SECURITY REQUIREMENTS TO HELP PROTECT AGAINST LOGICAL ATTACKS

For more information visit ncr.com or contact us at financial@ncr.com
Introduction

For far too many years, to reduce costs, security has played a minor role in the purchasing decision of ATMs, but with the increase in criminal attacks on ATMs and pressure from industry bodies such as PCI and EMV, security and compliance is no longer an option.

This document describes the primary activities required to be performed to ensure the security and integrity of an ATM estate.

NCR Secure Minimum Configuration

This document defines the minimum security configuration requirements for an NCR ATM. All NCR ATMs MUST be configured as per the guidelines explained in this document. These minimum security requirements are necessary to defend against known or feasible attacks on an ATM. These guidelines are not optional; they should be viewed as mandatory to protect the ATM in today's environment.
**NCR Secure: Software Configuration and Implementation Guidelines**

**Rule 1: Secure the BIOS**

The BIOS is a set of programs, typically in firmware (PROM, EEPROM or flash memory), that enables a computer’s CPU to communicate with peripheral devices. The BIOS provides startup Power-On Self-Test (POST) and then bootstraps the operating system on power-on or bus-reset. The BIOS consists of code (typically operating CPU in real mode) and configuration settings. The configuration settings are used to control the operation of the BIOS programs and also the hardware parameters that are exposed to the operating system.

Securing the BIOS is fundamental to the security of the ATM. This step **MUST NOT** be omitted.

Administration of the BIOS must adhere to the following principles:

- **During normal operations,** you should configure the BIOS to boot from the primary Hard Disk only. All other bootable mechanisms should be removed from the boot order.
- **Automatic BIOS updates must be prevented.**
- **Editing of BIOS settings must be password protected.**

To manually configure the BIOS, please contact your NCR Account Manager for a copy of *Manually Securing the BIOS*. This document covers BIOS configuration for:

- Pocono
- Riverside
- Talladega
- PIVAT
- Kingsway

**NCR recommends NCR SECURE Remote BIOS Update.**

NCR SECURE Remote BIOS Update:

- Remotely, through software distribution, secures BIOS for Pocono, Riverside, Talladega & Kingsway cores
- Configures boot from primary Hard Disk only
- Sets a customer specific BIOS password
- Sets up UUIDs

**Rule 2: Establish an Adequate Operational Password Policy for all Passwords**

It is up to each and every ATM deployer to ensure that they implement a secure user account and password policy. Banks should use an account management system that will allow them to manage accounts centrally, for example Microsoft Active Directory. Moreover, they should ensure that all passwords are secure. It is up to the ATM deployer to ensure that they implement a policy for securing ATM BIOS and OS user accounts.

All default passwords **MUST** be changed. Unique passwords should be used for each user account on the ATM. This gives maximum protection at each ATM as a successful attack at one ATM cannot lead to a successful attack at another ATM.

- NCR recommends that passwords be at least 14 characters long and must not contain more than two consecutive characters from the user name.
- The password should also be complex and must contain at least three of the following 4 categories
  - English uppercase alphabet characters (A–Z)
  - English lowercase alphabet characters (a–z)
  - Base 10 digits (0–9)
  - Non alphanumeric characters (for example !@#$%)
- User and Administrator account passwords must be changed every 90 days

BIOS passwords are often limited by length and complexity. Nonetheless, BIOS passwords should be as complex as the BIOS allows.

**Rule 3: Implement Communications Encryption**

Sensitive information must be encrypted during transmission. Earlier versions of the TLS protocol have been demonstrated to have weaknesses which can be exploited therefore only TLS 1.2 and above should be used.

PCI DSS mandates that cardholder data sent of public networks must be encrypted.
NCR further recommends not to:

- Use end-user messaging on an ATM
- Send cardholder data over public networks

NCR Recommends **NCR Secure TLS Encrypted Communications.**

### Rule 4: Establish a Firewall

The Default configuration of the Windows 7 firewall blocks all incoming communications connections, any applications that require incoming connections must be explicitly configured. All outgoing communications are allowed by default.

The ATM firewall must be configured to only allow known authorized incoming and outgoing connections per program rather than per port.

For more information, refer to the documentation for your firewall product.

**Windows XP**

If you use the Windows Firewall in Windows XP, you may need to add services or programs to the exception list.

There is a known issue in Windows XP regarding firewall configuration with a network adapter using checksum offloading. Microsoft does not have a fix for this issue but you can apply the workaround detailed in the Microsoft Knowledge Base article KB904946


**Windows 7**

If you are using the Windows Firewall in Windows 7, which supports Network Location Awareness (NLA), this enables Windows 7 to detect changes in network connectivity so that applications can continue to operate seamlessly when network changes occur. Windows recognizes three different types of network location:

- **Domain network** - A network on which Windows can authenticate access to a domain controller for the domain to which the computer is joined.

- **Private network** - A network that has been specifically designated by the user or by an application as being a private network located behind a gateway device such as a NAT router.

- **Public network** - A network that provides a direct connection to the Internet or is in a public place such as a café or airport.

The Windows Firewall uses NLA to identify each network type and then automatically associates/configures a firewall profile for that network type. The corresponding firewall profiles are as follows:

- **Domain profile** - Applies to network connections identified as domain network connections.

- **Private profile** - Applies to network connections identified as private network connections.

- **Public profile** - Applies to network connections identified as public network connections.

With the different network types in mind, it may be necessary to add services or programs to the exception list for a particular profile.

### Rule 5: Remove Unused Services and Applications

It is recommended that you remove any unused services and applications from the system to reduce the attack surface area. By adopting the principle of 'If you don’t use it, disable it', you remove potential points of attack by disabling modules and components that your application does not require.

For example, if your application does not use output caching, you should disable the ASP.NET output cache module. Thereafter, if future security vulnerabilities are found in this module, your application is not vulnerable.

NCR strongly recommends removing any remote desktop access (including Microsoft Remote Desktop Protocol (RDP)).

The following table lists examples of the recommended applications that should be removed from the ATM software stack if they are not used on the ATM:

<table>
<thead>
<tr>
<th>Application</th>
<th>Filename</th>
<th>Description/Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Resolution Protocol</td>
<td>arp.exe</td>
<td>Display/edit network address</td>
</tr>
<tr>
<td>File Attribute</td>
<td>attrib.exe</td>
<td>Display/edit file attributes</td>
</tr>
<tr>
<td>File Transfer Protocol</td>
<td>ftp.exe</td>
<td>Transfer files between two hosts</td>
</tr>
<tr>
<td>NetBios over TCP/IP</td>
<td>nbtstat.exe</td>
<td>Display network information</td>
</tr>
</tbody>
</table>
Rule 6: Deploy an Effective Anti-Malware Mechanism

Anti-malware software will:

- Maintain the integrity of your ATM software stack
- Prevent malicious software compromising your ATM.

An effective active white-listing solution will provide online protection beyond known malware threats. For example, memory protection, zero-day attacks and threat alerting.

NCR Recommends Solidcore Suite for APTRA.

- Solidcore Suite for APTRA is more effective than anti-virus software
- Solidcore Suite is an active whitelisting application for increased malware protection
- Solidcore Suite for APTRA prevents execution of the malware. If unauthorised software is detected, Solidcore will prevent the code from running.
- Solidcore Suite for APTRA can provide alerting if the client software has been disabled
- Solidcore Suite for APTRA provides memory protection
- Solidcore Suite for APTRA protects against zero-day attacks – known and unknown threats.

If you intend to run traditional anti-virus software on the ATM, consider the following recommendations:

- Run anti-virus software in silent mode with no pop-ups.
- Before deploying the anti-virus software, decide what to do if a virus is suspected, for example:
  - If a virus is suspected, log (centrally or locally) that a virus is suspected and continue.
  - Quarantine or delete the suspected file.
- If anti-virus software is running in real-time mode, do not check log files frequently because they are updated too often.
- If anti-virus software is running in the background, consider process priorities.
- If anti-virus software runs on command, put the ATM out of service before scanning or run during quiet periods.
- Update the signature files daily.

Rule 7: Establish a Policy for Applying Secure Operating System Hotfixes

Keeping up to date with Microsoft security hotfixes ensures that attackers do not take advantage of known vulnerabilities within the operating system. The weaknesses may allow malware to be installed onto the ATM or allow attackers access to the ATM software.

NCR provides a service offering of which Microsoft Windows 7 hotfixes should be applied on an APTRA software stack.

Rule 8: Establish a Regular Patching Process for all Software Installed

Keep all software running on the ATM up to date with the latest vendor security patches for the software. This ensures that attackers do not take advantage of known vulnerabilities within the deployed software. The weaknesses may allow malware to be installed onto the ATM or allow attackers access to the ATM software.

If a vulnerability within the software stack has been addressed by a patch which has been installed onto the ATM then it will no longer be exploitable.

Rule 9: Disable Windows Auto-play

Auto-play is a feature of Windows operating systems which allows software to run from removable media as soon as it is detected on a USB, DVD or CD. Disabling the auto-play feature within the operating system will
prevent malware being automatically run when it is detected on removable media.

Disabling auto-play is a configuration option within Security for APTRA.

### Rule 10: Ensure the Application Runs in a Locked Down Account with Minimum Privileges

Implement a locked-down user account for automatically running self-service functionality (SST-mode). This will restrict the privileges and behavior of the ATM to allow only the functions necessary for a self-service environment.

**NOTE:** the locked down user account should **NOT** be a member of the Administrators group.

### Setting up Security on Windows XP and Windows 7

Security consists of setting up a trusted environment on a standalone ATM based on the following requirements:

- Allowing only boot from fixed disk
- Preventing automatic running of programs on removable media
- Providing a locked-down user account for automatically running self-service functionality (SST-mode)
- Optionally providing access to other user accounts (PC-mode)
- Implement a keyboard disabler to block keypresses being interpreted within the locked down account.
- Hide the Windows taskbar
- Uninstall PowerShell.

Setting up security on an ATM always consists of the following stages:

1. Prepare Application Software for Installation on the ATM
2. Configure the BIOS
3. Install Security Settings
4. Automatic Logon to SST-Mode

**NCR Recommends Security for APTRA**

Security for APTRA protects the operational security of an ATM via the creation of a trusted environment to protect the ATM’s assets. The trusted environment encompasses a comprehensive set of security features including: preventing the automatic running of programs on removable media (Rule 9), providing a locked down account for automatically running self-service functionality, controlling access to external devices and running of software which effectively locks down the runtime environment of the ATM software environment at the registry level. In excess of 500 registry settings are automatically set when the software is installed in “Secure Mode”. These registry settings are a balance between the minimum settings required to operate an ATM in a stand-alone environment, and the recommendations of both the NSA and Microsoft Security experts.

### Rule 11: Implement Role Based Access control

For all users accessing the ATM environment, user accounts should be created and given only the access permissions based on the role of that user.

Restrict functionality allowed via remote desktop access to ATMs and if remote access is required then two factor authentication must be enforced for that access.

### Rule 12: Deploy a Remotely Authenticated Hard Disk Encryption Solution

Deploying full hard disk encryption protects the integrity of the ATM hard disk. This means that the ATM is protected against:

- Malware attacks when the ATM hard disk is offline
- attackers reverse engineering software on the ATM hard disk
- attackers harvesting data from the ATM hard disk

Full hard disk encryption protects the ATM hard disk from offline attacks if any of the following occur:

- ATM is booted from removable media
- Hard disk is removed from the ATM and mounted as a secondary drive
- The core is removed from the ATM

**NCR Recommends NCR SECURE Hard Disk Encryption**

- Protects against attackers installing malware onto the ATM hard disk
- Renders the contents of the hard disk unreadable to protect against offline attacks, reverse engineering of code or data harvesting
- Provides a centralized encryption status of the ATMs being managed
• Prevents attackers deriving or harvesting the decryption keys locally to circumvent encryption technology

**Rule 13: Ensure Communications between the ATM core and the Dispenser is protected**

Protecting the communications between the ATM core and the dispenser will prevent black box attacks. If attackers attempt to send commands to the dispenser directly, the dispenser will recognize these commands as invalid. Only commands from the ATM software stack will be authenticated and processed by the dispenser.

Ensure there is protected communications

**NCR Recommends**

NCR Dispenser Encryption Enhancement set to Level 3 (Physical)

Personas Dispenser Encryption Enhancement.

**Rule 14: Perform a Penetration Test of your ATM annually**

Best practice defines that a penetration test is performed on your ATM by an organisation external to your company. The penetration test will comprise of various simulated attacks in an attempt to find misconfiguration, weaknesses and vulnerabilities that could be exploited by an attacker in a production level ATM. The penetration test will allow you to do identify any areas that need addressed to ensure your ATM is optimally secure.

**Rule 15: Deploy a software distribution tool that provides Confidentiality, Integrity and Availability**

In order to meet rules 7 and 8, it is essential to have remote software distribution capabilities. Additionally, if malware is found or suspected to be on an ATM, software distribution will expedite the deployment of patches and updated virus dat files across an ATM estate. This will help put the ATMs into a more secure state, prevent attacks occurring and help limit damage to those ATM that may be compromised.

**NCR Recommends**

APTRA Vision Software Distribution

Stinger files to detect and delete malware if an attack happens

**Rule 16: Consider the Physical Environment of ATM deployment**

The physical environment that an ATM is deployed within and the ATM type will influence the risk of an ATM being attacks. Lobby ATMs (e.g. P77 or 6622) should not be deployed in 24/7 unattended environments without compensating physical security controls. A Through the Wall ATM may be more suitable for these locations.

**NCR Recommends**

Through the Wall ATMs may be more suitable for unattended environments.

UL rated pick resistant Top Box locks SelfServ ATMs as a configuration option or upgrade kit.

**Rule 17: Consult a security enterprise specialist to assess and deploy industry best-practice security controls within your enterprise**

For example:

• Security Awareness Training for employees to minimize the risk of spear phishing
• Ensure a robust patching process is in place across the FI’s enterprise
• Deploy Role based access control
• Deploy Network Intrusion Detection/Prevention systems. Creating custom rules to detect and respond to unusual traffic behaviour. For example, block and alert on any ATM to ATM traffic.
• Deploy Network Access Control that provides endpoint authentication to only allow authorised authenticated devices(ATMs) and applications access to the network and services

NOTE: these are just examples and your Enterprise security specialist should advise on best-practice controls.
Why NCR?

NCR Corporation (NYSE: NCR) is the global leader in consumer transaction technologies, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables more than 550 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 Duluth, Georgia 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. The company encourages investors to visit its web site which is updated regularly with financial and other important information about NCR.