International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

NETWORK SECURITY: ATM PIN UNLOCKING AND AVOID SKIMMING BY UAN TECHINIQUE

A. Sabari Rajeswaran
Department of Information Technology, Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India
Sabari.rajeswaran@yahoo.com

Abstract

This paper deails with the solution of two major problems problems we are facing in ATM's are - one is about Skimming(Hacking) and the other is PIN blocking i.e., by the magnetic strip in the card this skimming technique is taking place and at the same instant PIN has been blocked by entering wrong PIN. As a result no further transactions cannot be initiated by next 24 hrs by PIN blocking and there is no exact solution to solve this skimming.

In this paper I am going to show how the UAN will solve both the above concern problem.

***Keywords*-- Primary Ticket, Secondary Ticket, UAN, AES Encryption, VBIP Network**

I. INTRODUCTION

The automatic teller machine (atm) is used for immediate transaction rather visiting a bank. This technique was first introduced by john shepherd-barron. After knowing this technique many parts in the world started to use the atm for transaction.

The atm transaction is mainly depend on the PIN . The user enter the PIN no so that the transaction is performed. Most of the atm is connected to interbank networks, enabling people to withdraw and deposit money from machines not belonging to the bank where they have their account or in the country where their accounts are held. Some of the examples of interbank networks include PULSE, PLUS, STAR, LINK, cirrus and interact.

Atm rely on authorization by card issuer or other authorizing institution via communication network. This is often performed through an ISO 8583 messaging system.

ATMs typically connect directly to their host or ATM Controller via either ADSL or dial-up modem over a telephone line or directly via a leased line. Leased lines are preferable to POTS lines because they require less time to establish a connection.

1.1 Kerberos protocol

Here we are using Kerberos protocol which contains authentication dialogue and TGS so that the data are secured from hacking.

1.2 TGS(Ticket granting service)

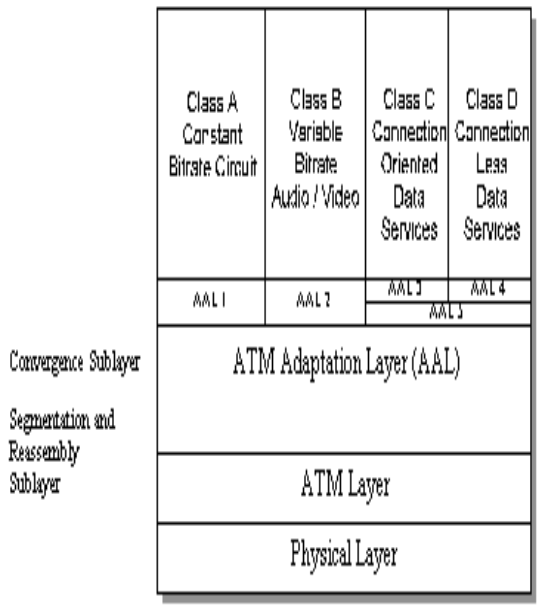
This ticket granting service contain ticket. Here the ticket is a date of birth of the user to provide a UAN secure without hack-ing.

1.3 Authentication server

The need of authentication server is to send the data to the server and to the client in a secure manner.

Here the authentication server will receive the primary key from the user access server and it checks the database for access rights. If there, then it will re-sponse the request and send the UAN to the main server and to the client.

II. ATM PROTOCOL ARCHITECTURE



Physical layer

The function of physical is

i. Cell delineation.
ii. Header error control.
iii. Insertion and removal of cell from physical medium.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

ATM layer

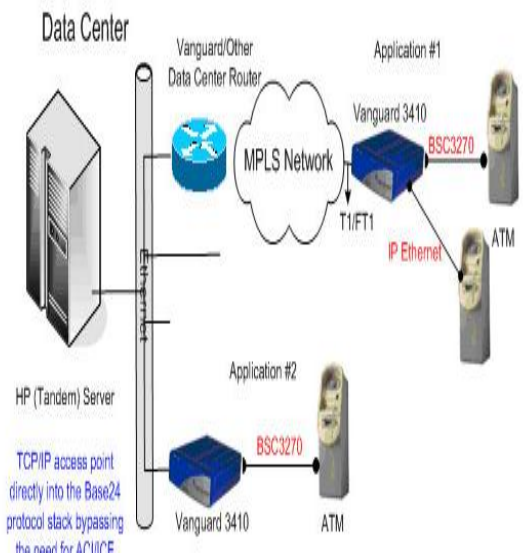
It provides cell transfer functionalities such as VC/VP(virtual circuit/virtual path) routing and multiplexing.

ATM Adaptation layer

It is a service independent and supports higher functionalities of user, control and management functionalities, such as cell segmentation and reassembly, timing control, flow control

III. VBIP ATM TRANSACTION NETWORK

Vanguard BSC3270 to TCP/IP conversion Network



Now most of the ATM machines use this VBIP Networks only for secure.

This VBIP also supports AES, DES, SSL to secure the control port and advanced QoS, as well as integral WAN interfaces ranging from 56K DSU to dual T1 ports.

IV. CRYPTOGRAPHIC ALGORITHMS

4.1.DES(Data Encryption Standard)

ATMs originally used Data Encryption Standard, to encrypt personal identification numbers (PIN).DES encrypts data in 64-bit blocks using a 56-bit encryption key.However, increases in computing power for personal computers have rendered DES insecure for ATM applications; ATMs using DES have been breached within 24 hours

4.2.Triple DES

Triple DES uses two encryption keys and applies the DES encryption algorithm three times, effectively increasing the length of the encryption key to 168-bits.

Triple DES is significantly more secure than DES, because it isn't realistic to search the individual bits of the encryption key to crack the code. According to the National Credit Union Administration, all new ATM installations since 2002 were required to employ triple DES encryption.

4.3. AES (Advanced Encryption Standard)

In 2001, the National Institute of Standards and Technology announced the adoption of a new encryption standard, known as the Advanced Encryption Standard, intended to replace DES.AES uses a variable length encryption key, with a length of 128, 192 or 256 bits, and encrypts data in 128-bit blocks. The only way for an unauthorized person to decrypt data encrypted with AES is by a so-called **brute force attack**, which involves testing all possible permutations of the encryption key, so AES is significantly more secure than DES or triples DES

V. PROBLEMS

Though the ATM machine is found a way for immediate transaction they may be a problem arises.

5.1 Problem1 (ATM PIN Blocking)

The ATM PIN will be blocked if the person enters the wrong PIN no more than 3 times.

5.1.1. Status of Blocking

Your PIN will be blocked and you can't perform any further transaction in any bank for 24 hrs.

5.1.3. Reason for Blocking

- If a person use more than one ATM card at a time then there may be a confusion with the PIN number.
- If the person doesn't use the PIN number for some time(month/year) then this problem can occur.

5.1.4. Solution

The solution to unlock the PIN number if it is has been blocked is to provide a USER ACCESS NUMBER

5.1.5. Concept

In this i am going to have a User Access Number to activate your current transaction that has be blocked by the PIN number

Note

Only the transaction its going to be released not the PIN.

BLOCK DIAGRAM

The block diagram explains the entire operation. Here we are going to additionally have 2 servers

1. Authentication server
2. User access server

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

3. Diagram Explanation

1 → user enters the PIN wrong for more than 3 times.

2 → alert indicates the your PIN has been blocked for entering wrong PIN and user UAN is activated.

3 → control is transferred from main server to user access server and the main server is under blocked state.

4 → the user access server checks whether the user is spam or not.

5 → verification is done and confirms that the user is not spam . if the user is spam then exit.

6 → send the primary ticket to the authentication server(which contains dob).

7 → the authentication server will now send the replaced number of the dob to the user access server.

8 → now both current UAN and next UAN will be send to the authentication server.

8A → control is transferred from user access server to main server and the user access server is in blocked state.

9 → main server will send the secondary ticket to the authentication server.

10 → authentication server will once again check the secondary ticket with the database information.

11 → checking of secondary ticket is over, now the authentication server will send the current UAN to main server and client.

12 → main server will now ask the client to enter the UAN .

13 → client enters the UAN and main server compares with that of with the client.

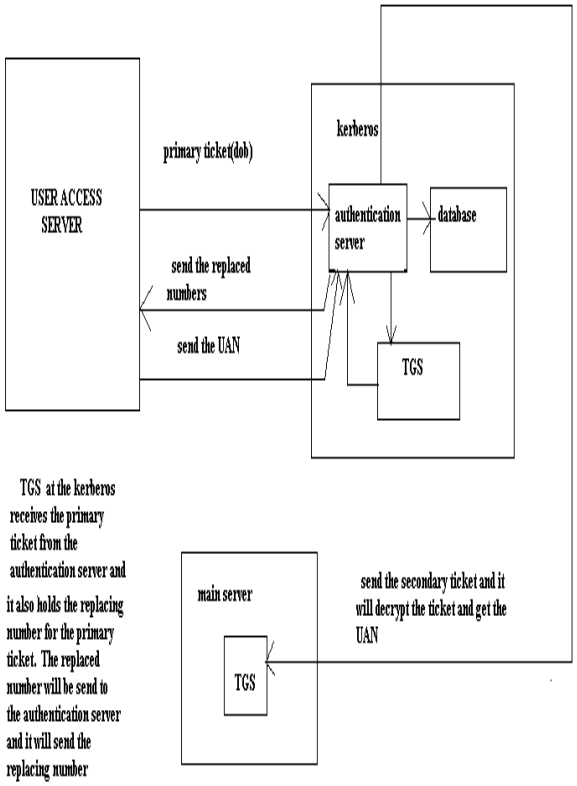
Now the blocked transaction will be released and for the next 24 hrs this will be current PIN for the user. After 24 hrs normal PIN will be activated.

User access server & authentication *server* → It has both once per log on session and once per type of service

Main server → once per type of service

5.1.6 Operation of Authentication server in Kerberos's

Diagrammatic Representation



Step 1 : primary ticket generation

As soon as the control is transferred from main server to user access server, the user access server will provide security question to check the user is spam or not.

If the user is not spam then the user access server will use the primary ticket which contains the dob of the user and send to the authentication server as a encrypted message.

The authentication server will receive the encrypted message and perform the decryption and get the primary ticket**.**

Step 2 : provide replacing numbers

Now the authentication will confirm that the user access server confirmed the user is not a spam .Now it will issue the replacing number of your primary ticket.

Step 3 : receiving the UAN

The user access server will generate the current and the next UAN . Authentication server will receive the current and next UAN.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

Step 4 : secondary ticket verification

By Authentication ServerTransfer the control from user access server to authentication server and to the main server.The main server will send the details of the user .The authentication server will once again check the secondary ticket.

Step 5 : Secondary ticket generation

It contains 2 information's

Ticket value

If value exceeds 2 the the user does not have the rights to access the UAN.

The main server is moved from blocked state to unblocked state or not.

Step 6 : sending the UAN from AS

The authentication server will now Send the UAN to both main server And client

Step 7 : releasing the transaction

The main server will now request the client to enter the UAN . Main server verifies the UAN received from the authentication server and from the client.If both matches the unlock the transaction that had been blocked.But for the next 24 hrs this will the user PIN. After that the normal PIN will be activated.

Steps in generating the UAN:

Here i am going to replace the numbers

0→0

1→3

2→5

3→1

4→7

5→2

6→9

7→4

8→8

9→6

5.1.7. Generating the 1st UAN

1. If(account no length=5)
   Suppose your date of birth is 28101995.

Now the replaced/reversed number for the date of birth is 58303662.

Now I am going to add serial no along with this number.

Serial no = (accno + age and replace the no)

Serial no = 18704 + 20= 18724

now replace/reverse this number.

1st serial no = 38457

1st UAN

58303662 + 38457 = 58342119

Generating the 2nd UAN

2nd UAN = previous UAN + serial no.

Serial no= (previous serial no + age and reverse it)

Previous serial no = 38457 + 20(age) = 38477.

After reversing, 2nd serial no = 18744

2nd UAN

58342119 + 18744 = 58360863.

Generating the 3rd UAN

3rd UAN = 2nd UAN + serialno.

Serial no= (previous serial no+age and reverse it).

Previous serial no= 18744 + 20(age) = 18764.

After reversing the serial no is 38497.

3rd UAN = 58360863 + 38497 = 58399360.

2. If(account no length<5)

Assume your Account no :1870

Reversed no : 3840 and add 0 at last. Now my reversed number is 38400. Finding the UAN is similar to previous steps.

3. If(account no length> 5 and account no <=10)

Consider,

your account no is 0916543218 (or)09165342

Then take the last 5 number i.e., 43218/65342. Finding the UAN is similar to previous steps.

This process will be continued for all other UAN.

5.1.8. Advantage

1. By this method the user can perform the transaction and there is no need to wait of 24 hrs or to visit my bank to release my PIN to perform my transaction.
2. Further this method will be time consumption of money transaction during the PIN blocked time.

5.1.9. Application

1. This technique could be applied in SIM card by entering the PUK code if the SIM has been blocked.
2. Can be applied to solve Birthday attack

5.2. Problem2 (ATM PIN Skimming)

Through the magnetic strip in the ATM card which contains both PIN and account no the Skimming activity is taking place.

5.2.1. Status of Skimming

Your PIN is hacked and the transactions can be changed.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

5.2.2. Result

ATM skimming [robbery]

5.2.3. Solution

Diagrammatic Representation of Avoiding skimming by UAN

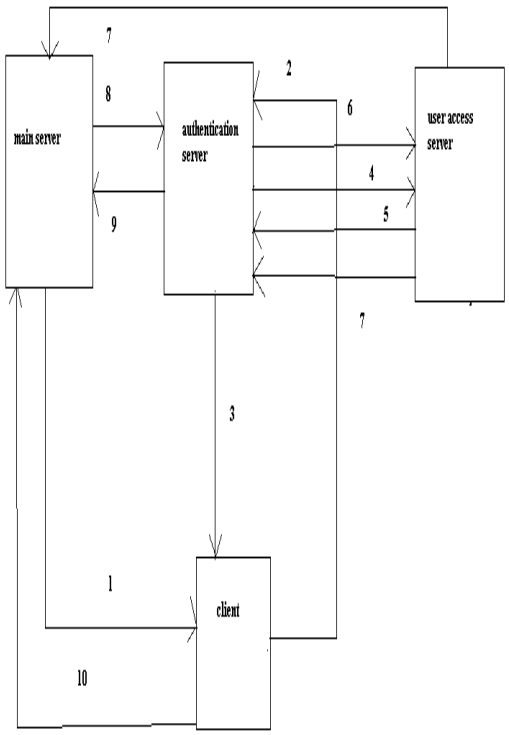


Diagram explanation

1 → user enter the PIN

2 → now the control is transferred from main server and from client to authentication server.

3 → now the authentication server will check whether the user is a spam or not.

4 → if the user is not a spam then the control is transferred from authentication server to the user access server.

5 → now the user access server will contain all the details of user as in main server and it sends the primary ticket along with the secondary ticket information of the user.

6 → the authentication server will response to the primary ticket and send the replacing number.

7 → the user access server generate the current and the next UAN and send this details to the authentication server and release the main server that has been blocked.

8 → based on the information of the secondary ticket obtained from the user access server the authentication once again request the main server for the secondary ticket.

9 →now the authentication server send the UAN to the main server.

10 → now the client perform the transaction.

VI. CONCLUSION

By using this Technique we can able to avoid the transaction problems during your PIN blocked. And this Technique could also be implemented in fields such as cell phone technology where the user enter the PUK the code at the time of blocking your SIM card.

If this technique has been implemented then it will be a greater benefit for the user who can avoid of waiting for the next day and also can avoid visiting a bank and waiting for the PIN to be released i.e., the user can avoid the problem of time consumption by this block.

Acknowledment

I gratefully acknowledge the contributions of Murari, Dilli Babu, yuvaraj, Professor Mala for their work on the orginal version of this document .

REFERENCE

1. Staffs

[1] Dilli Babu – Asst .Lecture in Panimalar Engineering College, Chennai.

[2] VeeraLakshmi – Asst. Lecture in Prince Shri Venkateshwara Padmvathy Engineering College.

2. Papers Presented at Conference Preceeding

[1] Proceedings of the NationalConference on Network Security, March 2012

[2] National level PaperPresentation on Information Security , August 2012

3. Books

[1] William Stallings, 2011 ,Cryptography and Network Security : Principles and practice, 5th Edition, Pearson Education, Prentice Hall