ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

Modern (ICT) Applications in Securing and Protecting ATM

Dr.Yasser Elmalik Ahmed Seleman

PhD in Computer Science (Excellent), Omdurman Islamic University, Sudan

Abstract: ATMs are a valuable extension of your financial institution, and they are viewed by customers as an essential part of consumer banking. Always available and ready to provide a variety of transactions, including cash. From our studies on the manual hacking of the ATM machine, I will agree with me that it affects the bank alone but using the software affects the individual or organization that owns the bank account.
We find that it's very necessary to identify the problem, assistance in finding solutions and highlight of the weaknesses point.
The paper reviews the risks faced by the ATM network connection, encryption and software .
Researcher shows some applications, software and systems that help to solve the problems of ATMs.

Keywords: **ATM**: Automatic Teller Machine,
ICT: Information and Communication Technology
E-banking: Electronic banking.

I. INTRODUCTION

Breakthroughs banks of the problems and risks that directly affect the national economy and lose customer confidence in the Bank evolved the more artistic and technical aspects of information and communications technology evolved crime and intrusions methods. The intrusions are a result of some of the gaps in computer and network security, uses the term gaps to refer to places weaknesses in these systems, which allows the attackers to the attack on the integrity of the system there is a set of obstacles and risks a major security gaps facing ATMs aimed at the paper to see the impact of information and communication technology in secure and protect ATMs and through a review of security gaps and weaknesses and work on them and fill these gaps by identifying security systems and modern applications that help secure and protect electronic banking through uses ATMs paper discusses models for some breakthroughs that has in many countries of the world and conferences discussed topics breakthroughs and to clarify the application of modern information and communication technology in secure and protect electronic banking.

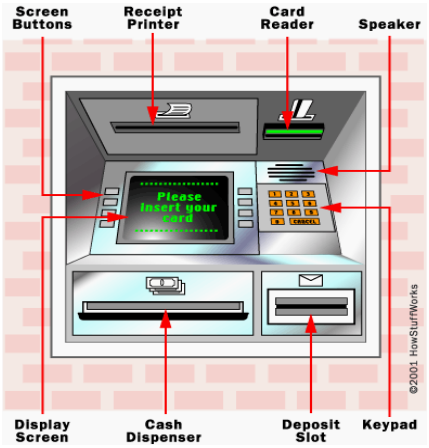

Figure (1) shows the device ATM components.

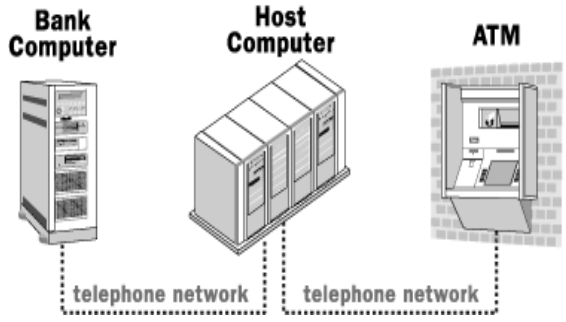

Figure (2) shows how to configure the computer network of the bank to achieve coherence between ATM machines within the confines of the building.

II. THE PROBLEM

There are a range of risks to the research was divided into:

1- Risks of operating systems ATM
2- Risks connected electronic banking networks
3- Risks encryption system
4- Risk software

The paper discusses these problems and weaknesses and solutions and review of models of some breakthroughs that has to ATMs

1- Risks of operating systems ATMIs the risk that for the first phase of the stages of the system which is the operational phase of ATM interfaces to deal with the client and those risks are the following items (): -
The user's operating system is Windows operating system, a weak system reliability, especially with regard to network management that use the Microsoft Windows operating system is in itself a major gap is not a defect in the system, but because the use of the base is very large, it

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

is here the discovery of loopholes and problems much faster than the other of the regulations.

2- Risks connected electronic banking networks

The security concerns in previous years is limited due to the fact that ATM uses a custom banking transactions - and is a secure network isolated from any external link but now an independent network became a unified network. And unified network of banks became vulnerable to intruders than ever before, and here lies the fundamental problem if one of the hackers managed to access the network from one bank the rest of the banks to be infiltrated.

3- Risks encryption system

Note from the researcher to the user's system DES encryption and after the study turned out for the researcher that this code has been virtually impenetrable.

4- Risk software

The client makes the process through ATM, what is being encrypted PIN for ATM card only while the rest of the information be sent as they are without encryption (card number - the customer's account, the type of operation, the amount withdrawn).

Also displayed on the screen the customer account after the completion of the process, and the big problems in the program that deals with the client and the user ATM card number printed on the receipt Alamlah.hzh gaps are at risk of exposure information in front of the penetrator and then may be used, for example, to change some of the transmitted data accuracy.

Summarize the actual problems: -

- Reliance on windows operating system instead of other regulations such as Linux or OS / 2
- Adoption of DES 3 encryption instead of DES
- Use TCP / IP protocols in the shared network.

Security vulnerabilities in the ATM in the electronic banking: -

- Unified network of banks have become more vulnerable than ever before to outsiders if hackers managed to access the network and one all banks are under his control and his behavior.
- Use Microsoft Windows system is a big problem in the ATM.
- DES encryption system was breached.
- Operations carried out by the client through the entire ATM are illustrated reports extracted from ATM (card number - the amount withdrawn - No. Abav- banks name - the remaining amount) and sometimes the account number. We find that encryption is the only user PIN.

Security systems that help secure and protect electronic banking through the use of ATMs:

- Software running on ATM surveillance system Solid core For APTRA is a program that prevents a person from tampering with any software on your ATM is not allowed to run the program except for authorized programs and protect these programs hard disk and memory so that unauthorized software will not work.
- Issuing ATM cards that feature contain a smart chip card Smart Chip make safer where he is providing these precautionary security measures. And raise the security protection of electronic services that are offered to customers through various electronic channels level, the application of a number of means and methods that achieve additional protection for customer accounts.
- Enable banks to identify customers on any operation conducted on their accounts by SMS received by the mobile phone numbers registered with the bank, in order to avoid direct and fast any potential scam may be on their accounts without their knowledge.
- The application of what is known as binary standard to verify the identity of an electronic system used to add more security to customers' E-banking transactions, which are made through the use of online banking.
- - The use of electronic signature beside PIN credit card and is based on the verification of personal trader based on the physical characteristics of individuals, such as fingerprint personal, human eye scan, facial recognition Bushra, the properties of the human hand to verify the tone of voice, and signature of the person and be sure to figure trader by inputting the information to a computer or modern methods such as capturing an accurate picture of the user's eye or his voice or his hand and is stored encrypted in a way that the computer memory of the then conformity.
- Network Virus device wall 300 employs information gathered from Trend Micro's global network of centers of anti-virus research, called Trend Labs SM at the ends of networks to help organizations detect intrusion and protection, control and eliminate them help Network Virus Wall devices institutions to improve operational flexibility through the alleviation security risks and facilitate the control of virus attacks, and reduce the time crashes systems.

Researcher Solutions:

1- Separation of ATMs from other networks (Physically- Virtually) with the building firewalls Systems.

2- Encrypt all data sent from the network.

3- Use encryption technology DES3 instead of DES.

4- Change the operating systems of the Windows operating system safer.

5- The use of other protocols is TCP/IP.

III. CONCLUSION

The results of the scientific paper:

-The paper reviews the risks faced by the ATM network connection, encryption and software.

-That in the past was used ATMs run abused non-Windows system devices to this there are no such problems now, because the Windows operating system in which many of the weaknesses, the network also contains a set of the most important risks of these risks are linked to the network internal link.

-Researcher shows some applications, software and systems that help solve the problems of ATMs.

-Coding of all statements sender from the network.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

-Use the technological coding DES3 instead about DES.

-Use Biometric Signature for the realization from the agent on the bodily characteristics.

-Coding report which requests her agent from ATM and lack of appearance (Card Number–Amount-Balance-Date).

Problems and risks of ATM researcher reached
Hardware and Software solutions will be discussed in the form of points Use the following security systems to protect ATMs and secure E- banking:

1- Protection system (Solid Core for APTRA) is programs that monitors and prevent tampering with the ATM program and not allowed to run any unauthorized programs.

2- ATM use smart cards that contain a smart chip (Smart Chip) to raise the level of protection.

3- Send SMS to confirm the CUSTOMER operations, and the client is here is to make sure that the process is carried out.

4- Application binary standard to verify the identity (electronic safety system uses
E- Banking transactions Balamlaean own through the use of online banking).

5- The use of electronic signature with the PIN number of the card to verify the client's personal (handprint, human eye scan, Signature Profile).

REFERENCES

1 - Kahate Atul (2004), Cryptography and Network Security, "User Attention Mechanism", pp. 303-304, III rd Edition, McGraw-Hill Publications.
2- Ciampa, Mark. Security + guide to network security fundamentals. – Boston: Thomson Course Technology, 2005.
3- Schwarz alder, R. (1999). Intranet Security. Database Magazine, 22(2), and 58.
4- Bandyopadhyay, T., Jacob, V., & Raghunathan, S. (2010). Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. Information Technology & Management, 11(1), 7-23

BIOGRAPHY

Dr. Yasser Elmalik Ahmed Seleman, Sudane
- PhD in Computer Science (Excellent) - Omdurman Islamic University - Sudan.
- M.Sc. In Information Technology - University of Newcastle- USA.
- M.Sc. In Information Technology - TheNational Ribat University .