Threat to Automated Teller Machine

Mohammad Jabed Morshed Chowdhury

Automated Teller Machine (ATM) allows an authorized cardholder to conduct banking transaction without visiting a branch. It is popular for its convenience to the customers, and cost-effectiveness for the bank. Though there is a common understanding that ATM is secured but several security incidents have shaken the client's confidence. Security attacks are main tow types, physical and technical. This article is hoped to describe a general picture of ATM crime, help ATM owner understand threats facing their ATM security, raise bank and cardholder awareness about risks faced when using ATM. Criminals use different technical methods to steal the wealth of others. Here few important security risk and attacks will be discussed.

Card Skimming

In credit card skimming schemes, thieves use a device to steal credit card information in an otherwise legitimate credit or debit card transaction. For example, credit card skimming devices are often placed on ATMs or even held in the hands of waiters and store employees. When a credit card is run through a skimmer, the device stores the credit card information. Thieves use the stolen data to make fraudulent charges either online or with a counterfeit credit card. In the case of ATM and debit cards, thieves withdraw cash from the linked checking account. Credit card skimmers are even popping up on Redbox movie rental kiosks. Victims of credit card skimming are often unaware of the theft until they receive a billing statement or overdraft notices in the mail.

Magnetic card information details are compromised by a disguised card reader known as skimming device which is normally installed in front of card reader entry slot or some ATM room-door lock. Skimming is by far the most popular method of ATM network attack, accounting for over 80% of ATM fraud, or around $800 million. The main reason makes it popular is high ROI from this attack.

In card skimming, the criminals use a fake card reader to read the information in the card and use spy camera or PIN pad overlay to steal the PIN numbers.

Spy camera: Install a fake advertising box or mailbox with small convert camera inside to observe PIN entry. With the wireless technology developing, the captured PIN can be real-time transited to allow producing counterfeit card immediately, compared with old stand-still capture method.

PIN PAD Overlay: Place a false plastic PIN pad on the original one. Transfer or store PIN when customer enters the correct PIN number in the system.

The Winnetka bank branch reported an ATM skimming device, in which 25 customer bank cards were swiped. Not all of the customers' accounts were compromised, O'Herlihy said at the time. A Romanian man who stole hundreds of thousands of dollars by placing skimming devices on area bank machines was sentenced to 23 months in prison, plus three years of federal supervision.

Cash is trapped by false withdrawal shutter

Cash Trapping

Criminals fix a false withdrawal shutter slot, causing cashes to get stuck inside when customers attempt to do a withdrawal. The customer leaves assuming that the machine is out of order or goes inside the bank to report the incident and the thieves return to retrieve the notes.

Two men have been arrested for allegedly trying to steal cash from bank customers by tampering with an ATM in Chingford. They placed a small plastic strip in front of ATM so that when cash is ejected it becomes stuck City of London Police entered a flat in Harrow; arresting two Romanian men aged 23 and 25. They found six cash traps, which are placed over a cash machine and use a metal bar to prevent the customer receiving the money. There were 1,738 recorded incidents in three months.

Software and Network Attack

Instances where thieves use specially designed malware to infect the machines or hack into the ATM's internal data networks to steal the account information. The first lunched malicious attack was detected in 2008 in Russia. Till now it has spread outside Europe, and reported incidents in Latin America, Romania, even in Vietnam.

A new banking Trojan with infection rates similar to SpyEye and Zeus in some regions has emerged. The Sunspot Trojan has already been linked to instances of fraudulent losses, according to transaction security firm Trusteer. The Windows-based malware is designed to carry out man-in-the-browser attacks, including web injections, page-grabbing, key-logging and screen shooting.

Solution: Biometric Authentication

Biometric authentication has become more and more popular in the banking and finance sector. The use of biometric technologies at ATMs, POS terminals and online-banking is currently only used in very small projects with few users except in Japan. Since August 2005 Japanese banks have had to replace customer losses from improper cash withdrawals by law unless culpable behavior can be proved against the customer. Actually there are more than 40 Japanese banks using palm-vein recognition at more than 19,000 ATMs. More than 600,000 customers of the Tokyo Mitsubishi Bank UFJ are using biometric verification at ATMs. Another bloc of financial companies, which have adopted a technology that uses the pattern of veins in a person's fingertips, including Sumitomo Mitsui Banking Corp., Mizuho Bank and Japan Post, will also accept interbank ATM users. The Columbian Bancafe bank is introducing fingerprint scanning across its entire ATM network, designed by NCR Corporation. In 2007 the Brazilian "Bradesco" bank will implement this system with 25,000 ATMs. The difference between biometrics in the banking and finance sector and other applications is that the storage of identification information in a central database is in conflict with data privacy protection laws. The better solution would be a verification in which the biometric data can be stored encrypted on a smart card.

At the time of transaction fingerprint image is acquired at the ATM terminal using high resolution fingerprint scanner. Security measures at banks can play a critical, contributory role in preventing attacks on customers. These measures are of paramount importance when considering vulnerabilities and causation in civil litigation. Banks must meet certain standards in order to ensure a safe and secure banking environment for their customers CJ