

# BEST PRACTICE FOR ATM CYBER SECURITY

---

International minimum security guidelines for the ATM industry



---

**Produced by the Global ATM Security Alliance**

# Table of Contents

<b>Foreword</b>		<b>1</b>
<b>Part One</b>	<b>Operating System Security</b>	
<b>Chapter One</b>	<b>Operating System Configuration</b>	<b>2-7</b>
<b>Chapter Two</b>	<b>Account Security</b>	<b>8-9</b>
<b>Part Two</b>	<b>Network Security</b>	
<b>Chapter Three</b>	<b>Restrict Access</b>	<b>10-11</b>
<b>Chapter Four</b>	<b>Detection/Protection</b>	<b>12</b>
<b>Acknowledgments</b>		<b>13</b>
<b>Disclaimer</b>		<b>13</b>

## Foreword

Financial institutions and ATM operators are replacing and upgrading aging Automatic Teller Machine fleets across the globe in order to satisfy regulatory and business imperatives.

Regulatory requirements include the use of the Triple DES encryption algorithm, whilst business drivers include demands for increased functionality, enhanced customer experience and system integration to streamline management and monitoring.

In order to satisfy these business and regulatory drivers, new platforms utilising “mainstream” technologies are being introduced which is dramatically altering the vulnerability landscape associated with this traditionally proprietary system.

The use of proprietary technologies afforded ATMs a degree of defence against malware, “hacking” toolkits and utilities, denial of service attacks and other threats that have been used to exploit vulnerabilities in more prevalent operating systems and networks.

Most modern ATMs are now running on operating systems and network communication protocols known by, and familiar to, the majority of computer users. As a result, they exist within the identical vulnerability landscape that the majority of computing systems and networks in use today experience, and are consequently exposed to many of the associated threats.

The recommendations presented in this manual are essentially designed to provide a “common sense” approach to risk mitigation as a result of the rapidly changing threat model that the introduction to the ATM channel of the Windows XP and other common use operating systems, as well as the TCP/IP network protocol suite, has created.

Please note that this manual should be read in conjunction with GASA’s General Cyber Security manual and the white paper on a Continuous Cyber Security Process (CCSP) on [www.globalasa.com](http://www.globalasa.com).

Ian Simpson, CISSP

Technical Compliance Manager

IT Policy, Risk and Compliance

Bank of Western Australia Ltd.

September 2004

---

# Part One      Operating System Security

---

## Chapter One

### Operating System Configuration

#### 1.1      Operating System Components

The default installation of modern operating systems includes many components, packages or clusters. The selection of system components ultimately installed as part of an operational build can usually be made either during installation, post-installation, or both. However, as the majority of ATMs are delivered with a standard operating system build, the only opportunity to remove unnecessary packages is at post-installation. Only the components necessary for the normal operation of the ATM should be installed. The decision to remove a particular package needs to be analysed against the ATM vendor's application requirements, and the acquirer's management, monitoring and other operational considerations.

#### 1.2      System Patching

It is sound security practice to ensure that the operating system patch level meets the latest requirements prior to the ATM being deployed. This will require consultation with the ATM vendor and operating system software support staff and/or knowledge databases to determine applicability, operational impact and depth of regression testing. Any additional patches applied should be included as part of a standard build for multiple ATM deployments. It is possible that any patches or hotfixes applied to a customised, or "hardened" operating system may undo the system modifications. Pre-deployment patching should be undertaken prior to the introduction of these changes.

Ongoing system patching is critical to risk management and security assurance throughout the lifetime of the ATM. A communication channel should be established between the vendor and the ATM owner/service provider to ensure timely notification of the existence of vulnerabilities and operating system or application patches. All system patches should be applied in a test environment prior to their implementation into the production fleet.

## 1.3 Operating System Services

Most commercial operating systems are designed to enable, and automatically start, a large number of various services that would not normally be required by an ATM. Only operating services necessary for normal operation of the device should be enabled and set to start automatically. The decision to disable a particular service needs to be analysed against the ATM vendor's application requirements, and the acquirer's management, monitoring and other operational considerations. Services should be run with the least privilege necessary.

## 1.4 Operating System Security Policies – Windows XP

Windows XP permits the configuration of granular security settings through the “Local Security Policy”. The recommendations below should be analysed and tested on non-production ATMs to ensure compatibility with specific ATM Operating System versions, applications and operational support requirements. Additionally, consult the ATM vendor for a determination on specific settings listed below.

### 1.4.1 User Rights

“User Rights” control what actions specific users and/or groups are permitted to perform on the system.

<b>Policy</b>	<b>Recommended Security Setting</b>
Access this computer from the network	No one
Act as part of the operating system	No one
Add workstations to domain	No one
Adjust memory quotas for a process	Administrators
Allow logon through Terminal Services	No one
Back up files and directories	Administrators
Bypass traverse checking	Administrators
Change the system time	Administrators
Create a pagefile	Administrators
Create a token object	No one
Create permanent shared objects	No one
Debug programs	Administrators
Deny access to this computer from the network	Not Defined
Deny logon as a batch job	No one
Deny logon as a service	No one
Deny logon locally	Not Defined
Deny logon through Terminal Services	Everyone
Enable computer and user accounts to be trusted for delegation	No one
Force shutdown from a remote system	Administrators
Generate security audits	Local Service; Network Service
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	No one
Log on as a batch job	No one

Log on as a service	Network Service
Log on locally	Administrators; Specific Users
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	Not Defined
Replace a process level token	Local Service; Network Service
Restore files and directories	Administrators
Shut down the system	Administrators
Synchronize directory service data	No one
Take ownership of files or other objects	Administrators

## 1.4.2 Security Options

“Security Options” allows the configuration of many specific parameters. Any changes to the default configuration should be applied after consultation with the vendor, and then thoroughly tested in a non-production environment.

<b>Policy</b>	<b>Recommended Security Setting</b>
Accounts: Administrator account status	Enabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Accounts: Rename administrator account	Rename
Accounts: Rename guest account	Rename
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Shut down system immediately if unable to log security audits	Disabled
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled <sup>1</sup>
Devices: Restrict floppy access to locally logged-on user only	Enabled
Devices: Unsigned driver installation behaviour	Warn but allow installation
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined

<sup>1</sup> The Windows installer may not function if this setting is enabled on XP Pro Service Pack 1

Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Not Defined
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	7 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled
Interactive logon: Message text for users attempting to log on	Configure Locally
Interactive logon: Message title for users attempting to log on	Configure Locally
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	0
Interactive logon: Prompt user to change password before expiration	14 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled
Interactive logon: Smart card removal behaviour	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Not Defined
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Not Defined
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled

Network access: Do not allow storage of credentials or .NET Passports for network authentication	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	Not Defined
Network access: Remotely accessible registry paths	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Send NTLMv2 response only/refuse LM & NTLM
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security, require 128 bit encryption
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security, require 128 bit encryption
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Disabled
Shutdown: Clear virtual memory pagefile	Enabled
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled
System objects: Default owner for objects created by members of the Administrators group	Object creator
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled

## 1.5 System Auditing

Certain events that relate to account access or operating system status should be configured to be captured in the system event logs. As a minimum, the following items should be audited. However, the ability to configure specific system auditing will be dependant on the ATM operating system:

Account Modification – track changes to the account database on the operating system. Specifically, capture account creation, deletion or modification (e.g. changes to group membership).

Account Use – track successful and unsuccessful attempts to logon onto the operating system.

Privilege Use/Elevation – track unsuccessful attempts to access privileged programs or gain elevated privilege level access (e.g. the use of the “*su*” command in Linux)

Major System Events – track system restarts, shutdowns or runtime mode changes.

System event logs should be protected from unauthorised modification or deletion by suitable access control lists or file permissions.

# Chapter Two

## Account Security

### 21 System Accounts

A typical operating system installation will include various system and user accounts (e.g. “Guest”) that are usually not necessary for the normal operation of the ATM. These accounts need to be locked, disabled or deleted depending on the operating system and the function of the account.

The ATM operating system will also have a “super user” or administrator account, and if permissible, this account should be renamed to a unique account for each ATM. The account name and password should be released to authorised individuals as required for support purposes.

If the introduction of unique “administrator” accounts for each ATM is determined to be operationally untenable, the passwords should consist of 14 characters, with complexity enforced.

Accounts should be set to “lockout” after 3 failed logon attempts if the unsuccessful attempts occur within a 15 minute period. In environments where the password length is 14 characters with complexity enforced, it is reasonable to increase this “lockout” threshold to 5.

The accounts should be locked out for a specific period of time, and it is recommended that this be set to 15 minutes.

ATM application design should ensure that elevated account privilege levels are not required for normal operation. Any additional software installed to provide business or support enhancements should also abide by this principle.

If the operating system permits, access to the desktop or command line shell should be denied to the runtime account.

## **22 Account Password Security**

Depending on the operating system and application design, there may be one or more privileged accounts configured at the operating system level. The passwords assigned to these accounts should adhere to standard privileged account password security principles. Namely:

Password uniqueness – each privileged account on each ATM should have a unique password.

Password Complexity – each privileged account on each ATM should have passwords that are a minimum of 8 characters consisting of letters, numbers, mixed-case and meta-characters. Additionally, the password should not match the account name.

Password ageing – Whilst it is recognised that all passwords should be subject to ageing, the frequency of password changes cannot be determined in isolation. When considering the lifecycle of a password, the following should be taken into consideration:

- Privilege level of account

- Frequency of use/access

- Administrative overhead/cost of actually implementing the password change

- Operational impact of implementing the password change

Password history – Configuring password history requirements will preclude a previously used password from being re-applied to a particular account. It is recommended that password history for privileged accounts be set to 12, which essentially prevents any of the previous 12 passwords from being chosen as the new account password.

Password Storage – All privilege level passwords should be stored securely and provided to administrative and support staff as required. Passwords should only be released to authorised personnel and the release recorded for audit purposes.

## **23 Application Password Security**

Some ATM applications (e.g. Maintenance/Administrative Mode access, firewall software) may require passwords to be entered in order to gain access to the functions or configuration menus they provide. Access to these application menus should be treated as a privileged event, and the passwords that control access treated accordingly. The passwords should be changed from any default setting prior to deployment, and they should abide by the principles contained in section 2.2 “Account Password Security”.

### Chapter Three

### Restrict Access

ATMs should be separated either physically or virtually from networks that provide general business connectivity.

#### 3.1 Physical Separation

ATMs should connect to Host systems via dedicated network segments that are not shared by general purpose servers and workstations.

#### 3.2 Network Enforcement Points

There are several points along the communication path connecting the ATM with the host system that would permit the introduction of firewall enforcement points depending on the network topology. Access from within the general network to the ATM network should be controlled by the use of an enterprise “statefull” firewall.

In situations where network architecture does not permit the use or introduction of a single (or several) firewall enforcement points on the internal network due to technical or business limitations, packet filters should be configured on the “next hop” perimeter router that provides TCP/IP connectivity to the ATM.

Where ATMs share network infrastructure (e.g. remote ATMs on Branch networks), border router access control lists should be used to restrict access to the ATM from within the branch network if the traffic is passed through a suitable router.

In environments where an ATM shares a VLAN with other branch traffic, the use of layer two (in TCP/IP terminology) controls, such as switch port security and static ARP mapping, should be employed to restrict intra-LAN access violations.

Unused switch ports should be disabled until required for the addition of devices onto the network.

Network HUBS should not be used due to the ability to capture network traffic and the lack of security features they provide.

Some ATMs are being shipped with firewall capability either bundled with a 3rd party product, or as part of the actual operating system, and this should be enabled and configured irrespective of the extent of additional network enforcement points present or intended on the network.

### 3.3 Default Deny

The design of any firewall ruleset or router access control list must be based on the principle “what is not expressly permitted, is denied”. The opposite position to this principle (“what is not expressly denied, is permitted”) if employed will render the protection afforded by the ruleset virtually null.

Determine exactly what network addresses, protocols and ports are required to support the ATM in terms of transactions, management and monitoring; then **deny everything else**.

# Chapter Four

## Detection/Prevention

### 4.1 Intrusion Detection Systems

The ATM network access point into the central processing host systems should deploy one or more (depending on topology) network intrusion detection systems (NIDS). The NID(S) must be supported by appropriate management, monitoring and incident response policies and procedures.

### 4.2 Malware Protection

If the ATM supports it, malware protection should be installed. Careful analysis of the product, signature file update management, engine update management, periodic scan invocation and status changes/alert notification needs to be undertaken.

#### 4.2.1 Signature and Engine Updates

Updates should be applied to a control/test group as soon as possible after release by the software vendor. System stability should then be confirmed prior to the deployment of the update to the production systems.

#### 4.2.2 Malware Scans

Periodic system scans have the potential to cause degraded performance, and should be conducted when the ATM is out of service. The frequency of the scans should be determined based on ATM service level agreements, business requirements and additional security controls employed (e.g. firewalls, intrusion detection)

#### 4.2.3 Status Changes/Alert Notification

Different Anti-virus products can behave differently with respect to advising of status changes (e.g. AV disabled) or alert notification (e.g. Virus detected). Ensure that any AV installed does **not** result in screen alerts or messages being displayed *on the consumer terminal*.

# Acknowledgments

1. **Ian Simpson, Technical Compliance Manager, Bank of Western Australia Ltd**
2. **The National Security Agency, USA**
3. **SANS Organisation**
4. **NCR**
5. **Diebold**
6. **Jim Richardson, President, K3DES LLC**
7. **The Cyber Security Project Team of GASA**

---

## Disclaimer

This manual has been developed in furtherance of GASA's and ATMIA's nonprofit purposes. The information contained in this manual is intended to identify Best Practices in the ATM industry, but is not a standard for best practice. Therefore, use, reference to, or review of the material in the manual does not and cannot guarantee the elimination of risk inherent in the delivery of ATM services and should not be used as a standard or mandatory requirement for conducting business in the ATM industry. It is recommended that the manual be used as guidance in connection with the implementation of Best Practices, but not as a substitute for diligent review and analysis regarding application of the Best Practices.

GASA and ATMIA have taken reasonable measures to develop the manual and recommended Best Practices in a fair, reasonable, open, and objective manner. However, GASA and ATMIA make no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information being provided. In addition, views of appropriate practices may change over time and errors or mistakes may exist or be discovered in this material. As such, inclusion of material in this manual does not constitute a guarantee, warranty, or endorsement by GASA or ATMIA regarding the views, methodologies, or preferences for implementing the Best Practices. Further, neither ATMIA nor GASA nor its officers, directors, members, authors, or agents shall be liable for any loss, damage, or claim with respect to any such information or advice being provided. All such liabilities, including direct, special, indirect, or consequential damages, are expressly disclaimed and excluded.