Chapter 13
On The Design of Secure ATM System

Lawan Ahmed Mohammed
King Fahd University of Petroleum & Minerals, Saudi Arabia

EXECUTIVE SUMMARY

Over the past three decades, consumers have been largely depending on and trust the Automatic Teller Machine, better known as ATM machine to conveniently meet their banking needs. ATM is a data terminal, it has to be connected to, and communicate through, a host processor. The host processor may be owned by a bank or any financial institution, or it may be owned by an independent service provider. Moreover, an ATM can support multiple ATM cards owned by different financial institutions or banks. Most host processors can support leased-line or dial-up machines. However, despite the numerous advantages of ATM system, ATM fraud has recently become more widespread. Recent occurrences of ATM fraud range from techniques such as shoulder surfing and card skimming to highly advanced techniques involving fraudulent mobile alerts, and account takeover via stolen information and call centers, software tampering and/or hardware modifications to divert, or trap the dispensed currency. In this chapter, we provide a comprehensive overview of the possible fraudulent activities that may be perpetrated against ATMs and investigates recommended approaches to prevent or deter these types of frauds. In particular we develop a model for the utilization of biometrics equipped ATM to provide security solution against must of the well-known breaches associated with the current ATM system practice.

INTRODUCTION

An automated teller machine (also known as Cash Machine), is a computerized device that provides the customers of a financial institution with the ability to perform financial transactions without the need for a human clerk or bank teller. Most modern ATMs identify the customer by the plastic card that the customer inserts into the ATM. The plastic card can contain a magnetic stripe or a chip that contains a unique card number and some security information, such as an expiration date

DOI: 10.4018/978-1-60960-015-0.ch013

and card validation code (CVC). When using an ATM, customers can access their bank accounts in order to make cash withdrawals (or credit card cash advances) and can check their account balances as well as purchasing mobile phone prepaid credit, paying bills and so on. ATM, was first introduced in 1960 by City Bank of New York on a trial basis, the concept of this machine was for customers to pay utility bills and get a receipt without a teller (NetWorld Alliance, 2003). It allows financial institutions to provide their customers with a convenient way, round the clock, to carry out varying transactions which included withdrawal of funds, made deposits, check account balance, and later on included features to allow customers pay bills, etc. There was no need for a cashier to be present or for a customer to physically visit the financial institutions premises to carry out such transactions. ATMs are not only located at banks but also increasing numbers of businesses, especially retailers for both customer convenience and a new revenue stream. Similarly this will reduce the cost of transactions as transactions that normally would require a bank employee's time and paperwork can be managed electronically by the customer with a card. A global ATM market forecast research conducted by Retail Banking Research Limited (RBR, 2010) shows that there are 1.8 million ATMs deployed around the world today and the figure is forecast to reach 2.5 million by 2013. In a similar research by European ATM Security Team (EAST), the total number of ATMs in Europe continues to show year on year growth as shown in the Figure 1. In addition, there are 84,500 ATMs in Russia, which are not shown in the figure.

Authentication methods for ATM cards have little changed since their introduction in the 1960's. Typically, the authentication design involves a trusted hardware device (ATM card or token). The card holder's Personal Identification Number (PIN) is usually the only means to verify the identity of the user. Further, many existing designs based on such devices use a delegation technique whereby the device acts on behalf of the user by deploying its strong cryptographic capability. Typical ATM authentication process is depicted in Figure 3.

However, due to the limitations of such design, an intruder in possession of a user's device can discover the user's PIN with brute force attack. For instance, in a typical four digits PIN, one in every 10,000 users will have the same number.

As ATM card becomes widely used, it produces new kinds of crime, mostly derived from the security pitfalls of the magnetic media. The data in the magnetic stripe is usually coded using two or three tracks. The standard covering this area is ISO 7811. The technique for writing to the tracks is known as F/2F. The reason is that it is not that

Figure 1. Number of ATMs in Europe (excluding Russia) from 2005 - 2009