ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Literature Survey on Mobile Banking Security

Sudeep George,Reshma M

P.G Scholar, Dept. of Computer Science and Engineering, Cochin College of Engineering, Kerala, India Assistant Professor, Dept. of Computer Science and Engineering, Cochin College of Engineering, Kerala, India

ABSTRACT: Security is one of the biggest challenges for any online based services. For banking services, it become much more important, as it deals with customer's money and any security issues can put theirbusiness into a huge risk like money loss, client loss etc. The aim of this paper is to identify and classify the different security challenges associated with mobile banking. Identifying and resolving the security problems reported till now is very important. In this survey, we will be comparing different encryption algorithms, different security challenges identified and we will be proposing a new method for overcoming the challenges.

KEYWORDS: Security in online services, mobile banking, protocols of mobile banking,security challenges in mobile banking, comparison of encryption algorithms

I. INTRODUCTION

Mobile banking and Internet banking are very similar, except you are using a smart phone to bank alternately the computer. The applications of many smartphones connect you directly to your bank, allow you to transfer money, and some banks even allow you to make deposits by taking a picture of the check [1].

Mobile banking is becoming increasingly popular due to convenience and flexibility it offers. Mobile banking has a lots of advantages like

- Saving time and energy
- Reduced cost
- Easy to use
- Easy to use compared to internet banking

On the other hand, mobile banking has a lot of security challenges or issues associated with it. Security issues associated ranges from the basic DDOS attack to the complex Trojans and social engineering techniques to hack someone's credentials.

In order to prevent user from security attacks, it is important identify the risks involved which include risks in server , mobile devices etc.

II. RELATED WORK

The related works in mobile banking security is divided in to 8 sections

- Identify vulnerabilities of mobile banking
- Identify risks in wireless application protocol
- Identifyrisks in servers
- Security needed in mobile commerce
- Secure Architecture of Mobile banking
- Different protocols of mobile
- Review of Encryption Algorithm
- Proposed Method

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Vulnerabilities of mobile banking

a) Distributed Denial of service (DDOS)Attack

A distributed denial-of-service (DDoS) is a type of computer attack that uses a number of hosts to overwhelm a server, causing a website to experience a complete system crash. DDOS attack is ranked as third highest threat as per FBI. DDOS is the most common attack of banking system.

DDOS attack is ranked as third highest threat as FBI said. DDOS is the most common attack of banking system. DDOS attack orbit the attack to target system. Before an attack is happen, attacker will be attack network by scanning open ports [2].

b) Malware

Malware is short for "malicious software" - computer programs designed to infiltrate and damage computers without the user's consent. "Malware" is the general term covering all the different types of threats to your computer safety such as viruses, spyware, worms, Trojans, rootkits and so on.

c) Backdoors

d) TCP/IP Spoofing

e) Tampering

Tampering is an intentional modification of products in a way that would make them harmful to the consumer [3].

f) Exploits

Exploit is a piece of software, or a data which acts as a bug or vulnerability in order to matter surprising behaviour to exist on computer software, or hardware [4].

g) Social Engineering and Trojans

Trojans act as no authorized programs. Can delete, block, modify, and copy data. However, Trojan is not like a viruses and worms, it is not able to self-replicate [5].

Risks in wireless application protocol

- Eavesdropper attacker
- Unencrypted data during switching between protocols
- Attacker can contact to unencrypted data [6]

Risks in servers

- System may crash
- Server may be failed
- Virus may be attack

Security needed in mobile commerce

- Transaction privacy
- Authentication of parties
- Proof of transaction authorization by user
- Impossibility of unauthorized payments [7]

Secure Architecture of Mobile banking

It is divided in to 7 layers

- Mobile Service Provider Layer
- Services Broker Layer
- Communication Layer

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

- Mobile Application Layer
- Middleware Layer
- Applets Layer
- Secure layer

In order to add more security to mobile transactions, 4 additional security services are implemented

- Mobile registration and identity management
- Mobile public key interface (PKY)
- Mobile authentication and authorization
- Secure messaging

There are different technologies for authenticating the customer. Such as customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices, one time passwords (OPTs), USB plug in or other tokens, transaction profile scripts, biometric identification

Online threats of mobile banking

Broad threats	Phone threats	Online threats
Unauthorized access Malicious hacking Malware, Mobile Viruses	Memory cards, Downloads, Various, Application, Mobile Browsers, Smart cards	Mobile E-mail, SMS, Mobile IM, Voice, Online Games, Gateway

Different protocols of mobile

- **Secure Electronic Transaction (SET) protocol:**The Secure Electronic Transaction (SET) protocol has been proposed by a consortium of credit card companies and software corporations to secure e-commerce transactions. When the customer makes a purchase, the SET dual signature guarantees authenticity while keeping the customer's account details secret from the merchant and his choice of goods secret from the bank. [8]
- **IKP Protocol:**The IKP technology is based on RSA public-key cryptography. Depending on requirements, an electronic payment transaction using IKP may involve one, two, or three public keys: in all cases the bank acquiring the transaction for processing will have a public-private key pair for receiving confidential information such as credit card numbers and signing authorization messages; in many cases the merchant will also have a public-private key pair for receiving confidential information and signing payment requests and purchase confirmations; in some cases even customers may have a public-private key pair for signing payment transactions. In all cases they have a PIN for confirming authorization of payment. [9]
- **Mobile ID protocol:**The Mobile-ID protocol carries the context information of the man in the middle from the mobile client to the Mobile-ID server which then compares this information with the information belonging to the intended service provider and stops the protocol by notifying the mismatch. [10]

- **GPRS Protocol:**The flow of GPRS protocol stack and end-to-end message from MS to the GGSN is displayed in the below diagram. GTP is the protocol used between the SGSN and GGSN using the Gn interface.This is a Layer 3 tunnelling protocol. [11]

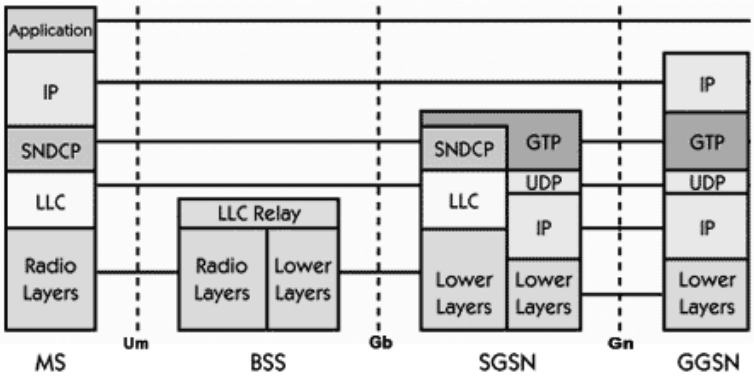
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017



Comparison of Encryption Algorithms

PARAMETERS	DES	3DES	AES	RSA	BLOWFISH
DEVELOPMENT	In early 1970 by IBM and Published in 1977.	IBM in 1978.	Vincent Rijmen, Joan Daeman in 2001	Ron Rivest, Shamir & Leonard Adleman in 1978	Bruce Schneier in 1993
KEY LENGTH (Bits)	64 (56 usable)	168,112	128,192, 256	Key length depends on no. of bits in the module	Variable key length i.e. 32 – 448
ROUNDS	16	48	10,12,14	1	16
BLOCK SIZE (Bits)	64	64	18	Variable block size	64
ATTACKS FOUND	Exclusive Key search, Linear cryptanalysis, Differential analysis	Related Key attack	Key recovery attack, Side channel attack	Brute force attack, timing attack	No attack is found to be successful against blowfish.
LEVEL OF SECURITY	Adequate security	Adequate security	Excellent security	Good level of security	Highly secure
ENCRYPTION SPEED	Very slow	Very slow	Faster	Average	Very fast

- **DES:**DES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must know and use the same private key. DES is symmetric key algorithm based on the backbone concept of Feistel Structure. Once the go-to, symmetric-key algorithm for the encryption of electronic data. It is a block cipher that uses a 64-bit plain text with 16 rounds and a Key Length of 56-bit, originally the key is of 64 bits, one bit has been selected as 'parity'
- **Triple-DES:** Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. There are three keying options in data encryption standards:
  - All keys being independent

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

- Key 1 and key 2 being independent keys
- All three keys being identical

Key option #3 is known as triple DES. The triple DES key length contains 168 bits but the key security falls to 112 bits.

- **Blowfish:**Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Since then it has been analysed considerably, and it is slowly gaining acceptance as a strong encryption algorithm. Blowfish is unpatented and license-free, and is available free for all uses.
- **IDEA:**IDEA (International Data Encryption Algorithm) is an encryption algorithm developed at ETH in Zurich, Switzerland. It uses a block cipher with a 128-bit key, and is generally considered to be very secure. It is considered among the best publicly known algorithms. In the several years that it has been in use, no practical attacks on it have been published despite of a number of attempts to find some. IDEA is patented in the United States and in most of the European countries. The patent is held by Ascom-Tech. Non-commercial use of IDEA is free.
- **TEA:**The Tiny Encryption Algorithm (TEA) block cipher was designed with speed and simplicity in mind. It is a variant of the Feistel Cipher. TEA operates on a 64 bit block of data that is then split up into two 32 bit unsigned integers during the encryption process. TEA uses a 128 bit key, and a magic constant is also utilized which is defined as 2^32/(the golden ratio).
- **CASTS5:**CAST-128 is a 12- or 16-round Feistel network with a 64-bit block size and a key size of between 40 to 128 bits (but only in 8-bit increments). The full 16 rounds are used when the key size is longer than 80 bits. Components include large 8×32-bit S-boxes based on bent functions, key-dependent rotations, modular addition and subtraction, and XOR operations. There are three alternating types of round function(image on the right), but they are similar in structure and differ only in the choice of the exact operation (addition, subtraction or XOR) at various points. Also its based in the Feistel Cipher structure.
- **AES(Rigndael):**Rijndael is the block cipher algorithm recently chosen by the National Institute of Science and Technology (NIST) as the Advanced Encryption Standard (AES). It supercedes the Data Encryption Standard (DES). NIST selected Rijndael as the standard symmetric key encryption algorithm to be used to encrypt sensitive (unclassified) American federal information

III. PROPOSED SOLUTION

- Channel Manager: Channel Manager provides an API in form of web services to handle transactions or queries expected from Internet Banking, and Mobile Banking. Channel Manager accepts only requests from known devices and other applications which are accepted by channel manager.For each entity which wish to perform an operation, it must get registered with Channel Manager Application. Channel manager will provide a shared unique secret key to every entity. Entity will be responsible to preserve this key securely, and use it to generate a checksum for every request sent out and verify checksum by Channel Manager Application for every request received.

  In Channel manager there is two security layers:

  - Authentication:For authentication of each request, we choose following attributes
    - User name
    - Vendor name
    - Password
    - Secret key
  - Authorization: For Authorization of request the following have been selected.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

- User name
- Vender name
- Action name
- Password
- Check sum
- Secret Key

Channel manger uses timestamp and checksum for authorisation. It uses SHA-256 for encryption along with secret key. Channel manager validates checksum followed by validation of time stamp of the service.

IV. CONCLUSION AND FUTURE WORK

The main reason that Mobile Banking scores over Internet Banking is that it enables 'Anywhere Banking'. Customers now don't need access to a computer terminal to access their banks, they can now do so on the go – when they are waiting for their bus to work, when they are traveling or when they are waiting for their orders to come through in a restaurant.

In this paper we tried to gather all information regarding mobile banking like its architecture, different protocols of mobile, vulnerabilities found till now, comparisons of different encryption algorithm etc.

In final stage, we proposed a more secure system for mobile banking which has 2 security layers.
Authorization and Authentication. In order provide additional security in network layer, a mechanism for authorizing the message which is encrypted in SHA-256 is discussed.

As a future work, it has been planned to implement the cloud technology in bank sector. This ensures secure authentication thereby increasing the bank revenue and reducing the networking problems which arise mainly due to congestion and unauthenticated sessions. Further study in the encryption techniques that can be used along with this system will increase security in mobile banking to a greater extent. Integration of other bio metric mechanisms along with this system could also be done with some research in terms of cost, effectiveness and feasibility might increase the security by folds.

REFERENCES

1. Ashok Bahadur Singh, "Mobile banking based money order for India Post: Feasible model and assessing demand potential", International conference on emerging Economies-Prospects and challenges (2012)
2. Md. Shoriful Islam," Systematic Literature Review: Security Challenges of Mobile Banking and Payments System", International Journal of u- and e- Service, Science and Technology Vol. 7, pp. 107-116(2014)
3. Paul Judge and Mostafa Ammar, "Security Issues and Solutions in Multicast Content Distribution: A Survey ", IEEENetwork,(2003)
4. Hameed Ullah Khan, "E-banking: Online Transactions and Security Measure", Research Journal of Applied sciences, Engineering and technology 7(19): 4056-4063, (2014)
5. Rajpreet Kaur Jassal1, Ravinder Kumar Sehgal," Study of Online Banking Security Mechanism in India: Take ICICI Bank as an Example ", IOSR journal of computer engineering (IOSR-JCE), p-ISSN: 2278- 8727 Volum13, Issue1 ,PP114-121,(2013),
6. Jeong, B. K., & Yoon, T. E. , "An Empirical Investigation on Consumer Acceptance of Mobile Banking Services", Business and Management Research, 2(1), 31-40 , (2013)
7. "Alternative Graphical Authentication for Online Banking Environments", Proceedings of the Eighth International Symposium on Human Aspects of Information Security &Assurance (2014)
8. G. Bella, F. Massacci, and L. C. Paulson,"The verification of an industrial payment protocol: The SET purchase phase" In V. Atluri, editor, 9th ACM Conference on Computer and Communications Security, pages 12–20. ACM Press, (2002)
9. M.Ebrahimi, S. Khan, Shujjat kahn, UMer Bin Khalid,"Symmetric Algorithm Survey: A Comparative Analysis", International Journal of Computer Applications (0975 – 8887)Volume 61– No.20,(2013)
10. Haiyong Xie, Li Zhou, and Laxmi Bhuyan, "Architectural Analysis of Cryptographic Applications for Network Processors", Department of Computer Science & Engineering, University of California
11. ElBahlul ElFgee, Ahmed ARARA, "Technical Requirements of New Framework for GPRS Security Protocol Mobile Banking Application", International workshop on intelligent techniques in distributed systems (ITDS), Procedia Computer Science 37, (2014)