Best Practice for ATM Security

Overview of ATM security situation, forecast, and best practices

GRGBanking Equipment (HK) Co., Ltd
2011/5/27
About GRGBanking

GRGBanking is a leading currency recognition and cash processing solutions provider in the global market. We have been specialized in the development of Automatic Teller Machine (ATM) for financial institutions and retailers, Automatic Fare Collection (AFC) equipment for railway or metro systems, as well as other currency recognition and cash processing equipments for over 20 years. Besides, our various multi-channel software solutions and services cover the needs of the financial industry, retail, transportation, payment, self-service, cash automation, cash management outsourcing and managed services, customized for different customers around the world.

In 2007, GRG set up the ATM security research institute dedicating to providing the latest security information, product, training and consultant services.

For contacting GRGBanking or general enquiries on security matters, please contact following details:

Email: ATM@grgbanking.com
Mail address: 9 Kelin Road, Science City, Luogang District, Guangzhou, China 510663
Tel : +86 (0)20 8218 8379
Fax: +86 (0)20 8218 9024
Table of Contents:

Part 1 Summary ................................................................. 4

Part 2 Types of ATM attack ......................................................... 5
    Physical attack: ........................................................................... 6
        1.1 Ram-raid: ................................................................. 6
        1.2 Cutting: ................................................................. 7
        1.3 Explosive: ............................................................. 8
    ATM fraud: .............................................................................. 9
        2.1 Card skimming: .......................................................... 9
        2.2 Card trapping: ......................................................... 11
        2.3 Cash trapping: .......................................................... 13
        2.4 Transaction reversal: .................................................... 14
        2.5 Deposit Fraud: .......................................................... 14
    Software and network attack: .................................................. 14

Part 3 Forecast for 2011 ............................................................ 15

Part 4 Countermeasure ............................................................. 16
    Recommendation for Banks ..................................................... 16
    Recommendation for ATM manufacture ..................................... 20

Part 5 Conclusion .................................................................. 21

Part 6 GRG Security solutions and services ................................. 22
    Fraud Prevention Solution ..................................................... 22
    Physical Protection Solution .................................................. 22
    Software and network security solution .................................... 22
    Security Accessories ............................................................. 22

References ............................................................................ 23
Part 1 Summary

Today, ATM has become an irreplaceable communication and service channel between banks and cardholders due to its fast, convenience and human resource saving advantages; you can easily find ATMs in branches, convenience stores, airports, and shopping malls. But with the prosperity of installed ATM, the reported ATM crime also has been dramatic grown (Figure 1), causing big loss (Figure 2) for cardholders and banks. To build safe ATM use environment, maintain bank’s brand image and protect bank assets, all the involved organizations, institutions, and persons must research, develop and takes measures to meet the challenges faced by ATM crimes.

![Attacks against ATM by number of incidents](image)

**Figure 1: ATM related attacks. Source: EAST**
This paper 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, and provide a set of advice and countermeasure on how to identify and fight against ATM attack.

This document can not cover all the facets associated with ATM attack, forecast, and countermeasure, but should be taken as a useful guidance aiming to increase public awareness of ATM security.

**Part 2 Types of ATM attack**

There are a variety of ATM attacks because it is such an attractive target. We can not list all the types, but highlights some popular ones.

Basically, there are three basic types of ATM attacks:

- Physical attack: Brute force attack to ATM machines with the intention of gaining access to cash within the safe
- ATM Fraud: Theft of bank card information.
- Software and network attack: Theft of sensitive information or controlling ATM spew out bills automatically.

**Physical attack:**

This kind of crime is active in Euro-American, Russia, and Africa, and is also showing a trend of escalation in Asia-pacific area. According to a recent report release by EAST, a total of 2,062 physical attack incidents in Europe were reported in 2010.

**1.1 Ram-raid:**

The common method is physically removing ATM from premise with vehicle or heavy truck, and then steal cashes with opening safe by force.

*A vehicle failed to steal an ATM*
An ATM was brute removed from a convenience store

Recent incidents:

In UK, it was reported that on May 11th, Ram-raiders who stole a cash machine from a Bingley shop caused about £30,000 of damage after repeatedly driving a car into the shutters. The masked burglars towed away a cash machine using a 4x4 vehicle.

Police in Salzburg said on April 9th that a cash terminal was ripped out of its foundations. The unidentified gang most likely used a chain to remove the heavy device in what has been the 25th failed or successful attempt to steal a cash terminal in Austria in the past 14 months.

1.2 Cutting:

Use rotary saw, blow torch, thermal lance, and diamond drill to brutally open safe gaining direct access to cash.
Recent incidents:

Police in Neunkirchen, Lower Austria, announced in April that one automated teller machine (ATM) was cut open by the felons with special tools, which cause 20,000 Euros loss.

A man carrying multiple blowtorches broke into the ATM drive-through building on 2nd March, causing a small fire in the process. There is damage to the interior of the ATM, fire damage as well as torches were located inside but no description of how much money the burglar may have made off with.

1.3 Explosive:

Criminals use solid explosive material or combustible gas to explode with intent of gaining access to the security enclosure. The most serious is explosive not only causes cash loss, but also facilities and environment damage or casualties.
Recent incidents

One man involved in the high-risk robbery which involved pumping flammable gas into a Bank of Queensland ATM at Geebung was arrested in May. The explosion allowed them to steal $118,000 from the money cartridges inside the machine\textsuperscript{535}.

Thieves have detonated a gas bottle in order to rob an ATM machine in the small locality of Mihovljani in Zagorje. The thieves blew up the ATM machine during the night, hours after it had been filled with cash. The ATM machine was also destroyed\textsuperscript{532}.

ATM fraud:

2.1 Card skimming:

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 in 2008 full year\textsuperscript{573}. The main reason makes it popular is high ROI from this attack.
Recent incidents:

The same Winnetka bank branch reported an ATM skimming device in December 2010, 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 Monday to 23 months in prison, plus three years of federal supervision.

In April, a Twenty-eight-year-old Viktor Kafalov admitted Wednesday in U.S. District
Court in Newark that he conspired with others to install the so-called skimming devices on ATMs at Valley National Bank branches in Nutley and Belleville. He and his accomplices took more than $278,000 from customers’ accounts.\(^{[10]}\)

### 2.2 Card trapping:

Trap or jam the card by placed wire, tapes or other mechanism in the card entry slot.

![Lebanese Loop, commonly used for card trapping](image)

**Recent incidents**

In several hotspots of borough, more than 30 residents have reported thieves stealing their money or cards at cash machines in less than three months the May. The thieves have used techniques such as the “Lebanese loop”, a plastic strip they insert into the cash machine to capture bank cards.\(^{[11]}\)

In Thailand, a criminal placed toothpicks in ATM card slots to trap the cards of people who tried to withdraw money from the machines. Police do not know how many millions he has allegedly stolen from ATM machines over the years. But they say Mr Wasan’s bank records going back three months suggest he was making at least 150,000 baht a day, allegedly from ATM thefts.\(^{[12]}\)

Instead of the theft card information in skimming crime, card trapping is actually intended to physically capture card. But no matter trapping or skimming, criminals
have to capture customer’s PIN. Several different methods are used by fraudsters to capture PIN:

- **PIN PAD Overlay**: Place a false plastic PIN pad on the original one and text PIN when customer enters.

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

- **Powerful telescope**: Scammers observe PIN entry activity and judge PINs from finger movement during operation.

- **Honey trap**: Place an false advertisement, notice or service hotline number
hocusing to get PIN by “Help” or “recommendation”

2.3 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.¹³

Cash is trapped by false withdrawal shutter

Recent incidents:

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.

2.4 Transaction reversal:

Transaction reversal scams use certain methods to create an error condition at the ATM so as to re-credit amounts withdrawn to the account. Sometimes thief removes only portion of the bills from the dispensing tray. They let the ATM “Time out” and retract the rest.

2.5 Deposit Fraud:

Deposit fraud includes various criminal techniques from making false deposits, trapping deposits through skilful manipulation of ATM with the deposit function.

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.

Recent incidents:
A former Bank of America programmer has been sentenced to 27 months in jail for unauthorized access to the bank’s computer system. He was hired by BofA and had been assigned to work on a project involving the bank’s ATM system. From March 2009 to October 2009, Caverly knowingly and with intent to defraud exceeded his authorized access by gaining access to one or more protected [BofA] computers and deployed a malicious computer code to select [BofA] ATMs.  

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 (a feature that captures screenshots of the location of a mouse as a user types his/her password on a virtual keyboard).

Part 3 Forecast for 2011

1. Card skimming will be No.1 threat;

Even the reported skimming incidents is falling down, card skimming will be the NO.1 threat to ATM security. The main reason is the maturation of skimming business. Criminal can easily buy skimming device of more sophisticated technology with cheaper price. Also wireless component widely merging allows thieves to fast produce counterfeit card throughout the world and make money immediately, which also because they are not easy to be caught. We also should know that high ROI makes criminals are eager to this kind of crime. In some countries even they are arrested and prosecuted, the punishment is far lower than brute crime. Another fact we have to know that card skimming occurs globally, with EMV migration steadily being pushed, parts of the world that are not EMV compliant will be the “severely afflicted area.”
2. **Malicious and Trojan will bring big threat to ATM:**

Software and network attacks, especially malicious attacks are getting more sophisticated, which often implemented by criminal organizations with strong software engineering capabilities. Most malicious is able to remain silent, which may be cause big loss but undetected by banks. The most serious problem is we don’t have enough measures or detection tools to prevent it.

3. **The number of explosive will be growing:**

Although physical attacks have fallen in the past year, the total number of reported explosive and gas attacks has gone up. The main reason is gas explosive provides fast access to safe than traditional safe-breaking method. Also this kind of crime is easy to implement. Maybe only one bottle of gas and one lighter can bring big money.

**Part 4 Countermeasure**

**Recommendation for Banks**

Deploy layered security rules to protect ATM physically and software, such as installing EPP shield, installing monitoring system and security software. Provide a safety environment for cardholders.

<table>
<thead>
<tr>
<th>Category</th>
<th>Recommendation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM Fraud Prevention</td>
<td>Physical</td>
<td>Anti-skimming devices are able to prevent skimming devices from capture card information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PIN PAD Shield can shield onlooker’s view preventing PIN from compromised when entered.</td>
</tr>
</tbody>
</table>
Consumer awareness mirror is a means to be aware of surroundings.

Upgrade card reader with “jitter” function.

Some anti-skimming solution provides fascia scanning function to detect if any foreign objective attached.

Biological recognition system make PIN compromise impossible.

Management

Educate cardholder how to choose a safe ATM, how to check physical surroundings, how to check ATM, and how to do when suspicious event happens. For detailed information, please find GRG released Safety tips.

Work out ATM security check list and Formulate patrol inspecting system. Scheduled checks of ATM branch, ATM surrounding

Physical attack Protection

Physical measure

Audible alarm could help dissuade a thief from following through with their ATM theft.
Intruder system can detect if any suspicious event happens. Thermal sensors, seismic sensors, and explosive detector are the basic requirement in this system.

Monitoring system should view the ATM and record suspicious events, also should be remotely monitored by monitor center.

Installation: choose a safe place to install ATM; visibility from the road is main factor. Well-constructed base is very important which make ATM securely fixed to floor by a minimum of four anchor bolts.
<table>
<thead>
<tr>
<th><strong>Barriers:</strong></th>
<th>anti-ram bollards, kerbs or similar furniture's can be installed in front of ATMs. Also some barriers that wrap around ATMs in order to make lassoing or lifting the ATM more difficult.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lockers:</strong></td>
<td>Lockers, known as anti-theft mechanism, could make physically removing ATM very difficult by being attached to the main body of the ATM.</td>
</tr>
<tr>
<td><strong>Cash degradation system:</strong></td>
<td>Cash degradation system could immediately dye notes when activated in case of ATM being moved or attacked. It is also an excellent means to deter cash theft or robbery for CIT by providing end-to-end security.</td>
</tr>
</tbody>
</table>
Security accessories, such as tamper evident label and lock, cable ties, can easily find if any unauthorized access to safe and cassettes.

<table>
<thead>
<tr>
<th>ATM network security</th>
<th>Management</th>
<th>Work out ATM security check list and formulate patrol inspecting system. Scheduled checks of ATM branch, ATM surrounding</th>
</tr>
</thead>
</table>
| Security policies deployment | Security policies deployment | USB ports management  
Use complex logon password.  
Install Anti-virus software.  
Install patches from vendors. |

<table>
<thead>
<tr>
<th>Management</th>
<th>Employee education</th>
</tr>
</thead>
</table>

**Recommendation for ATM manufacture**

1. Pay more attention to ATM security: Fully consider meeting all security standards in ATM field when early in the design process, such as UL291 standard, PCI-EPP, and ensure ATM has a variety of security features of crime prevention and protection before delivery.
2. To actively develop detection software, security solution and security service.
3. Work closely with banks to put countermeasure of ATM security prevention.
Part 5 Conclusion

From the first ATM being installed in the world till now, ATM has gradually become a target of crimes due to it providing direct access to safe and cash. While with the constantly evolving of reported ATM crime, ATM industry has begun to pay attention to the safety of ATM, even cardholders. We believe under the joint and sustained effort of ATM suppliers, banks, and related organization, a more safe and convenient transaction platform and channel will be built up eventually.
Part 6 GRG Security solutions and services

ATM security is the prime concern of financial institutions from the beginning of deploying. GRG has set up the ATM security research institute dedicating to providing the latest security information, product, training, and consultant services, which is the leading security institute with over hundreds of engineers and researchers. From ATM fraud prevention solution-to-physical protection solution and software and network solution-GRG provides overall and multi-layered solutions of financial institute.

Fraud Prevention Solution

PCI EPP: tamper resistance, triple DES encryption
Card reader: EMV certified, jitter, ERCS
Consumer awareness mirrors
Biometrics Identification technology
PIN PAD shield
Separate retract and divert cassette compartments
Fascia and gate design
Encrypted communication
Identity NoteTrace
Transaction image capture for surveillance

Physical Protection Solution

UL291 and CEN rated safe
Mechanical and electronic locks

DVR surveillance system with sensors and alarm network
GSM-Based alarm network
Local siren
Ink-dye system
Anchoring system

Software and network security solution

SECOOne: comprehensive terminal security system
FEEL View Express: Multi-Vendor ATM Monitoring System

Security Accessories

NON-residue Tamper Evident label
Frangible paper seal
Pull Tight Security Seal
Master Key System
Tamper Indicative Padlock
ATM Safety Tips Decal

For more information on solution details and security aspect, visit us at www.grgbanking.com or contact at +86 (0)20 8218 8379
References

1. http://www.thetelegraphandargus.co.uk/news/9016638.Ram_raiders_smash_their_way_into_minimarket/
10. http://online.wsj.com/article/APca7cfbaf0fd445ae9a914312aeaf1dd.html
13. ATM Crime: overvie of the European situation and golden rules on how to avoid it, ENISA, August 2009
16. A Risk-Based Approach to ATM Security: Best Practices and PCI Compliance,
www.co-opts.org


19. www.bankinfosecurity.com

20. WWW.atmia.com

21. www.atmmarketplace.com