A Framework for Safe Mode Alarm Reporting Technique (SMART) in ATMs

Madhu Sharma
Associate Professor and Research Scholar
S.S. Jain Subodh P.G. (Autonomous) College,
SGVU
Jaipur (Rajasthan), India

Vijay Singh Rathore
Director and Professor
Sri Karni College
Jaipur (Rajasthan), India

ABSTRACT

In current era, with the changes in financial transactional trends, the usage of Automated Teller Machines is excelling around the world to meet the customers need. The technological enhancement in this direction is supporting various aspects relevant to the smooth, safe and secure communication and functionality of Automated Teller Machine. But, in reality, the risk of hacking or robbing is also increasing even after the implementation of such security measures. Thus, the paramount requirement relevant to ATM is to maintain its security while accessing the cash and banking services through electronic communication network and its infrastructure. In this paper, we have introduced a specific security feature, to protect customers who are forced to withdraw cash from ATM on gun-point and under threat by criminals. In this paper, an innovative approach to handle the safety and security of customer through modifications in software and physical security system of the ATM, in such duress cash withdrawal has been proposed. The proposed framework is expected to safeguard customer's life risk and restrict the financial loss of customer as well as bank associated with ATM, along with the tracing of looted cash.

General Terms

Automated Teller Machine (ATM), Global Positioning System (GPS), Personal Identification Number (PIN), Asymmetric Digital Subscriber Line (ADSL), Virtual Private Network (VPN), Systems Network Architecture (SNA), Synchronous Data Link Control (SDLC).

Keywords

Safe Mode Alarm Reporting Technique (SMART), nano-chip, coerced attack, security plane, emergency PIN.

1. INTRODUCTION

Many machines and devices have been introduced, invented and implemented to meet out the need of speedy and automated monetary transactions. Automated Teller Machine (ATM) is one of among them. Since, ATM machines are installed at public locations, high security at user interface points along with the backend points, is a key requirement of this machine.

An authorized ATM user performs transaction through ATM's user interface, initiated with the entry of Personal Identification Number (PIN) issued by the ATM and banking authorities. The customer's entered PIN is then compared, authenticated and verified as per the bank's recorded PIN of reference, through the communication network setup to connect ATM and the banking financial network. In general, ATMs are connected directly to their server or host machines or ATM Controller through Asymmetric Digital Subscriber Line (ADSL) or through dial-up connection using a telephone or a leased line cable network. Leased lines require lesser time in connection establishment, but they are expensive in comparison to telephone lines in case of lesser traffic. Thus, high-speed Internet Virtual Private Network (VPN) connection is more preferable connection in all situations. Systems Network Architecture (SNA) over Synchronous Data Link Control (SDLC), TC500 over Asynchronous X.25, and TCP/IP over Ethernet are the lower layer communication protocols which are preferred for efficient communication with banking system. A basic ATM work model can be seen as shown in figure 1.

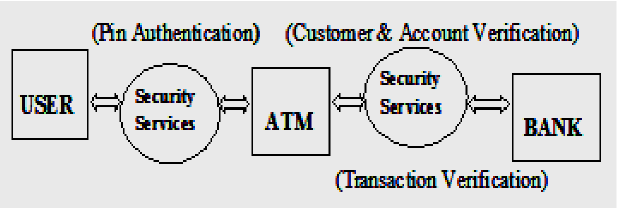

Fig. 1: Basic ATM Work Model

Research on various security mechanisms have been introduced and published, but in particular, still there is need of more work specifically in direction of putting a security check on the threat-based forced cash withdrawal or coerced cash withdrawal [1][2][3][4].

The proposed work area involves the development of a support system for a secret security check to assist in Physical security for a threat-based cash withdrawal through a genuine ATM card holder for any reason like demand of ransom money or blackmailing. As, the overall aim of the proposed study is to introduce and design a security system in ATM, which could report or raise a secret alarm to the ATM and banking authorities and the nearest local Police service in such duress cash withdrawal directed by criminals. Timely information about a crime and a speedy response of Police could surely help in an effective prevention of such crime and reduction in the intensity of harm or loss from such criminal activities. Thus, the proposed system is expected to be capable of delivering secret alarm in fraction of seconds to the security control room in coerced cash withdrawal situation. Here, the embedding of smart nano-chip within cash notes has been introduced, which get activated as the cash is withdrawn from ATM emergency repository and come in contact of natural light. This nano-chip is further associated with Global Positioning System (GPS) [5], enabled network connected with all ATM security relevant services, to assist in tracing the looted cash even after that is hidden far away from the ATM location.

2. PHYSICAL SECURITY PROBLEM RECOGNITION

Since, ATM is installed at public places, before its on-site installation, an intensive software or logical and hardware security testing has to be done, at public interface end and the backend computer systems, which is aimed to execute transactions with minimum machine, network failures or any other break down. Physical security threats and attacks, logical or software security threats and attacks and card frauds are the major categories of ATM security vulnerabilities. There are number of systems and techniques invented and installed to prevent ATM and customer from these various types of attacks.

Ram-raiding, plofkraak, tunnel digging, staff robbing, theft of cash from the ATM, duress or coerced cash withdrawal are few of the very common physical attacks seen in current scenario [4][7][8]. Out from these, though every attack consequences an irrecoverable financial loss to customer as well as associated banks, but the most unsafe and life threatening attack is a coerced cash withdrawal, which not only involves risk to the customer's and bank's finance, but also to his life and his near one's life. In situations, like demand for ransom money, blackmailing or some other threat by criminals, a genuine card holder of an ATM, withdraws cash due to an indirect gunpoint on himself or on his close relatives. Practically, it's not feasible as well very risky to deny for cash withdrawal in such critical situations.

Till now, there is no such security system implemented so far, which could provide the financial as well as physical safety and security of customers with the provision of assistance to police services to catch and trace criminals and looted cash even after they ran far away from the ATM location or hide that cash.

3. SAFE MODE ALARM REPORTING TECHNIQUE (SMART)

To provide safety and security to customers in duress cash withdrawal, to safeguard the cash withdrawn from ATM, and to trace the looted cash, we have proposed a Safe Mode Alarm Reporting Technique (SMART), to solve the above stated problem. The solution begins with the entry of special PIN number in case of emergency situation, which sends a secret alarm to police and ATM banking services, whereas at the same instant of time, ATM on receipt of this special emergency PIN, withdraws cash from emergency cash repository instead of withdrawal from general cash repository. A GPS enabled nano-chip [6] is embedded within the cash notes stored in such emergency repository. The nano-chip of cash notes will get activated as it will come in contact of natural light. Thus, when the customer would go for coerced cash withdrawal, the police will get activated on receipt of secret alarm generated on entry of emergency PIN entered by the customer under attack and in addition to this, the nano-chip of emergency notes would help and assist police in tracing the cash hid by criminals, even after the criminals ran far away with the looted cash. The SMART security framework could be seen divided as an Eight-Planar structure, as described below:

Plane 1: User Plane
Plane 2: ATM Plane
Plane 3: Security Plane
  Sub-Plane 3.1: Software Security Plane
    Sub-Plane 3.1.1: PIN Verification System
    Sub-Plane 3.1.2: Emergency PIN System
    Sub-Plane 3.1.3: Software Security Alert System
  Sub-Plane 3.2: Hardware Security Plane
  Sub-Plane 3.3: Network Security Plane
Plane 4: Banking Services Plane
Plane 5: Cash Repository Plane
Plane 6: Special Emergency Repository Plane
  Sub-Plane 6.1:Emergency GPS Enabled Cash Release System
  Sub-Plane 6.2: GPS Enabled Chip System
    Sub-Plane 6.2.1: Chip Activation System
    Sub-Plane 6.2.2: Chip Power Supply System
Plane 7: GPS Network Plane
Plane 8: Police Security Service Plane

A basic description stating the connectivity between the eight planes of SMART can be seen as shown in figure 2.

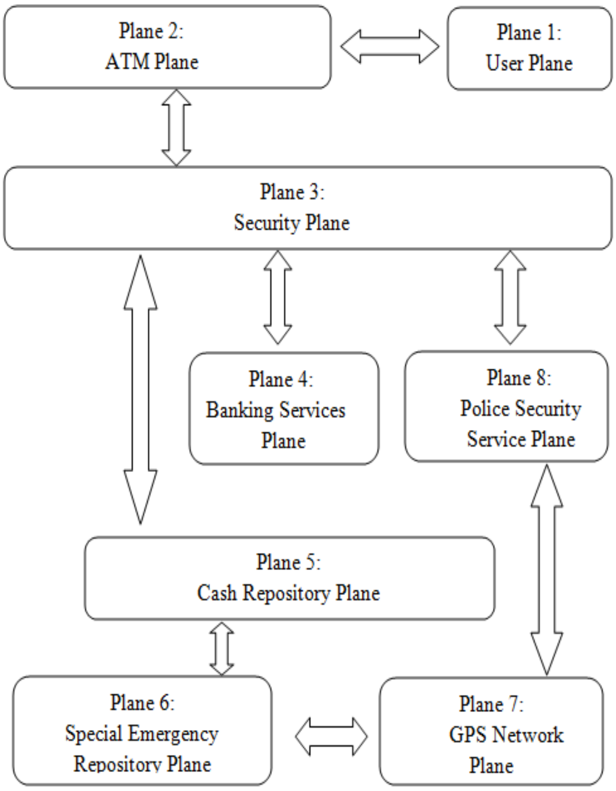

Fig. 2: Connectivity between different planes of SMART Framework

A basic description stating the connectivity between the sub-planes of Security Plane of SMART can be seen as shown in figure 3.

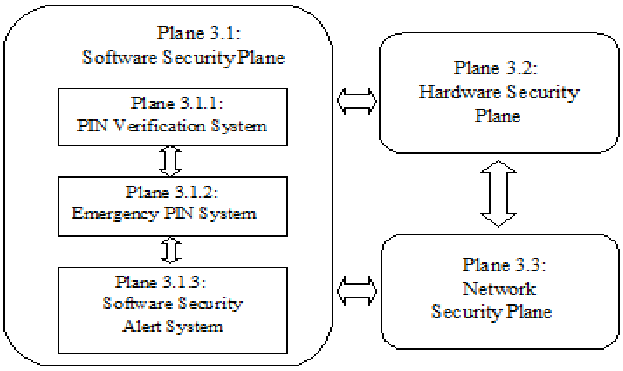

Fig. 3: Connectivity between Sub-planes of Security Plane

A basic description stating the connectivity between the sub-planes of Special Emergency Repository Plane of SMART can be seen as shown in figure 4.

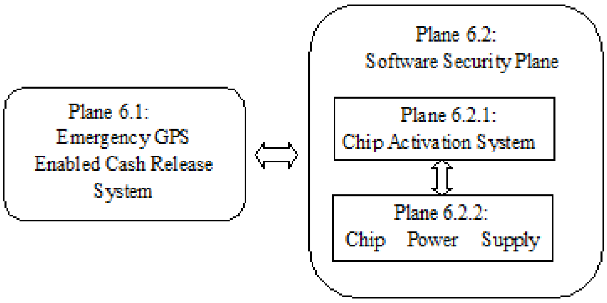

Fig. 4: Connectivity between Sub-planes of Special Emergency Repository Plane

The framework for Safe Mode Alarm Reporting Technique (SMART) has to be developed by using suitable technological support and programming language.

4. CONCLUSION AND FUTURE WORK

In this paper, the framework for Safe Mode Alarm Reporting Technique (SMART) in ATMs aimed for the strengthening of the Physical security system specifically for coerced or duress cash withdrawal by the customers due to indirect gun-point or threat to their life or their near ones has been proposed. The SMART system has to be developed and implemented for the safety and security of customers, banking authorities and provides assistance to the Police services and thus strengthens the ATM's security system. The proposed technology is expected to be utilized in tracking of other precious things like jewellery or expensive gadgets.

The future plan includes the development and implementation of the SMART system for ATM, with its performance analysis.

5. REFERENCES

[1] D Teitelbaum, "Violent Crime At ATM", The Business Lawyer, 1990 - JSTOR, Vol. 45, June 1990.

[2] Schreiber, Francis B., "ATM Crime & Security Newsletter, Vol. 2, No. 2" (1992). [Online], Available: http://repository.stcloudstate.edu /atmcs/4.

[3] Sharma M., Rathore V.S., "An Investigative Study on Physical Security and Reporting Mechanisms in ATM", OORJA International Journal of Management & IT, ISSN NO: 0974-7869, Volume 16,/No. 1, 2014 (In Press).

[4] Sharma M., Rathore V.S., "A Review on Security and Reporting Mechanisms for Coerced Cash Withdrawal from ATM", Unpublished.

[5] Pratap Misra and Per Enge, "Global Positioning System: Signals, Measurements and Performance", Second Edition, 2006, #2500-2.

[6] CP Poole, FJ Owens, "Introduction to nanotechnology", Cambridge Univ Press, 2003.

[7] Tim Prenzler, "Strike Force Piccadilly and ATM Security: A Follow-up Study", Oxford Journals, Volume 5, Issue 3, 2011, Pp. 236-247.

[8] Samuel H. Bosch, Jonathan H. Bosch, "Remote currency dispensation systems and methods", US8332321, Dec 11, 2012.