Impact Factor Value 4.046 e-ISSN: 2456-3463
National Conference on Quality Up-gradation in Engineering, Science and Technology (NC-QUEST018)
Organized by College of Engineering and Technology, Dhanamgaon Rly-444709
International Journal of Innovations in Engineering and Science, Vol. 3, No.6, 2018
www.ijies.net

"Security Features in ATM (Automatic Teller Machine)"

Mr. Bhushan Shambharkar , Mr. Vrushabh Rode , Mr. Swapnil Joshi

[1]*A DES's College of Engineering & Technology,*

Dr. BabaSaheb Ambedkar Technological University, Lonere, Dhamangaon rly, India,444309

[2] *A DES's College of Engineering & Technology,*

Dr. BabaSaheb Ambedkar Technological University, Lonere, Dhamangaon rly, India,444309

[3] *A DES's College of Engineering & Technology,*

Dr. BabaSaheb Ambedkar Technological University, Lonere, Dhamangaon rly, India,444309

Abstract – An ATM is an electronic device which allows a banks customer to make cash withdrawals and check their account balance at any time without a need for a human teller. Many ATMs also allow depositing cash or cheques, transfer money between their banks.

Security in the ATM Network is very necessary because it is widely spread in all areas such as financial, network administration and other important parts of financial network which requires very sensitive handling transmission of data.

Keywords: ***Automated Teller Machines , Biometric Technology , Electronic , Security***

INTRODUCTION

The first ATM in Korea was installed by Korea exchange Bank in 1975, and after installation of ATM by Shinhan Bank in 1982, the civilian can use the ATM of various banks with Starting of operation of common CD network which is controlled by Korea financial telecommunications & clearings institute.

In today's technically advanced world, autonomous systems are gaining rapid popularity. As the social computerization and automation has been increased and the ATM and credit card has been installed and spread out to simplify the activity for financial activity, the banking activity has been

simplified, however the crime related with financial organization has been increased in proportion to the ratio of spread out of automation and devices.

The security specification includes the security services that are needed and necessary for the users to protect their ATM cards from being misused. Confidentiality, Data Integrity, Accountability, Correct Functionality, Availability and Access Control are the main objectives for ATM. Principal functional security requirements can be identified to deal with the generic threats. They are:

I. AF-SEC-1: Verification of Identities;
II. AF-SEC-2: Controlled Access and Authorization; AF-SEC-3: Protection of Confidentiality;
III. AF-SEC-4: Protection of Data Integrity;
IV. AF-SEC-5: Strong Accountability;
V. AF-SEC-6: Activity Logging;
VI. AF-SEC-7: Alarm Reporting;
VII. AF-SEC-8: Audit;
VIII. AF-SEC-9: Security Recovery;
IX. AF-SEC-10: Management of Security.

These functions are from AF-SEC-1 to AF-SEC-10.

THREATS TO AN ATM NETWORK

ATM network will suffers a lot of threats. Few of the network threats are :

Eavesdropping
Eavesdropping is a threat in which attacker connects into the transmission media and gain unauthorized access to the data. It is one of the most common attacks to the network.

Masquerade Masquerade is a threat in which one person pretends to be someone else and by doing that, tries to gain access to information.

Service Denial
Service Denial occurs when on entity fails to perform its work and prevents other entities to perform its work.

Traffic Analysis
Traffic analysis refers to a threat that the hacker can get information by collecting and analyzing the information like the volume, timing and the communication parties of a VC
(Virtual Channels). Volume and timing can reveal a lot of information to the hacker even though the data is encrypted, because encryption won't affect the volume and timing of information.

Corruption of Information The transmitted data is altered, deleted, changed and delayed by an entity with a proper authorization.

Forgery Forgery refers to, when the fake data is sent and is claimed to have been received. The authenticated person's information must be changed to do this authentically.

SECURITY SERVICES

The ATM Security Framework

In figure 1 shows the Schematic representation of ATM security components in which each VPN (Virtual Private Network) has a switching device to enter into the network (Public Network). Between switching device & network there is a Crypto unit inserted. This crypto unit performs all the encryption & decryption work. Communication has to be between Network to Network or User to Network. For maintaining the security & privacy few functions should be maintained which we will discuss now.

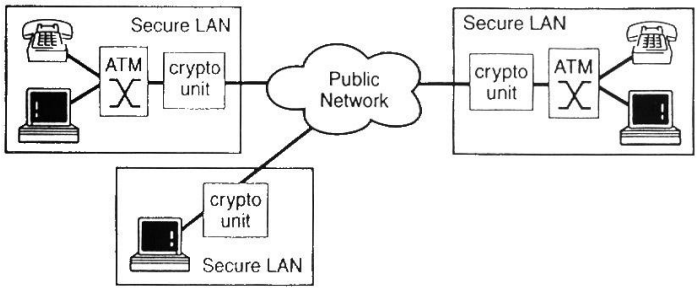

Figure 1: ATM Security Components (Schematic Representation)

AF-SEC-1 Verification of Identities

The ATM network shall support capabilities to establish and verify the claimed identity of any actor in an ATM network. In this function the basic authentication should be done. Authentication is done to avoid Masquerade. Few security services should be made available for this purpose.

- User Authentication
- Data Origin Authentication
- Peer Entity Authentication

AF SEC-2 Controlled Access and Authorization

The ATM network shall support capabilities to ensure that actors are prevented from gaining access to information or resources they are not authorized to access. The access control method decides whether the connection is authenticated or not. If the connection is not authenticated, it will not proceed further otherwise the connection will be initialized. It is very important for the multilevel secure ATM with trusted component.

AF SEC-3 Protection of Confidentiality

The ATM network shall support the capability to keep stored and communicated data confidential. Protection of confidentiality is used to protect user related information. The confidentiality service provides the protection for the disclosure of exchanged data to the unauthorized access.

AF SEC-4 Protection of Data Integrity

The ATM network shall support granting the integrity of stored and communicated data. Protection of data integrity is used to protect ATM network user related information. The integrity service ensures the correctness of exchanged data, insertion, deletion and modification of the new data.

AF SEC-5 Strong Accountability

The ATM network shall support the capability that an entity cannot deny the responsibility for any of its performed actions as well as their effects. Strong accountability means Non-repudiation. In this one has to prove that data has actually taken place. It is very important for everyone to be responsible for his work.

AF SEC-6 Activity Logging

The ATM network shall support the capability to retrieve information about security activities stored in the Network Elements with the possibility of tracing this information to individuals or entities. Activity logging is for controlling security policies. It is necessary to log information about security related events which occurs security relevant operations.

AF SEC-7 Alarm Reporting

The ATM network shall support the capability to generate alarm notifications about certain adjustable and selective security related events. In alarm reporting, security information is provided which provides information about security relevant events.

AF SEC-8 Audit

The ATM network shall support the capability to analyze and exploit logged data on security relevant events in order to check them on violations of system and network security. An audit is to test sufficiency of system control.

AF SEC-9 Security Recovery

The ATM network shall support recovery from successful and attempted breaches on security. A very frequent problem in cell encryption is the loss of cell. If cells are lost decryption will not be possible. Some modes operate on the algorithm of handling lost cells.

AF-SEC-10 Management of Security

The ATM network shall support capabilities to manage the security services derived from the security requirements listed above. Management of security comprises of important aspects of systems, which includes all activities to establish, maintain & terminate.

RESEARCH BACKGROUND

Crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators and this financial crime case rises repeatedly in recent years . A lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations. Passwords and PINs can be illicitly acquired by direct covert observation. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric authentication technology may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card.

Biometrics can be defined as a measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification. It is automated methods of recognizing a person based on a physiological or behavioral characteristic. It is a measure of an individual's unique physical or behavioral characteristics to recognize or authenticate its identity. Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost.

Fingerprint Biometrics

In the world today, fingerprint is one of the essential variables used for enforcing security and maintaining a reliable identification of any individual. Fingerprints are used as variables of security during voting, examination, operation of bank accounts among others. They are also used for controlling access to

highly secured places like offices, equipment rooms, control centers and so on .

The result shows that a substantial margin exists between the uses of fingerprint for identification over other biometrics such as face, hand, iris, voice, signature and middleware.

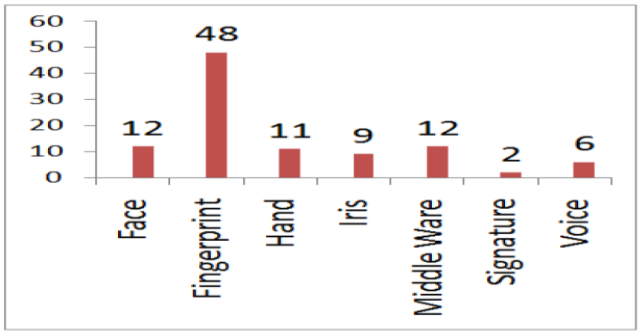

Figure . Comparative survey of fingerprint with other biometrics

The following reasons to the wide use and acceptability of fingerprints for enforcing or controlling security:

a. Fingerprints have a wide variation since no two people have identical prints.
b. There is high degree of consistency in fingerprints. A person's fingerprints may change in scale but not in relative appearance, which is not the case in other biometrics.
c. Fingerprints are left each time the finger contacts a surface.
d. Availability of small and inexpensive fingerprint capture devices.
e. Availability of fast computing hardware.
f. Availability of high recognition rate and speed devices that meet the needs of many applications
g. The explosive growth of network and Internet transactions
h. The heightened awareness of the need for ease-of-use as an essential component of reliable security.

CONCLUSION

This topic of security features in ATM proves that there is a requirement of strong security specification for ATM network and on the other hand there are many pitfalls and numerous problems. Authentication, confidentiality and data integrity are the important security framework that fulfills the user needs for secure network. So ATM safety and security provides strong protection of user security and safety and offers the new possibilities to make a network strong.

Biometric authentication technology using fingerprint identifier may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual.

REFERENCES :

1)www.google.com
2)www.w3schools.com