARI, RA2 e.t.c.., which provide risk management and risk assessment for different information systems like banking, medical e.t.c. In this aspect we consider the scenario of mobile banking in banking sector.**

Keywords—information security, risk management, risk assement, technologies, risk mitigation, mobile banking

I. INTRODUCTION

The banking industry has never seen such a fundamental change as mobile banking. Globally, millions of consumers are already using a wide array of mobile devices to conduct banking - and millions more are expected to go mobile in the coming future. But with that growth come a whole new set of threats: mobile malware, third-party apps, unsecured Wi-Fi networks, risky consumer behavior. And it does not matter whether an institution uses a proprietary or third-party mobile banking application - the bank owns the risks.

II. KEY SECURITY RISKS

A major challenge for the adoption of mobile banking technology and services is the perception of insecurity. In the survey conducted by the Federal Reserve, 48% of respondents cited their main reason for not using mobile banking was "I'm concerned about the security of mobile banking". In the same study, respondents were asked to rate the security of mobile banking for protecting their personal information and 32% rated it as somewhat unsafe and very unsafe, while 34% were not sure of the security. These statistics represent a significant barrier to the use of mobile banking products and services. ("Consumer and Mobile Financial Services," 2012)

When the security risks of the mobile space are analyzed, many of these feelings are not necessarily irrational. The lack of maturity of the mobile banking space brings many risks in the areas of new technologies, new inexperienced entrants in the ecosystem and a complex supply chain with risks in secure integration of the complex ecosystem. Many of these new entrants are innovative and dynamic with minimal experience or attention to security as a discipline. These risks are most evident in the mobile application development and mobile hosting areas. New privacy risks are brought to light with personal data collected by the applications and information about the customer's physical location. Finally, customers are largely uneducated or have a high risk tolerance and unfortunately may opt into services that put their security and privacy in jeopardy.

The security risks associated with mobile devices are very similar to any other computing device with a few key exceptions:

- Mobile devices have a smaller form factor and therefore are more susceptible to loss or theft
- Mobile devices are more personal and there will be a tendency for users to use devices in a more personal and confidential way
- Security controls and tools available have not matured to accommodate the constraints of limited processing power and limited battery life

The key risks to the mobile device include:

- Malware
- Malicious applications
- Privacy violations relative to application collection and distribution of data
- Wireless carrier infrastructure
- Payments infrastructure/ecosystem
- SMS vulnerabilities
- Hardware and Operating System vulnerabilities
- Complex supply chain and new entrants into the mobile ecosystem
- Lack of maturity of Fraud tools and controls

A. Mobile Device and application vulnerabilities

Malware is becoming a growing challenge with mobile devices ninety nine percent of the malware growth was in two categories: spyware and SMS Trojans. The integrity of applications is key risk relative to mobile devices. There are various malicious applications posing as legitimate applications that users download and then become infected. The warranties of the device may be nullified when a device is jail broken. Despite these risks, the efforts to overcome the manufacturer's impediments to jail break persist. Short Message Service (SMS) is susceptible to misuse including redirection, hijacking and spoofing. The SMS channel can also be compromised by malware as was the case with a malicious application posing as a free well known Android application.

B. *Privacy*

Privacy of user information is a particularly challenging issue as mobile devices are much more personalized and tied to the user's identity than a traditional computer. Risks related to legitimate applications passing user data to other applications or 3rd parties in an unauthorized manner is gaining more attention in the public arena.
user permission to use their location data; unfortunately it is not clear all the ways that application may use the data.

C. *Wireless Carrier*

In addition to the internet, mobile devices have another key network involved in the processing of mobile communications. The wireless carrier is the primary interface to the mobile device. The radio component of the mobile device communicates to the cell sites. The cell sites then communicate through dedicated circuit or microwave to the mobile switching center (data center) which contains both the voice processing and data processing equipment and systems. The switching center contains the gateway to the Internet and other carrier networks. If there is a security weakness in any part of this network, it can put the customer's data at risk.

D. *Payments Technology*

The payments infrastructure can also have vulnerabilities that lead to security risk. The keys stored on the secure element can be vulnerable to exposure if the keys are not protected properly from unauthorized access and use. Mobile payment applications employ a pin or password that is required to unlock the data in the secure element.

III. RISK MITIGATION

RISKS	MITIGATION
Mobile more susceptible for loss or theft	• Customer Education • Implementation of remote wipe,passcode and automatic lockout
Users are more likely to store personal and sensitive information on mobile device	• Customer Education • Device encryption • Ensure applications don't store customer sensitive data locally
Malware	• Mobile malware protection • Don't jailbreak your device
Malicious	• Customer Education
Applications	• Use only reputed sites to download apps • Ensure that apps are tested for security
Privacy Violations	• Customer Education • Security testing of applications and data handling
Wireless carrier infrastructure	• Vet the security of the carrier infrastructure and services through targeted questions
Payment system infrastructure	• Ensure the point of sale device vulnerabilities are addressed • Utilize EMV where possible
SMS vulnerabilities	• SMS should not be used as 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	• Current online tools and controls are extended to the mobile challenge • Secure provisioning/de-provisioning

IV.CONCLUSION

The mobile banking and payments ecosystem is complex and dynamic. It is not clear who will emerge as the winner(s) in the growing space from a financial services, application provider or technology perspective. Security and the perception of security will clearly play a role in who ends up dominating. Traditional financial service companies (banks, processors, and card associations) clearly have an advantage from controlling the existing banking and payments infrastructure. The extent to which they can strategically extend their products and services in a way that maintains the customer's trust in their services be key to their success. A foundational element of that trust is the security of the products and services. The wireless carriers are challenged by entering a segment with little financial service experience. Wireless carriers are challenged by being perceived as simply a wireless bandwidth pipe and have struggled with this since the advent of wireless data. Application providers within this space clearly hold an edge relative to innovation and speed to market, however, lack of focus on security and privacy will inhibit progress. Additionally, both wireless carriers and

application providers are at a clear disadvantage in terms of understanding the regulatory environment faced by current financial service providers.

v.ACKNOWLEDGEMENT

We would like to thank our project guide Mr. V D Kiran in guiding us and helping us to complete the research paper. We would like to thank our academic co coordinator and HOD of CSE in giving us an opportunity to do a research oriented project as part of our academics.

REFERENCES

[1] The Allan, Ant. "Q&A: Phone-Based Authentication Methods", Gartner, June 24, 2010

[2] Basso, Monica and Gammage, Brian. "Smartpone Virtualization: Making Mobile Applications More Trustable", Gartner, April 21, 2011

[3] Eigdon, Emmett. "US Mobile Banking Forecast", Forrester, January 31, 2011 Essers, Loek. "Untethered jailbreak for iOS 5.1.1 available for download", May 25th,2012,

[4] Hesse, Alexander. "The Time is Right to Start Experimenting with Mobile Banking for Marketing and Sales", Forrester, April 5, 2011