ATM SECURITY

EXPLAINING ATTACK VECTORS, DEFENSE STRATEGIES AND SOLUTIONS

An NCR white paper

NCR

SECURE

Each day there are new reports of attacks on ATMs around the world and criminals continue to vary and modify their attacks and attempt to bypass the protections in place. The sophistication of the criminal's tools and methods have also increased.

Understanding all of the various attack vectors and crimes can seem complex and overwhelming at times but looking out over the landscape, a broader attack type and structure emerges. The attacks fall into three general categories:

1. **Identity Theft**
2. **Logical Theft of Valuable Media**
3. **Physical Theft of Valuable Media**

This document will describe the available attack techniques that are used, illustrate how the attacks evolve as an arms race develops between the defenders and the attackers and also describe effective strategies that can be used for each category to win the battle.

TABLE OF CONTENTS

1 IDENTITY THEFT

2 LOGICAL THEFT OF VALUABLE MEDIA

3 PHYSICAL THEFT OF VALUABLE MEDIA

1. IDENTITY THEFT

Identity Theft refers to the category of crimes that capture the data used by a consumer to authenticate themselves at a Self-Service Terminal to enable their financial services.

The most frequent attack vectors in this category include Card Skimming, Card Trapping, and Card "Sniffing."

A card skimming attack is defined as 'the unauthorized capture of magnetic stripe information by modifying the hardware or software of a payment device, or through the use of a separate card reader.' Skimming is often accompanied with the covert capture of customer PIN data. Armed with this information, the fraudsters create dummy cards and raid the customer's account.

The devices used in Card Skimming Attacks fall into a variety of categories. However, they all have in common the use of foreign electronic devices to read and capture data from the card's magnetic strip being used to activate the ATM transaction.

The most common forms of Card Skimmers are:

- Bezel Mounted Card Skimmers: These are devices that are made to fit over the existing bezel of the ATM. They appear to look like the authorized bezel.
- Insert Skimmers: Are small electronic devices, designed to fit inside the card reader. Due to the nature of their size Insert Skimmers are nearly impossible for the layman to detect.

Card Skimming remains, by far, the most frequent form of ATM attack and currently represents nearly 95% of all losses.

Card skimming frequency remains high even in markets where EMV has been fully deployed and chip cards are used. This is because the vulnerability lies with the magnetic strip that is on the card. As long as the magnetic stripe remains on the card and the card is passed through any device that reads the magnetic stripe data, there will be the risk of card skimming.

These forms of card skimming can be effectively prevented through the deployment of comprehensive anti-skimming solutions. Card Skimming has become something akin to an arms race. Historically, there has been a vicious cycle between the criminals and the ATM manufacturers and companies who sell card skimming devices. A solution is developed in response to a form factor of the skimmer, the criminals then go back and vary the skimmer to bypass the solution, making that current solution vulnerable. The ATM deployers are then is forced to seek out new solutions and the pattern then repeats itself.

NCR's strategy to card skimming solutions takes a different approach to this challenge.

First, effective anti-skimming must contain the ability to both detect the presence of a skimmer, attempt to disable the skimmer and provide notification to the ATM operator that skimming is occurring at that ATM. All of these components are included in NCR Skimming Protection Solution (SPS).

SPS provides sophisticated detection and allows the device to note when any item is placed in or around the card bezel. On motorized card readers, NCR provides jamming capabilities to effectively disable the skimmers capability to capture the card information.

SPS is built with a field programmable framework. This allows you the ability to enhance functionality should criminals modify their attacks. SPS also can be configured to be highly integrated into the ATM monitoring system, allowing ATM operators to receive up to 16 different alerts and notifications. With this level of detail, the ATM operator can determine how they respond to the attack including having the option to take the ATM out of service.

Identity theft is also carried out by other attack types.

Eavesdropping Attacks: In this attack, a hole is made in the ATM or access gained to the top box of the ATM. Electronic hook ups are then attached directly to the card reader to attempt to capture card and PPIN details. The eavesdropping attacks can be prevented by retrofitting existing ATMs with physical barriers around the internal card reader. NCR has an anti-eavesdropping kit that offers an easy and inexpensive protective measure. Further, NCR is working closely with our card reader manufactures on new designs for card readers that add further protection. NCR's Skimming Protection solution also provides enhanced protection around the card bezel in the form of drill plates which make it more difficult for the criminal to cut a hole in the ATM in order to place an eavesdropping device on the card reader.

Network sniffing attack: With this approach the criminals attempt to capture the cardholder information as it is being sent from the ATM to the ATM switch or host. This is done by attaching a device onto the network connection cables. There are several layers to the defence strategy to protect against network sniffing attacks.

First, the easiest and immediate defence would be to add a physical barrier to prevent any unauthorized access to the network cables. This can be by shielding the wires in a conduit, or behind the wall. More sophisticated solutions would be to deploy secure communication connections. NCR recommends the implementation of TLS encryption. Encrypted wireless communication can also be deployed in addition to the TLS to provide additional protection against this form of attack.

Skimming Category	Description	Recommended Solutions
Bezel Overlay	Manufactured overlay containing a skimmer which fits a specific ATM model	SPS with Skimmer Detect and Alert Monitoring
Bezel Insert	Manufactured insert containing a skimmer which fits a specific ATM model	SPS with Skimmer Detect and Alert Monitoring
Card Read Tap - Destructive (Eavesdropping)	Attacks that penetrate the ATM fascia or cabinet with the intention of providing direct access to the card reader	SPS with Skimmer Detect and Alert Monitoring, plus Anti-Eavesdropping Kit
Card Read Tap - Non-Destructive	Attacks that involve opening the ATM cabinet with the intention of providing direct access to the card reader	ATM location security, appropriate cabinet locks, encrypted USB
Differential Skimming (Stereo Skimming)	Using twin read heads connected in differential mode to negate the effects of a jamming signal	SPS with Skimmer Detect and Alert Monitoring
Deep Insert Skimmer	A device placed inside the card reader using the card slot as the entry point	Card reader device detection firmware, Third party anti-insert kits
Sabotage	Any attempt to disable any anti-skimming technology	SPS with Skimmer Detect and Alert Monitoring
Shimming	Capture of chip card data with the intent to produce a cloned mag strip card	Transaction Authorisation as per EMV
Network Sniffing	Capture of card data via sniffing of network communications to the host	Communications Encryption TLS 1.2
Malware Sniffing	Capture of card data via malicious software installed on the ATM Hard Disk	See controls for Offline and Online Malware in the following section

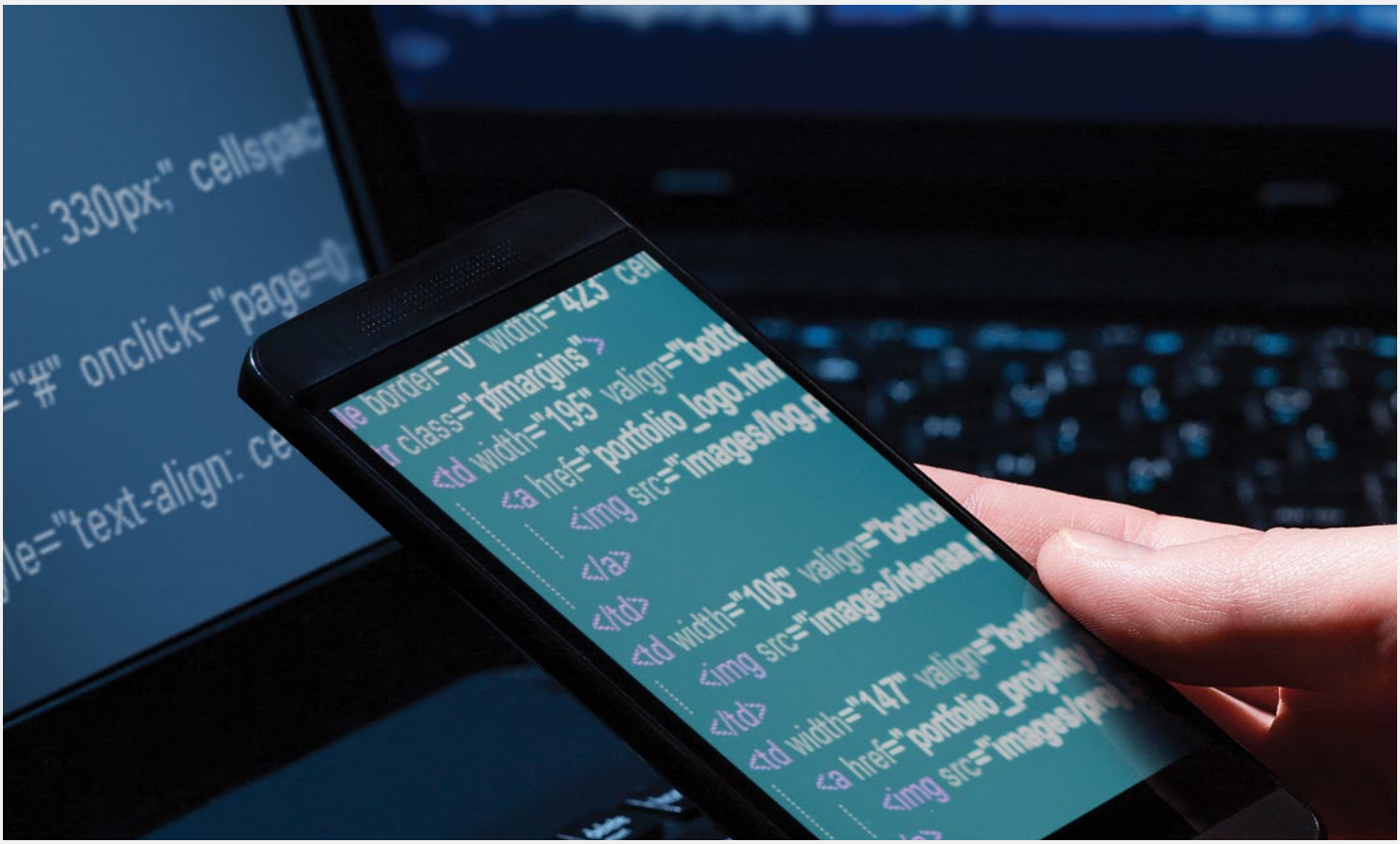
2. LOGICAL THEFT OF VALUABLE MEDIA

Logical theft of valuable media refers to the category of crimes that are used to steal cash or other valuable media from the ATM using methods which do not physically breach the cash enclosure.

This category is the one where there has been the greatest rise in number and variety of attacks. This category is also the one which makes use of the latest technology to exploit features of ATMs which would not have been considered vulnerable at the time of the original ATM design and manufacture. Since 2012, there has been an alarming increase in the frequency of these forms of attacks. Financial institutions, manufacturers and security experts have now seen successful logical attacks occur in all global regions. The nature of these crimes allow the attack to occur on a large number of ATMs at once. The outcome of the crime could be the theft of all of the cash in the ATM and lead to very significant financial losses in a very short period of time.

Typically, these attacks fall into three major categories:

- Black box attacks
- Malware in the Network
- Malware installed on the ATM



In a Black Box Attack, the criminal gains access to the dispenser cable inside the ATM. They then bypass the ATM's core processor and connect an electronic device to the cash dispenser.

The criminal is then able to send unauthorized commands to dispense cash from the ATM. NCR SelfServ ATMs have high levels of internal dispenser encryption to provide protection from these forms of attack. This protection requires the ATM operator to set the Dispenser Security Setting at Level 3 (Physical) as well as run the most current versions of platform software and device firmware.

The second category, is where malware in the network allows the criminal to intercept the communications between the ATM and host. With this criminals are able to capture information or cause unauthorized dispense of cash from the ATM, amongst other things. Encrypting the communications channel between the ATM and the host, along with good network security controls, can prevent these network based attacks.

Another type of attack is when malware is installed on the ATM hard drive. This software is often designed to allow the criminal to send commands to the ATM that cause an unauthorized dispense of cash.

There are two major variations of these malware attacks:

1. The attack is done while the ATM hard disk in online (with its operating system up and running in its normal state). This is typically done using USB devices with Auto Play enabled or using a known Windows Administrator password.
2. The other variation, which is the most common logical attack against ATMs, is an offline attack. An offline attack is when an attacker inserts removable media (for example, DVD, CD or USB) into an ATM core and reboots the ATM. The ATM will then boot to the removable media. Malware is then copied from the removable media onto the ATM hard disk. The ATM is rebooted again with the removable media detached allowing the ATM to start up as normal. However, now the ATM has malware running on its hard disk.

These forms of attacks can be prevented by:

Deployment of Whitelisting solutions tools. Solutions such as NCR's Soldcore Suite for APTRA are designed to protect the software that is installed on the ATM. This is done by ensuring that only authorized code can run. That authorized code or memory cannot be tampered with or hijacked.

Encrypting the ATM hard disk. This makes the hard disk unreadable when offline. When it is unreadable, attackers cannot copy malware onto the hard disk.

Locking down the BIOS. This prevents the ATM from booting to removable media. When an attacker inserts removable media into the ATM core and restarts the ATM, the ATM will not boot to that device. The ATM will start as normal.

Encrypting the ATM hard disk. NCR Secure Hard Disk Encryption is the most comprehensive protection against offline attacks on ATMs.

This solution:

- Protects against offline malware attacks by preventing malware being copied onto the hard disk when the ATM is booted from removable media
- Prevents malware being copied onto the hard disk when the ATM hard disk is removed and mounted as a secondary drive
- Ensures the contents of the hard disk is encrypted and unreadable when it is removed from the ATM core, when the core is removed from the ATM, or when network connectivity is compromised

In addition to preventing offline attacks, NCR Secure Hard Disk Encryption also prevents reverse engineering of the deployed software stack.

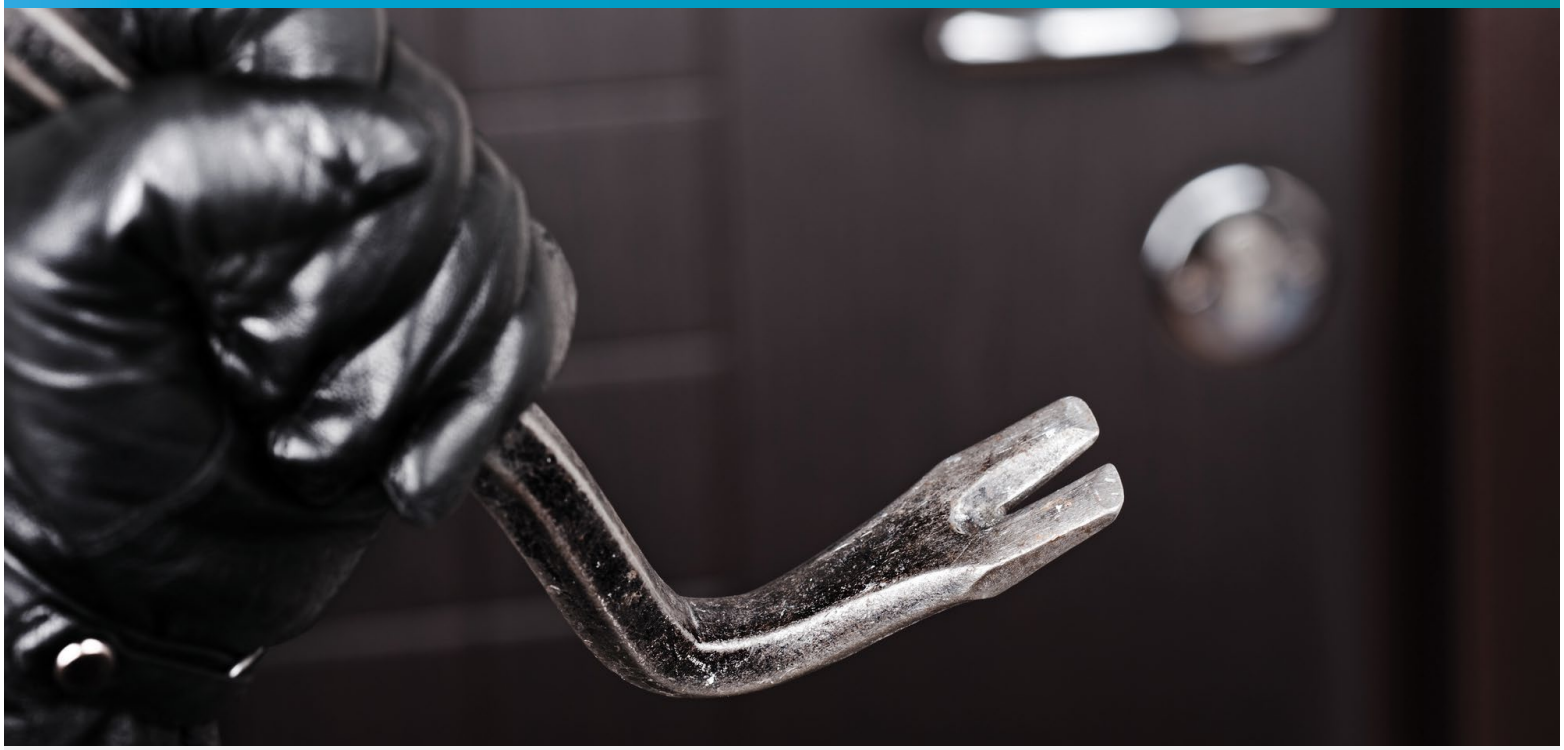
Protection from logical attacks is only possible through the complete deployment of a layered and comprehensive deployment of security guidelines.

These include:

- Secure the ATM BIOS to only allow boot from the primary hard disk. BIOS editing must be password protected
- Establish an adequate operational password policy for all passwords. A single password for every ATM is not secure
- Implement communications encryption (TLS encryption or VPN). This should be considered as mandatory if you are using public wide area networks
- Establish a firewall. This also should be considered as mandatory if the ATMs are on a public wide area network
- Remove unused services and applications. Any code is a source of vulnerability, so minimize it
- Deploy an effective anti-virus mechanism. NCR Recommends active whitelisting applications such as NCR's Solidcore Suite for APTRA
- Establish a patching process for Operating System patches
- Establish a regular patching process for all software installed
- Disable Windows Auto-Play
- Ensure the application runs in a locked down account with minimum privileges required.
- Define different accounts for different user privileges
- Remotely & securely control passwords with enhanced permissions
- Deploy a network authentication based Hard Disk Encryption Solution such as NCR's Secure Hard Disk Encryption solution
- Ensure there is protected communications to the dispenser of the ATM
- Perform a Penetration Test of your ATM production environment annually
- Use Remote Software Distribution. This helps enable some of the earlier security requirements
- Consider the physical environment of ATM deployment

An additional but critical layer of the solution strategy comes with the deployment of Enterprise Fraud detection solutions. This layer provides your financial institution with the ability to track and monitor transactions throughout all of your channels. The Fraud detection solution will provide the ability to note abnormal transaction patters. This can include frequency of transactions, location of transactions by geography and by merchant.

3. PHYSICAL THEFT OF VALUABLE MEDIA



Physical theft of valuable media—the category of crimes that are used to steal cash or other valuable media from the ATM using methods which physically breach the cash enclosure. This category includes all of the traditional robbery techniques that can be used to open a safe, and includes emerging trends such as the use of explosives.

These crimes continue to be major problem for ATM operators. According to data provided by the European ATM Security Team (EAST), nearly 50 million Euros were lost from physical attacks on ATMs in 2015.

The main categories of these physical attacks are:

- Cash Explosions to physically breach the safe. Traditionally this was done in certain regions where there was easy access to solid explosives, such as dynamite. More recently, security professionals have noted a frightening increase in the use of gas explosives occurring in more and more areas of the world.
- Cutting the safe by some means of brute force. This can be done using torches or grinders.
- Ram Raid—instances where the ATM is physically removed from its installation environment.

Key protective strategies here center around ensuring that ATM operators choose the correct safe based on the threat environment.

An additional but critical layer of the solution strategy comes with the deployment of Enterprise Fraud detection solutions. This layer provides your financial institution with the ability to track and monitor transactions throughout all of your channels. The Fraud detection solution will provide the ability to note abnormal transaction patters. This can include frequency of transactions, location of transactions by geography and by merchant.

These solutions include:

- SecureCash degradation solutions like Ink Staining or Glue Solutions that will make the cash unusable if the ATM cassette is breached.
- Gas Detection / Neutralization solutions can be installed to detect the presence of gas used as part of an explosive attack. These devices can be configured to trigger alarms, smoke, sirens, or other notifications. Gas neutralization will counteract the presence of an explosive gas to prevent an explosion from occurring.
- GPS devices and ATM trackers can be installed to both notify when motion is detected on an ATM and track the location of the ATM.

In summary, ATM operators face a real, material and ever-evolving threat to their ATM investments and operations. These threats can be mitigated with a proactive, comprehensive and layered approach to solution deployment. Security is not an option, should be your approach.

NCR account teams are ready to provide you with assistance to help you develop the security strategy that best fits your environment.

WHY NCR?

NCR Corporation (NYSE: NCR) is a leader in omni-channel solutions, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables nearly 700 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Atlanta, Ga., with over 30,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.

NCR

SECURE