ATM Software Security Best Practices Guide Version 3

International minimum security guidelines and best practices for operating ATM software

ATMIA
ATM INDUSTRY ASSOCIATION

Produced by the ATM Industry Association

Contributors Include:

Triton®
Partnership Measured in Decades...

gmv®
INNOVATING SOLUTIONS

Q-ATM

DFR
RISK MANAGEMENT
Deliberative. Formative. Responsive.

Copyright Information

Should you wish to join ATMIA's ATM Software Portal on www.atmia.com,
e-mail Mike Lee, ATMIA's CEO, at mike@atmia.com

Disclaimer

The ATM Industry Association (ATMIA) publishes this best practice manual in furtherance of its non-profit and tax-exempt purposes to enhance the security of ATM software security. ATMIA has taken reasonable measures to provide objective information and recommendations to the industry but cannot guarantee the accuracy, completeness, efficacy, timeliness or other aspects of this publication. ATMIA cannot ensure compliance with the laws or regulations of any country and does not represent that the information in this publication is consistent with any particular principles, standards, or guidance of any country or entity. There is no effort or intention to create standards for any business activities. These best practices are intended to be read as recommendations only and the responsibility rests with those wishing to implement them to ensure they do so after their own independent relevant risk assessments and in accordance with their own regulatory frameworks. Further, neither ATMIA nor its officers, directors, members, employees or agents shall be liable for any loss, damage or claim with respect to any activity or practice arising from any reading of this manual; all such liabilities, including direct, special, indirect or inconsequential damages, are expressly disclaimed. Information provided in this publication is "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or freedom from infringement. The name and marks ATM Industry Association, ATMIA and related trademarks are the property of ATMIA.

Please note this manual contains security best practices and should not be left lying around or freely copied without due care for its distribution and safekeeping.

ATM INDUSTRY ASSOCIATION GLOBAL SPONSORS – 2014

atmgurus	atm marketplace	ATMU	AXIS COMMUNICATIONS	BRINKS	CARDTRONICS
dP Clear2Pay	DIEBOLD INNOVATION DELIVERED	Euronet WORLDWIDE	GLORY	GRG Banking	HITACHI Inspire the Next Hitachi-Omron Terminal Solutions, Corp.
HYOSUNG	MORPHIS	NCR	OKI	payment alliance international	PROSEGUR
spinnaker	TMDSECURITY	Triton POWERED BY TDE	VersaSafe VersaLink	WINCOR NIXDORF	

Table of Contents

Table of Figures

Foreword

In April 2009, the ATM Software Security Committee released the first edition of this Best Practices guide which was subsequently followed by version 2 and then version 2.1 in 2011.

Since that time, the number of ATM malware attacks and attacks using sophisticated electronics, known as black box attacks, has become an ever important threat to ATM systems in many countries and regions.

As we launch this third edition of the Best Practices, the ingenuity and technical sophistication of those intent on either compromising cardholder information at ATMs or effectively jackpotting ATMs of most, if not all, of the cash held in the safe cannot be overstated.

The third edition includes some minor modifications throughout the guide and the following new content and significant updates:

- In Chapter 2: Understanding the PCI Framework for ATM Software on page 18, 2.2 Analysis of PCI DSS Standard and its Impacts on ATM Hardware and Software on page 19 and 2.3 PCI DSS Requirements on page 21 have been updated and expanded to reflect the latest requirements from the Payment Card Industry's Data Security Standard (PCI DSS version 3). New section 2.5 PCI PTS POI ATM on page 28 covers guidelines (rather than standards), issued by the PCI which specifically address ATMs; PCI PIN Transaction Security Point of Interaction ATM (PCI PTS POI ATM). New 2.6 Cryptographic Hash Functions on page 30 explains cryptographic hash functions and in particular highlights the need to adopt SHA-2 rather than MD5 or SHA-1.
- In Chapter 4: Mapping Software Operational Policy: Ensuring Confidentiality, Integrity, Availability on page 47, 4.4 Role of Encryption: Hardware and Software Perspectives on page 58 has been expanded to explain the importance and benefits of both software and hardware solution options for implementing full hard disk encryption (FHDE).
- Chapter 8 Detecting and Mitigating Malware and Black Box Attacks on page 99 is a new chapter which specifically addresses detecting and mitigating ATM malware and black box attacks.
    - Section 8.2 Black Box Attacks on page 99 explains the key characteristics of attacks using sophisticated electronics (black boxes) to take control of modules, such as the cash dispenser, for the purpose of gaining access to the cash within the ATM.

- Section 8.3 Malware Attacks on page 102 highlights the most common features of ATM specific malware used to compromise secret information, such as card and PIN data as well as gaining access to the cash held within the ATM.
- Section 8.4 Malware Examples on page 103 provides a catalogue of some of the ATM malware that has so far been discovered in the field.
- Section 8.5 Mitigation on page 108 identifies options that can be used to help detect and mitigate the risks from both black box and malware attacks targeting ATMs.

The ATM Software Security Committee of ATMIA believes this manual will help to secure the ATM node and its operating software to reinforce the ATM's internal trusted environment. This manual sets out international minimum security guidelines and best practices for ATM software security. To combat fraud, it is imperative that all ATM deployers in all regions and countries take best practices very seriously, and implement all guidelines and best practices contained herein to the greatest extent possible.

Mike Lee, CEO ATMIA

October, 2014

Executive Summary

Please note that this Executive Summary cannot replace reading the whole manual. The summary is merely a guide as to the content and main principles of ATM software security best practices.

The aim of this guide is to help you develop an IT security operational policy for your ATM operating software.

1. The scope of the manual covers governance of all ATM software: system, operating, application, and other software up to the point at which the ATM plugs into the communication link to the host system.
2. There is evidence that criminals are increasingly targeting ATM software and systems as a new frontier of fraud. The goal of this guide is to help you prevent and fend off potential ATM software and system attackers. Key to mitigating and reducing the risk is to understand the methods and tools used in attacks which include malware and sophisticated black box electronic devices.
3. A holistic and systematic approach will enhance the operational security of ATM software. Lifecycle security, therefore, covers everything from development through deployment to the continual maintenance of the systems in question.
4. A powerful way for Information Security professionals to assess any IT system's overall security is to consider the three pillars of security: confidentiality, integrity and availability.
5. Payment Card Industry (PCI) security standards and guidelines, while recognizing the unique nature of ATMs as opposed to general purpose computers and point of sale terminals, provide an excellent foundation for secure ATM operations.
6. Data encryption in an ATM system is implemented in three distinct ways: data at rest on the ATM, data in transit to/from the ATM, and the encrypted PIN and secret keys associated with the financial transactions.
7. Increasing usage of open architectures, such as Microsoft operating systems, CEN XFS-J/XFS device interface standards, and TCP/IP networks, means that ATMs are becoming vulnerable to new and more numerous threats from both internal and external sources.
8. The boundaries of the ATM's environment have expanded with new functionality and services. The need to incorporate ATMs within the corporate IT software security policy or create a specific IT software security policy is indisputable.

9. Apply several layers of defense to provide better security for ATMs. However, the balance between adequate layered security and unneeded complexity should be kept in mind.

10. Physical security of the ATM is vital to ensure that software-based defenses cannot be bypassed.

11. If possible, ATMs should be deployed on a segregated network that does not contain other types of equipment to reduce the ATM's exposure to attack.

12. Using enterprise-wide IT systems can be cost effective and result in stronger ATM security. Technologies that have proven effective in strengthening ATM security include firewalls, antivirus, and whitelisting (locks down the operating system so that only known applications and systems calls can be made).

13. Security engineering is the design and development of a dependable network system which can resist attacks. Security governance is the process of establishing and managing security in those systems. The process starts by understanding the value of the asset to be protected, in our case a self-service network. The next step is to assess the threats that endanger our assets, and the vulnerabilities associated with these assets.

14. It is necessary to understand threats and vulnerabilities in order to perform an impact analysis. For any identified threat, the first step is to assess whether the current ATM network is vulnerable to it. At this point a risk assessment is performed. The goal is to reduce or transfer the risk, not to eliminate it. Finally, security best practices and the security policy are invoked to address the threats and shore up the vulnerabilities. In summary, security governance includes security controls, vulnerability assessment, risk assessment, and application of a security policy.

15. The primary purpose of ATM monitoring is to maintain the best practical level of ATM availability. An ATM needs good monitoring to stay secure. There are three parts to monitoring: ATM application monitoring, general ATM health monitoring, and ATM security monitoring. A well-running ATM needs to have a healthy operating system and set of management capabilities as well as an ATM application that is running and serving customers. The foundation for ATM software security is set at time of installation but proper monitoring maintains the integrity of this foundation.

16. Virtualization technologies give new opportunities for reverse engineering of ATMs software and development of malicious software to carry out ATM attacks. Best practice is for ATM software vendors to introduce anti-reverse engineering technologies such as: obfuscation, program code virtualization, integration of behavioral analysis, and process isolation technologies.

17. Full hard disk encryption (FHDE), whether implemented in software or hardware, provides an important layer of protection for ATM software.

18. Software changes, such as patches, are inevitable. Strict and orderly change control is important. A central software distribution tool can help protect the integrity of the ATMs and reduce downtime.

19. It is important that dual-custody controls are used so that no single administrator can both develop a change and implement it. System management capabilities should always be used within a tiered administration structure where only top-tier administrators can perform the most powerful operations. Allowing the same person or people to both develop and be capable of implementing changes is a violation of the PCI Data Security Standard.

20. To help maintain the security of encryption keys, use an automated key distribution (remote key) system and follow key management best practices.

21. Communications security, including encryption of both transactional and management traffic, is part of a holistic approach for ATM security.

22. While the use of encrypting PIN Pads (EPPs) ensures that the PIN is always encrypted during communication, the risk of a criminal tampering with transactions in flight during transmission over the communications link is still of concern for ATM security. Message authentication code (referred to as MACing transaction traffic) is a technique that can protect against tampering with transaction data while it is in flight between the ATM and the financial switch.

23. Diligence is needed in outsourced ATM servicing to maintain security from a people perspective. Third-party service agreements for servicing and maintaining ATMs should explicitly assign liability for fraud – including any fraud that might be perpetrated through the software service interface of the ATM or by installing illicit software on the ATM. Both in-house staff and third-party providers need to be audited at least annually to ensure compliance with Lifecycle Security processes.

24. Dr. Donald Cressey developed the well-known fraud triangle for white collar crime: opportunity, financial need, and the rationalization, a useful model for understanding insider ATM fraud. Companies can control the factors of opportunity and financial need, but not how fraudsters rationalize their crimes.

25. Employee recruitment checks are a first line of defense against insider fraud and must be backed up with on-going vetting and staff monitoring. In addition, security access to premises needs to be tightened with a strict visitor access system as well as the introduction of an information policy and a company-wide clean desk and secure data storage and filing policy. Finally, preventing insider fraud requires a robust whistle-blowing procedure to minimize the risk of cover-ups of internal fraud.

26. As more advanced types of transactions are implemented via ATM integrated payments, protection of cardholder information and transaction processing integrity must be upheld.

27. Common vulnerabilities of ATMs include the following:
    a. Leaving passwords set as the manufacturer's default.
    b. Reusing passwords at multiple ATMs.
    c. Accessing the service password prompt without an additional layer of security, such as multi-factor authentication.
    d. Resetting passwords without affecting the current programming.
28. Such vulnerabilities can lead to the following types of fraud: denomination fraud, surcharge fraud, compromise of confidential information, and the introduction of malware.
29. Fraud should be reported to the authorities immediately to allow local and regional law enforcement to identify patterns across a geographic region and find those responsible for the fraud.
30. The ten immutable laws of ATM security are:
    a. If a bad guy can alter the operating system on your ATM, it's not your ATM anymore.
    b. If a bad guy has unrestricted physical access to your ATM, it's not your ATM anymore.
    c. If you allow a bad guy to upload programs to your ATM, it's not your ATM anymore.
    d. If a bad guy can persuade you to run his program on your ATM, it's not your ATM anymore.
    e. Weak passwords trump strong security.
    f. An ATM is only as secure as the administrators and developers are trustworthy.
    g. Encrypted data is only as secure as the decryption key.
    h. An out-of date security system is only marginally better than no security system at all.
    i. Absolute anonymity isn't possible, in real life or ATMs.
    j. Technology is not a panacea.
31. Remember it is best practice to read the entire best practice manual!

Acknowledgements

ATMIA is indebted to the individual contribution of the following experts:

Technical Editor:	Douglas Russell, DFR Risk Management Ltd.
Contributor:	Henry Schwarz, Triton
Contributor:	Juan Jesus Leon Cobos, GMV
Contributor:	Irmantas Brazaitis, Smart Card Security Ltd.
Contributor:	Jim Tomaney, Q-ATM Ltd.

Finally, we wish to thank the original contributors to previous versions of this document, upon whose excellent work this guide is built. Contributors include:

Terence Devereux

Peter Kulik

Susan Matt

Pat Telford

Rafael Navajo Garrido

Michael Kalinichenko

Pat Bitton

Kenney Falconer

Martin Koffijberg

Fabian Soler

Kiran Gandhi

Andrew Jamieson

Jim Kirkhope

Narayanan Krishnan

Gaurav Marwaha

Joe McGinley

Joe Stevens

Chapter 1. Introduction

In the years since their first deployment, the environments in which Automatic Teller Machines (ATMs) operate have changed dramatically. While some characteristics of ATMs have stood up to the test of time, other characteristics, such as the operating system, ATM application, communication/connectivity, together with the different regulations and requirements, have not fared as well.

The objective of this document is to deliver an understanding of the different factors confronting ATM deployers while at the same time providing a guide on how these challenges can be addressed and transcended.

ATM Software Security and, in particular, delivering a secure ATM operating environment, cannot and should not be seen as implementation of one item, installation of one product, changing of one setting, or revising an ATM's configuration. Instead, a holistic and systematic approach must be taken, an approach incorporating all influencing factors and catering for all possible sources of risks.

Until fairly recently, most ATMs were deployed within proprietary, closed environments. However, the need for an ATM software security best practice and in particular software security guide have never been greater with industry developments, including:

- Increased migration to a multitude of private ATM operators.
- Use of ubiquitous operating systems such as Microsoft Windows®.
- Growing support and acceptance for device interface standards including CEN XFS-J/XFS (Comité Europeen De Normalisation Extensions for Financial Services, or Java Extensions for Financial Services).
- Migration from closed to open communication protocols, such as TCP/IP.
- Increased usage of web-based technology.

Failing to implement an ATM software security policy is detrimental to the well-being of a financial institution's or independent deployer's ATM channel, customer relationships, reputation, and brand equity. Experience has shown that security breaches or failures can have a dramatic effect on the public's willingness and confidence in using ATMs. The ATM industry would then be impacted by diminished transactions and increased flow to other more expensive channels of cash availability.

Apart from the migration from closed to open environments, one of the most important changes affecting the ATM channel is the development and release of the Payment Card Industry (PCI) security standards. PCI standards are designed to protect card information of consumers. In addition to the PCI DSS standard, the PCI Payment Application Data Security Standard (PCI PA-DSS) and PCI PIN Transaction Security (PCI PTS) standards may apply to ATMs and compliance in many parts of the world is mandatory.

1.1. A Brief History of ATMs

According to Wikipedia®[1] the first mechanical cash dispenser was developed and built by Luther George Simjian and installed in 1939 in New York City by the City Bank of New York. Unfortunately, due to the lack of customer acceptance the machine was removed, never to be seen in the public domain.

Figure 1: Advertisement for the first ATM in 1967.

Sir John Shepherd-Barron (1925 – 2010) is credited with the invention of our modern automated teller machine in 1965. De La Rue and Barclay's Bank launched the first live electronic ATM in Enfield Town North London, United Kingdom on 27 June 1967. The number of ATMs worldwide is forecast by Retail Banking Research to reach 3 million by 2015. The ATM has become the primary distribution channel for cash in all modern societies.

[1] http://en.wikipedia.org/wiki/Automated_teller_machine

1.2. Survey of the Current ATM Software Environment

The software environment in which modern ATMs operate has changed dramatically over the last decade. Today, most ATMs have adopted the Microsoft Windows operating system and are currently migrating from Windows XP (end of support) to Windows 7 and 8.

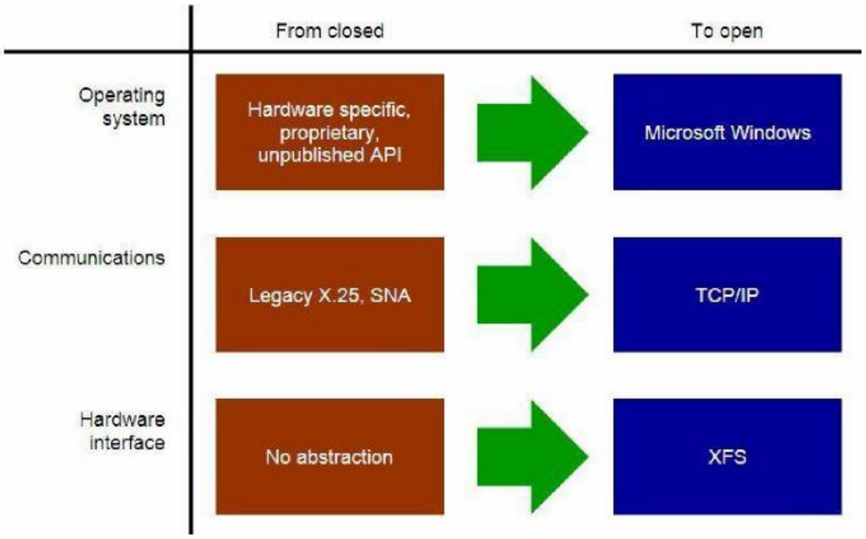


Figure 2: ATM Trends[2]

As ATMs trend from closed to more open environments, such as Microsoft Windows and the Internet, ATMs enjoy the benefits of such technological advances, but are simultaneously exposed to new threats. The modern ATM not only dispenses cash, but, depending on the territory and the IT infrastructure, also delivers more complex services, such as:

- Customer specific 1 to 1 marketing mobile phone prepaid top-up
- Financial services, such as credit extensions, money transfers, and statement status
- Deposits and check cashing
- Bill payment
- Lottery and gaming
- Ticketing (sport, music, travel and so forth)
- Pre-authorized cash transactions
- Charitable donations
- Dynamic currency conversion

[2] ATMs and Cash Dispensers, Western Europe 2010 (Retail Banking Research Ltd). www.rbrlondon.com

With these services, the ATM channel boundaries have been extended. No longer are they operating within a silo or walled garden, but together with services operated by third parties. Through this boundary expansion, the need for ATM security has become essential. The need to incorporate ATMs within the corporate IT software security policy or create a specific IT software security policy is indisputable.

Establishing a comprehensive ATM IT software security policy is a complicated undertaking. Numerous factors must be taken into consideration: ATM certification, staging and deployment, access control, connectivity and communication, operations management and monitoring, software management, continuity and disaster recovery, and more. A key factor for any future ATM software policy is to take into account PCI standards relevant to the ATM, a subject to which we now turn our attention.

Chapter 2. Understanding the PCI Framework for ATM Software

2.1. What is PCI SSC?

The Payment Card Industry Security Standards Council (PCI SSC) is an open global forum, founded by the five global payment brands – American Express, JCB, Discover Financial Services, MasterCard Worldwide, and VISA Inc. Participating council members today span the entire payment supply chain – merchants, payment processors, payment gateways, payment manufacturers, payment application software developers, consultants, attorneys, etc. The PCI SSC was formed in 2006 and is responsible for the development, management, education, and awareness of the PCI Standards.

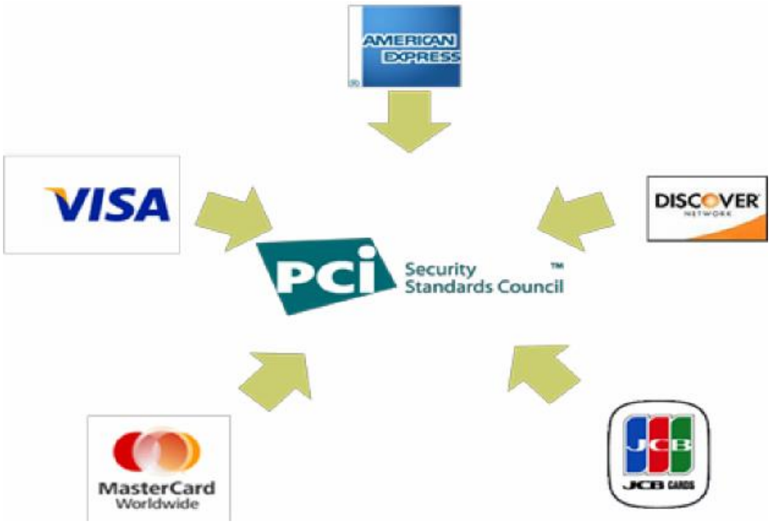


Figure 3: Payment Card Industry Security Standard Council

(Navigating PCI DSS: Understanding the Intent of the Requirements. © 2008 PCI Security Standards Council LLC)

Currently, the following standards are under the control of the Security Standards Council and freely available at https://www.pcisecuritystandards.org.

- PCI Data Security Standard (PCI DSS)
- PCI Payment Application Data Security Standard (PCI PA-DSS)
- PCI PIN Transaction Security (PCI PTS)

2.2. Analysis of PCI DSS Standard and its Impacts on ATM Hardware and Software

The PCI Data Security Standard (PCI DSS) is a set of requirements developed by the PCI Security Standards Council that address the security of cardholder data that is stored, processed, or transmitted.

PCI DSS applies to all "entities that store, process, or transmit cardholder data and/or sensitive authentication data" and thus applies to ATMs.

The main goal of PCI DSS is the protection of cardholder data. The protection requirements are specified by data type in two categories, Cardholder Data and Sensitive Authentication Data, as outlined below:

Data Type	Data Element	Storage Permitted
Cardholder Data	Primary Account Number (PAN)	Yes, if rendered unreadable
	Cardholder Name[1]	Yes
	Service Code[1]	Yes
	Expiration Date[1]	Yes
Sensitive Authentication Data[2]	Full Magnetic Stripe Data[3]	Never
	CAV2/CVC2/CVV2/CID	Never
	PIN/PIN Block	Never

Source: PCI DSS v3.0. © 2013 PCI Security Standards Council LLC.

[1] Other legislation (e.g., related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of these data elements, or proper disclosure of a company's practices if consumer- related personal data is being collected during the course of business.

[2] Sensitive authentication data must not be stored after authorization (even if encrypted).

[3] Full track data from the magnetic stripe, magnetic stripe image on the chip, or elsewhere.

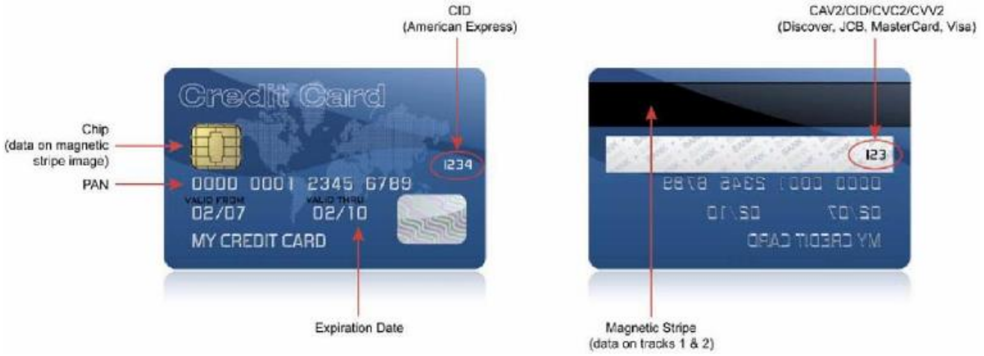


Figure 4: Plastic Card Layout Standard

(Navigating PCI DSS: Understanding the Intent of the Requirements, v2.0. © 2010 PCI Security Standards Council LLC)

2.2.1. Track 1

- Contains all fields of both track 1 and track 2
- Length up to 79 characters

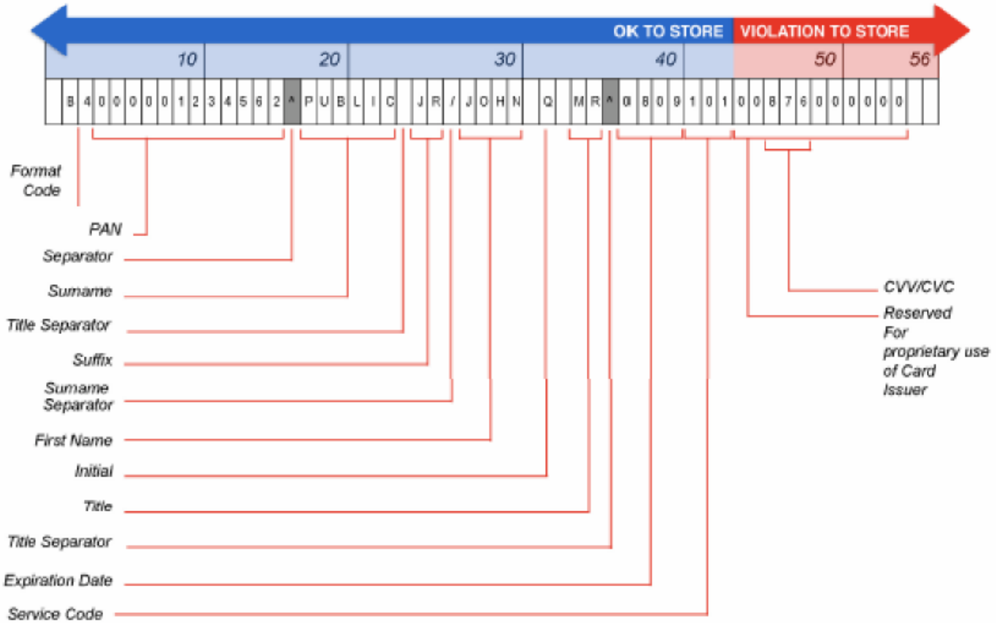


Figure 5: Track 1 Layout

(Navigating PCI DSS: Understanding the Intent of the Requirements, v2.0. © 2010 PCI Security Standards Council LLC)

2.2.2. Track 2

- Shorter processing time for older dial-up transmissions
- Length up to 40 characters

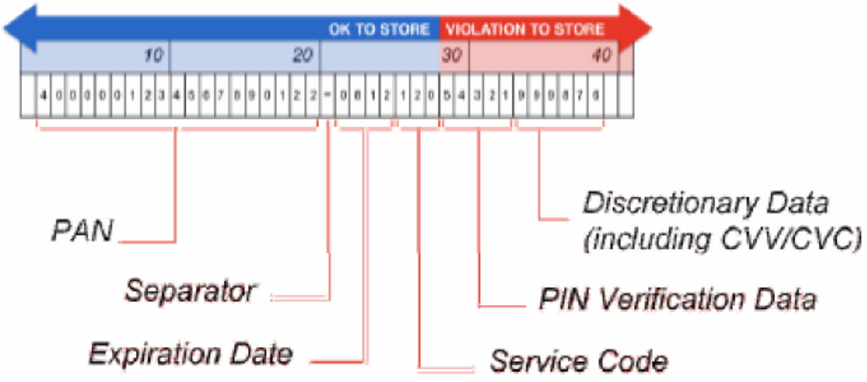


Figure 6: Track 2 Layout

(Navigating PCI DSS: Understanding the Intent of the Requirements, v2.0. © 2010 PCI Security Standards Council LLC)

2.3. PCI DSS Requirements

PCI addresses the security of cardholder data that is stored, processed, or transmitted. The PCI Security Standards Council has defined and specified a set of requirements that merchants and service providers manipulating such sensitive data must implement.

PCI DSS defines a set of twelve high-level requirements, which address six main areas:

1. Build and maintain a secure network and systems;
2. Protect cardholder data;
3. Maintain a vulnerability management program;
4. Implement strong access control measures;
5. Regularly monitor and test networks; and
6. Maintain an information security policy.

Following is a selected extract from the PCI DSS v3.0 specification. Please refer to the specification for testing procedures, guidance, and further details of the requirements.

2.3.1. Goal 1: Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

1. Establish and implement firewall and router configuration standards.
2. Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.
3. Prohibit direct public access between the Internet and any system component in the cardholder data environment.
4. Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network.
5. Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

1. Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.

2. Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.
3. Encrypt all non-console administrative access using strong cryptography. Use technologies, such as SSH, VPN, or SSL/TLS, for web-based management and other non-console administrative access.
4. Maintain an inventory of system components that are in scope for PCI DSS.
5. Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.
6. Protect each entity's hosted environment and cardholder data for shared hosting providers.

2.3.2. Goal 2: Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

1. Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.
2. Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.
3. Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.
4. Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs).
5. Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.
6. Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.
7. Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

1. Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.
2. Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).

3. Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.

2.3.3. Goal 3: Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs.

1. Deploy anti-virus software on all systems commonly affected by malicious software. For systems considered to be not commonly affected, perform periodic evaluations to identify and evaluate evolving malware threats.
2. Ensure that all anti-virus mechanisms are maintained as follows: are kept current; perform periodic scans; generate audit logs which are retained.
3. Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.
4. Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.

Requirement 6: Develop and maintain secure systems and applications.

1. Establish a process to identify security vulnerabilities using reputable outside sources for information and assign a risk ranking (for example, high, medium, and low) to newly discovered security vulnerabilities.
2. Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.
3. Develop software applications securely, in accordance with PCI DSS, based on industry standards and/or best practices, and incorporating information security throughout the software-development life cycle.
4. Follow change control processes and procedures for all changes to system components.
5. Address common coding vulnerabilities in software-development processes.
6. For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks.
7. Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.

2.3.4. Goal 4: Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know.

1. Limit access to system components and cardholder data to only those individuals whose job requires such access.
2. Establish an access control system for system components that restricts access based on a user's need-to-know, and is set to deny all unless specifically allowed.
3. Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.

Requirement 8: Identify and authenticate access to system components.

1. Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.
2. In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components.
3. Incorporate two-factor authentication for remote network access originating from outside the network by personnel, including users and administrators, and all third parties, including vendor access for support or maintenance.
4. Document and communicate authentication procedures and policies to all users.
5. Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: generic user IDs are disabled or removed; shared user IDs do not exist for system administration and other critical functions; shared and generic user IDs are not used to administer any system components.
6. Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: authentication mechanisms must be assigned to an individual account and not shared among multiple accounts; physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.
7. All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted.
8. Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.

Requirement 9: Restrict physical access to cardholder data.

1. Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

2. Develop procedures to easily distinguish between onsite personnel and visitors.
3. Control physical access for onsite personnel to the sensitive areas as follows: access must be authorized and based on individual job function; access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.
4. Implement procedures to identify and authorize visitors.
5. Physically secure all media.
6. Maintain strict control over the internal or external distribution of any kind of media.
7. Maintain strict control over the storage and accessibility of media.
8. Destroy media when it is no longer needed for business or legal reasons.
9. Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.
10. Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.

2.3.5. Goal 5: Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

1. Implement audit trails to link all access to system components to each individual user.
2. Implement automated audit trails for all system components to reconstruct various events.
3. Record at least the following audit trail entries for all system components for each event: user identification; type of event; date and time; success or failure indication; origination of event; identity or name of affected data, system component, or resource.
4. Using time-synchronization technology, synchronize all critical system clocks and times and ensure correctness when acquiring, distributing, and storing time.
5. Secure audit trails so they cannot be altered.
6. Review logs and security events for all system components to identify anomalies or suspicious activity.
7. Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis.
8. Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.

Requirement 11: Regularly test security systems and processes.

1. Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.
2. Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.
3. Implement a robust methodology for penetration testing.
4. Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network.
5. Deploy a change-detection mechanism to alert personnel to unauthorized modification of critical files.
6. Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.

2.3.6. Goal 6: Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel.

1. Establish, publish, maintain, and disseminate a security policy.
2. Implement a risk-assessment process.
3. Develop usage policies for critical technologies and define proper use of these technologies.
4. Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
5. Assign to an individual or team various information security management responsibilities.
6. Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
7. Screen potential personnel prior to hire to minimize the risk of attacks from internal sources.
8. Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data.
9. Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data.
10. Implement an incident response plan. Be prepared to respond immediately to a system breach.

2.4. PCI PIN Transaction Security Standard

In May 2010, the PCI SSC established a consolidated set of standards for manufacturers to build point of interaction (POI) payment devices. Rather than setting a standard for each type of POI device, such as point of sale terminals, ATMs, and mobile phones, the new PIN Transaction Security (PTS) POI covers all payment devices that handle PINs. These requirements were effective immediately, not actually mandated by any of the card associations until April 30, 2011, for all new device certifications, at which time the previous set of requirements was sunset.

Remember,

"Perfect Security is a Myth.... Effective Security is Achievable."

The following diagram shows the position of the ATM within the domain of the Data Security Standard, the controlling standard for payment providers. As you can see, there are three standards that, when implemented, provide the required security for the processing of card transactions involving PINs, PANS and other card data.

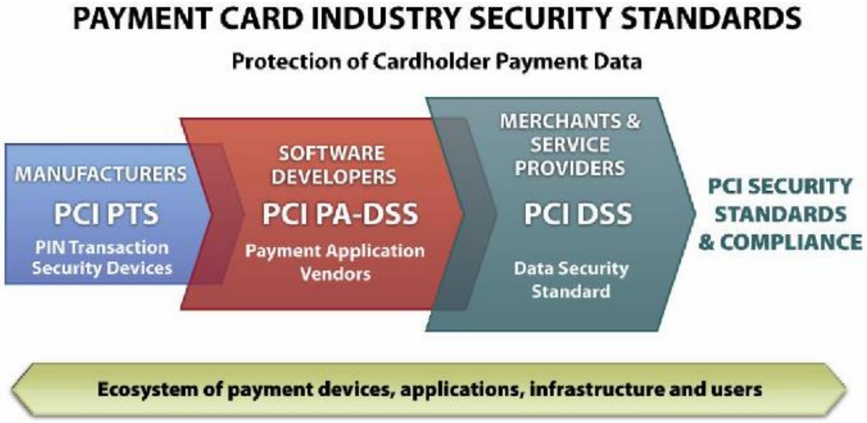

PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data
MANUFACTURERS
PCI PTS
PIN Transaction Security Devices
SOFTWARE DEVELOPERS
PCI PA-DSS
Payment Application Vendors
MERCHANTS & SERVICE PROVIDERS
PCI DSS
Data Security Standard
PCI SECURITY STANDARDS & COMPLIANCE
Ecosystem of payment devices, applications, infrastructure and users

Figure 7: PCI Security Domains and Standards

(© 2010 PCI Security Standards Council LLC)

The PCI PTS unites three previous standards, including PCI EPP, PCI PTS, and PCI PIN. All are focused on manufacturers designing equipment that secures PINs in payment devices.

The Payment Application-Data Security Standard (PA-DSS) addresses the application stack on the ATM that reads, processes, and/or transmits card data. The PCI DSS is the standard that all parties which store, process and/or transmit cardholder data must implement and maintain in order to be compliant and therefore allowed to process card transactions.

2.5. PCI PTS POI ATM

In January 2013, PCI released v1.0 of its ATM Security Guidelines, which is an Information Supplement to the PTS POI standard, and which "proposes guidelines to mitigate the effect of attacks to ATM aimed at stealing PIN and account data." The document contains best practices which are "not intended to be used as requirements for a validation program at the PCI SSC."

The document views ATMs from four perspectives, for each of which it lists various security objectives followed by guidelines and best practices aimed at achieving those objectives. The document also includes an annex discussing the design of privacy screens.

Below is a selected extract from the document, showing the four perspectives and their security objectives.

2.5.1. Integration of Hardware Components

A1: Avert physical local attacks that target account data.

A2: Avert physical local attacks that target PINs.

A3: Avert attacks aimed at stealing cryptographic, sensitive data stored in secure components.

A4: Avert attacks to disable security countermeasures added to the ATM.

A5: Mitigate potential negative impact stemming from the integration of service modules into ATMs.

A6: Protect against unauthorized access to sensitive areas and resources in the cabinet, including the fascia.

A7: Produce a security configuration of the ATM model.

A8: Provide security guidelines for hardware and software integrators.

A9: Provide security guidelines for service staff.

A10: Ensure that removal or unauthorized access to the EPP triggers an alarm.

A11: Prevent modifications of the hardware that may reduce the security protection level.

A12: Secure the communications between modules within the ATM.

A13: Contactless data should be secured to 16 points from the point of digitization of the data.

2.5.2. Security of Basic Software

B1: Prevent abuse of OS and reduce the attack surface of the ATM OS platform (Windows) and BIOS.

B2: Prevent exploitation of public domain vulnerabilities in the Open Protocols stack.

B3: Reduce attack surface from public and private networks.

B4: Prevent abuse by software suppliers.

B5: Use effective network isolation and intrusion detection/mitigation tools.

B6: Trace/log OS activity.

B7: Protect sensitive functions and enforcement mechanisms for appropriate key-loading procedures.

B8: Protect against unauthorized changes.

B9: Protect against the unauthorized remote control of the application.

B10: Protect against unauthorized installation of software.

2.5.3. Device Management/Operation

C1: Put in place adequate controls for the device’s production, transportation, storage, and use throughout its life cycle until initial deployment.

C2: Ensure adequate cryptographic initialization and service.

C3: Ensure secure distribution of software, updates/patches that impact security, and non-financial applications, including advertisements.

C4: Manage an updated inventory of ATMs and their configurations, including their hardware, software, logs and reports.

C5: Manage the life cycle, from manufacturing and initialization through decommissioning.

C6: Specify and execute proper security decommissioning procedures.

C7: Ensure the spare parts and decommissioned ATMs or parts have keying information and other sensitive data removed.

C8: Support user education at the ATM.

2.5.4. ATM Application Management

D1: Enforce best practices for application development, testing and distribution.

D2: Ensure the effectiveness of security functions driven by the application.

D3: Ensure the ATM application interacts securely with the ATM display and EPP.

2.6. Cryptographic Hash Functions

A cryptographic hash function is an operation which creates a hash code from input data and should be one-way (i.e., the original input data cannot be derived from the output hash) and collision-free (i.e., different input data will generate different hashes).

There are many different hash functions, some of which are now deemed obsolete, generally because techniques have been developed to create collisions. In particular, the MD5 and SHA-1 algorithms are unacceptably weak, whereas the SHA-2 set of algorithms is considered to be acceptable.

ATMs may employ hash functions for many purposes, such as software verification, remote key distribution, SSL certificates, SSL cipher suites, and more. ATMs should only use strong hash functions, such as SHA-2.

PCI PTS POI v3 expressly prohibits SHA-1 and allows SHA-2.

Note: *PTS POI standard's "overall requirements for unattended PIN-acceptance devices currently apply only to POS devices and not to ATMs," but PTS POI does apply to ATMs' components, such as encrypting PIN Pads and secure card readers.*

PCI DSS requirement 3.4 is to "render PAN unreadable" optionally using "one-way hashes based on strong cryptography". Given their published weaknesses, MD5 and SHA-1 cannot be said to be strong cryptography.

PCI does accommodate some exceptions. For example, the PTS POI FAQs state that "the initial code on ROM that initiates upon the device start may authenticate itself using SHA-1" and also that it is acceptable to use "parallel implementations of remote key distribution using asymmetric techniques, one supporting SHA-1 and the other SHA-2." Nonetheless, even if permitted by PCI, the best practice is to never use MD5 nor SHA-1 and to only use SHA-2.

2.7. Ensuring Harmony between Software Operational Policy and PCI

2.7.1. Secure Coding Practices

To be compliant with the PCI Standards, we remind the reader that commercial off-the-shelf ATM applications that process cardholder data must meet the requirement of the PCI Payment Application - Data Security Standard (PCI PA-DSS).

This standard is aligned with the PCI DSS requirements but distinct from the latter and specifically directed to application security and facilitating PCI DSS compliance. PA-DSS is a comprehensive set of requirements designed for payment application software vendors to facilitate their customers' PCI DSS compliance. PCI PA-DSS standards apply to commercial applications that take part in transaction authorization and/or settlement, and are designed to protect the storage, processing, and transmission of cardholder information by payment applications. PCI PA-DSS consists of the following requirements:

- Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), expiration date, service code, PVV, PVK, or PIN block data.
- Protect stored cardholder data.
- Provide secure authentication features.
- Log payment application activity.
- Develop secure payment applications.
- Protect wireless transmissions.
- Test payment applications to address vulnerabilities.
- Facilitate secure network implementation.
- Facilitate security of software algorithms.
- Cardholder data must never be stored on a server connected to the Internet.
- Facilitate secure remote access to payment applications.
- Encrypt sensitive traffic over public networks.
- Encrypt all non-console administrative access.
- Maintain instructional documentation and training programs for customers, resellers, and integrators.

This comprehensive standard is intended to help organizations minimize the potential for security breaches due to flawed payment applications, leading to compromise of full magnetic stripe data.

Guidance for web applications development can be found at:

- Open Web Application Security Project (OWASP) http://www.owasp.org/index.php/Main Page

- Other good references are SANS and Cert. In fact, these guidelines are called out within the PCI-DSS Requirement 6 itself and should be followed.

The Top 10 vulnerabilities identified by OWASP (2013) are:

- Injection
- Broken Authentication and Session Management
- Cross-site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Known Vulnerable Components
- Invalidated Redirects and Forwards

For a detailed description of these and recommendations for mitigation, visit the OWASP web site listed above.

2.7.2. Maintenance

The PCI DSS standard Requirement 6 refers to patching the systems. This includes system-level patches, custom code patches, and patches to other third-party applications used within the card processing infrastructure.

The PCI SSC provides the following guidelines with regards to unsupported operating systems within its FAQs: Are operating systems that are no longer supported by the vendor non-compliant with the PCI DSS?

PCI DSS Requirements 6.1 and 6.2 address the need to keep systems up to date with vendor-supplied security patches in order to protect systems from known vulnerabilities. Where operating systems are no longer supported by the vendor, OEM, or developer, security patches might not be available to protect the systems from known exploits, and these requirements would not be able to be met. However, it may be possible to implement compensating controls to address risks posed by using unsupported operating systems in order to meet the intent of the requirements. To be effective, the compensating controls must protect the system from vulnerabilities that may lead to exploit of the unsupported code. For example, exhaustive reviews may need to be regularly performed to ensure that all known exploits for that operating system are continually identified and that system configurations, anti-virus, IDS/IPS, and firewall rules are continually updated to address those exploits. Examples of controls that may be combined to contribute to an overall compensating control include active monitoring of system logs and network traffic, properly-configured application whitelisting that only permits authenticated system files to execute, and isolating the unsupported systems from other systems and networks. Note that these examples may complement an overall compensating control, but these examples alone would not provide sufficient mitigation. The use of compensating controls should be considered a temporary solution only, as the eventual solution is to upgrade to a supported operating system, and the entity should have an active migration plan for doing so. For assistance with compensating controls and for questions about whether a specific implementation meets PCI DSS requirements, please contact a Qualified Security Assessor.

2.8. What Can Be Done to the ATM to Comply with PCI DSS, PCI PA-DSS, and PCI PTS Requirements?

The following are best practice tools, processes and procedures to bring an ATM into compliance with the requirements of the PCI standards. The following is not an exhaustive list, nor are the listed suggestions the only means to address the requirements.

- Minimize and harden the base operating system.
- Follow your ATM Vendors' security hardening guidance. Many ATM Vendors thoroughly test security hardening procedures specifically for the ATMs they manufacture. Many also offer additional security applications (such as anti-virus agents) that have been specifically tested for their ATMs.
- Alternatively, the Center for Internet Security (CIS) provides security benchmarks and templates to harden and minimize many popular operating systems. These may require testing and customization for your particular ATM. http://www.cisecurity.org
- Use only PCI certified EPPs, and use them for both PIN entry and the entry of cryptographic data, such as encryption keys.

- Disable all unneeded EPP commands and parameters.
- Implement anti-skimming controls and measures.
- Install shields over PIN Pads to prevent PIN disclosure via shoulder surfing.
- Develop secure applications following the PCI-DSS standard (or use PA-DSS validated commercial off-the-shelf ATM applications).
- Implement two-factor authentication for ATM management features or enforce strong password controls.
- Install, configure, and maintain a firewall and firewall rule set on the ATM.
- Provide for secure communication from the ATM to the financial host. An SSL implementation in native mode is appropriate but make sure proper certificates are used and validated by the ATM.

  Note: *This will not authenticate the ATM to the network unless client-side certificates are used and validated by the gateway.*

  Another option is to support IPsec with both encryption and authentication options.
- Protect the communication link between the card reader and system or use an encrypting card reader.
- If possible, protect the communication link from the EPP to the processor. If using a USB connection, make sure that a USB sniffer cannot be introduced to the channel to read the encrypted PIN blocks.
- Install a reputable file integrity monitoring application to prevent the insertion of malware and provide a forensic audit trail. Protect audit and log files from alteration or deletion.
- Maintaining and monitoring physical security of each deployed ATM is vital. Although outside the scope of this guide, physical security that prevents access to ATM internals for illicit purposes will ensure that these software-based best practices cannot be bypassed through physical force.

2.8.1. Case Study: ATM Software Distribution

A top US financial institution with several thousand ATMs deployed decided to deploy a new, custom, Windows-based ATM software application. The decision was driven by the desire to improve the marketing content and value of their ATM fleet. However, the ATM network management group recognized the need to maintain the security of the ATM environment and plan for more frequent software updates than had been experienced with OS/2-based ATMs:

- Distribution of marketing content to ATMs to support ongoing sales campaigns would require new and multiple screens to be distributed with controls needed to schedule the start and end of each campaign.

- With a new software application being deployed, regular patch updates, for functionality and security, were expected for both the software application and operating environment.

To make the expected volume of ATM software updates practical by avoiding the cost of services calls to each ATM for every update, this institution chose to deploy a software distribution tool to their ATMs from the outset of the project. They chose to use their enterprise infrastructure by deploying a Tivoli-based system, which allowed them to schedule distribution, installation of distributed content and software patches, and reboot ATMs if necessary to complete installations.

This decision has proven wise for this financial institution. Distributions of content and software patches to more than 1,000 ATMs today take place once a month or more, without any service calls to the ATMs.

Some practical learning from experience to date:

- Controlling the portion of communications bandwidth used for software distribution is critical. On some off-premises ATMs with 8kB/s Class 1 frame relay capacity, distribution can easily consume 100% of the communication bandwidth, effectively taking the ATM out of service.
- Patches can be scheduled to download at midnight or 1am to avoid customer impact. Large patches can take many hours to distribute; one patch distribution started at midnight and took 10 hours to complete installation and begin rebooting ATMs at 10am. The *stop download at* time parameter, initially ignored, is important to set correctly.
- Some very large software updates can take days to distribute to ATMs with lower communication bandwidth. The distribution system needs to tolerate the timing needed to distribute the largest patch over the slowest communications link in the network; timeout parameters must be set to allow this distribution to be successful. In cases where a distribution is time-critical, allowing distribution to use a greater portion of available bandwidth will need to be evaluated.

Chapter 3. ATM Security Governance

This chapter provides guidelines for ATM network managers to assess security requirements and select security solutions for the ATM networks under their responsibility.

In today's security-conscious world, the complexity of our software systems makes logical security a complex and specialized discipline. Expert advice is needed to take the proper security measures for ATMs and other technology systems. However, security measures greatly differ from one system to another. Many IT security professionals face ATM network security as a new challenge and usually they will first need to understand the complexities and limitations that one finds when managing and operating a financial self-service network.

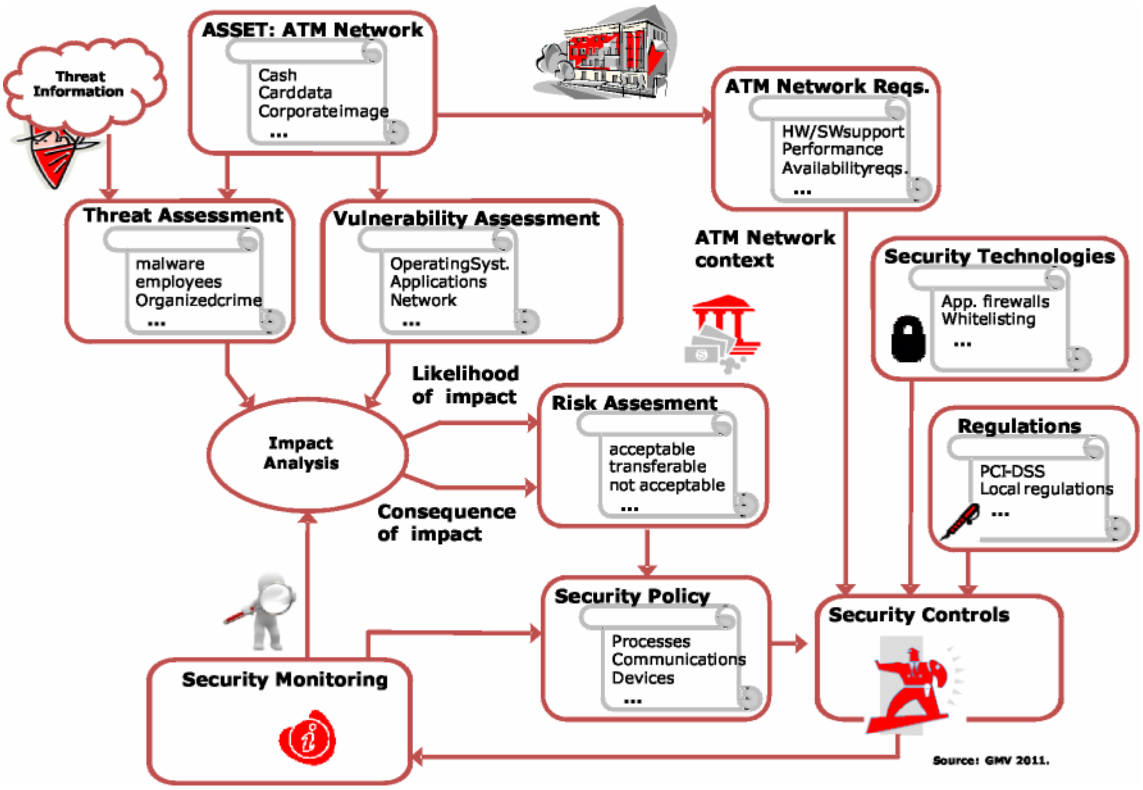
Similarly, it is important for the ATM expert to understand how security professionals approach the problem of securing a network, the meaning of relevant terms, and how to secure the system. This chapter aims to introduce the ATM manager to this discipline.

In exploring ATM software security, we will define lifecycle security to mean all ATM systems security controls implemented during development, continual maintenance, decommissioning, and cleansing of any sensitive information. Throughout the entire ATM lifecycle, security must always be considered concerning technology, people, and processes.

3.1. Security Engineering, Controls, and Governance

Security software products like firewalls and anti-malware, combined with secure configuration and secure operational procedures, are examples of what are commonly referred to as security controls. The selection of proper security controls for ATMs seems to be the obvious problem that the ATM network manager has to solve. However, this selection is only a fraction of the work that needs to be done in order to ensure that ATM networks are built and remain dependable in the face of malicious actions, attacks, or mismanagement. The design and development of such dependable systems is known as security engineering. The process of establishing and managing security in those systems is known as security governance.

Security professionals usually follow a well-established process in order to select appropriate security controls. This process is outlined in the following figure (and slightly simplified).



Source: GMV 2011.

Figure 8: ATM Security Governance Scheme

The process starts by understanding the value of the asset to be protected, in our case a self-service network. This includes not only the ATM itself, but also other important assets like the reputation of the financial institution. This is important because security comes at a cost, and it makes little sense to expend lots of money to secure assets of little value. Once this is understood, the next step is to assess the threats that endanger our assets and the vulnerabilities associated with these assets. This is not as easy as it might seem, since threats are difficult to foresee and all systems have unknown vulnerabilities. Often you have to make educated guesses.

Understanding threats and vulnerabilities is necessary in order to perform an impact analysis. For any identified threat, the first step is to assess whether the current ATM network is vulnerable to it. If so, produce a description of the unwanted results if the vulnerability is exploited. As a result of the analysis for the relevant vulnerable points and associated danger situations, you can determine the likelihood and consequences of an impact to the ATM network.

At this point a risk assessment is performed. A risk assessment consists of enumerating the previously identified situations, computing some associated risk for every one (either qualitatively or numerically) and determining whether each risk is either acceptable (live with the risk) or not acceptable (do something to reduce or mitigate the risk). Do not think in terms of eliminating the risk, but rather of reducing it.

There is also a third possibility, which is to transfer the risk. This is what you do, for instance, when you buy insurance for your car. In the case of ATM networks, risk transfer would be typically be accomplished by outsourcing some or all of the ATM operations.

Where risk transfer is desired, operations outsourcing should be considered broadly and together with all relevant implications. For instance, if you outsource cash management then some threats related to fraudulent cash withdrawal might become the concern of the outsourced company. Some financial institutions transfer some risk in their ATM fleets by having another organization operate it for them. The main problem of risk transfer in ATM environments is damaging the reputation of the financial institution; this is the impact on your institution from appearing on the news and being affected by ATM fraud or a compromise of confidential customer information.

When you know which risks you want to reduce, the value of the affected assets, the likelihood and impact of an exploit, and the cost to fix it, you have a better understanding of what steps to take next. The typical solution is to put additional security controls in place. In order to select appropriate controls, the best approach is to use security best practices. This is quite convenient for well-known scenarios (e.g., e-commerce portals), but might be tricky for an ATM network for three reasons:

- ATMs have special business requirements since they operate 24x7, are mission critical systems, and are highly visible to the public. There are many conditional business requirements that must be taken into account (e.g., would an antivirus application degrade the performance or reliability of the ATM?).
- Second, the threat is rapidly evolving and we need a self-improving security management model, known as Deming circle or PDCA (Plan-Do-Check-Act). For example, see http://www.balancedscorecard.org/TheDemingCycle/tabid/112/Default.asp. This approach is able to cope with emerging threats and the evolution of technologies.
- Finally, the specifics of an ATM might give us some advantages. Although an ATM is simply a PC with a lot of peripherals, its software is not changed very often and is always done in a controlled manner. The user interacts with the ATM in very limited and well known ways and it generally does not have the latest and most powerful CPU or memory configuration.

Summary: Security Governance includes security controls, vulnerability assessment, risk assessment, and security policy.

The intention of this document is to provide specific and concrete ATM security best practices and establish ATM-appropriate security policies which we will later use to select our security controls.

3.2. Introducing Security Policies

An ATM Security Policy can be simply defined as some set of rules stating what is acceptable and what must be controlled or even forbidden in our ATMs. Suppose for instance that one risk you want to reduce is the possibility that some malware is introduced in the ATM. You might state the rule, "only approved executable programs must be allowed to run." You might also forbid the use of USB storage devices altogether in the ATM maintenance process to reduce the risk of somebody extracting sensitive data. Policies need not involve technology; for instance a policy rule could be a password to access an ATM must be split between at least two people.

All policies, while reducing risks when enforced, may make your life more uncomfortable in other ways. For instance, what if you want to run some unapproved test program or your maintenance personnel are routinely using USB sticks? Well, this is why you perform risk assessment. You look at the pros and cons, decide which security policy you want in place, and then and only then, you select the appropriate security controls. The bottom line is do not put security in place for the sake of security. Do it only when there is a well-identified risk that you want to reduce, and take into consideration all the collateral effects of imposing the policy before you make the decision.

Now let us talk about how security policies can be enforced. Security controls are technological, procedural, or administrative protections that enforce security policies. As an example of a procedural control, think of the above mentioned rule: a password to access an ATM must be split between at least two people. The control should be some procedure that ensures that is indeed the case.

Selecting technological controls is somewhat different because you must be aware of state-of-the-art security technology and also understand how these controls may impact your ATM network.

Several options are available on the market to help reduce and mitigate the risks associated with an ATM network. After all, an ATM is a hardened PC with specific peripherals, and software to secure PCs has existed for a long time. However, the majority of PC security products have evolved for typical office computer environments, whose particular characteristics (stability, frequency of updates, connectivity, service needs, performance, etc.) are quite different to those of the financial self-service environment. PCs have interactive users of the operating system while ATMs have users that see only a single locked-down application.

Controls might also be imposed by regulations. For instance, PCI-DSS requires you to use a firewall to control communications. Regulatory and statutory compliance requirements will therefore influence your selection of controls.

Finally, your security controls must include monitoring capability that you use on a regular basis to analyze whether security conditions arise (e.g., alarms or warnings). Monitoring of your set of security controls is a very strong security control itself, and it's recommended alongside every other security control you put in place. This provides valuable information that you will use to improve your knowledge of the threats and your actual exposure to them. You will later use this knowledge to enhance your security controls.

In the rest of this chapter we are going to review these aspects – asset value, threats, vulnerabilities, security technologies, security policies and security controls in more detail.

3.3. Assets Exposed by your ATM Network

Let us start by discussing the value of your ATM network. It is unnecessary to emphasize its value as a first line channel with your customers. It must be usable, largely available, and extremely reliable. Downtimes must be reduced to a minimum. Physical security, design, and accessibility, all of these are features well studied. What about logical security?

There are essentially three valuable assets that are at stake if your network is compromised:

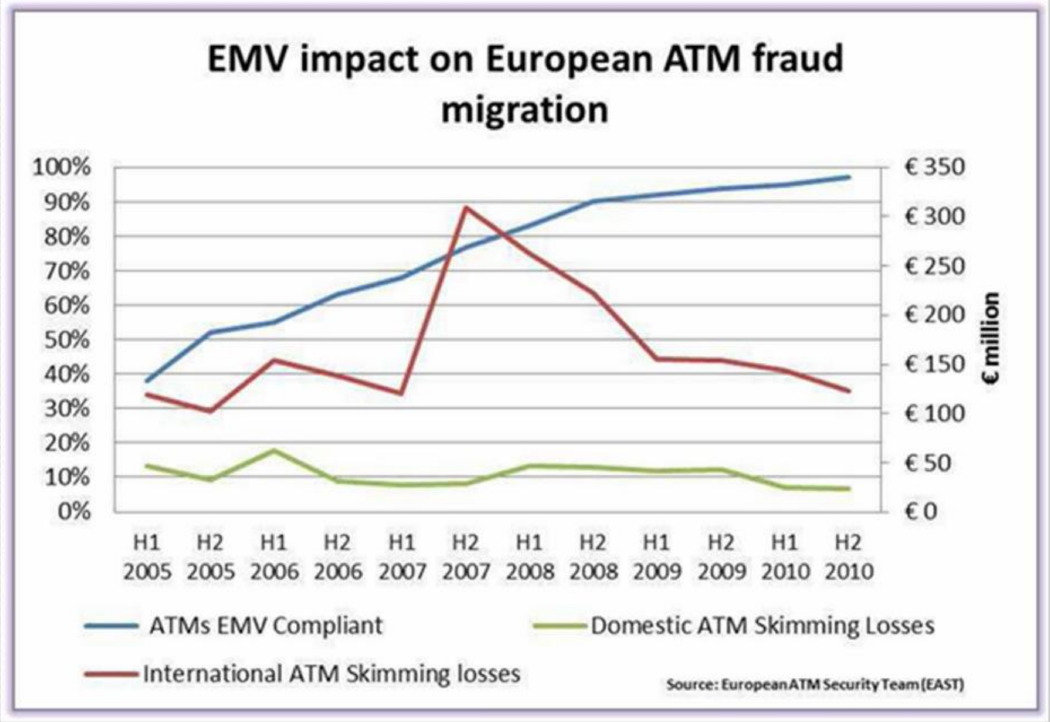
- Your cash
- Your data
- Your company's image

Cash is important, but it may not be the most important asset. Consider the possibility that specialized malware might be stealing card data from your ATMs. This might go on unnoticed for years, and the related fraud might result in substantial financial impact and loss of image. Or even worse, consider a defacement attack where all your ATMs show an inappropriate video when your customers access them or a scenario where all your ATMs are used as remotely controlled PCs used to perform Distributed Denial of Service attacks to a corporation or even to your government. So, how much do you value your data or your corporate image?

You know very well the importance of protecting your ATM network. At this stage you might be thinking, "Well, these situations are clearly unwanted, but do they reflect realistic scenarios? Are these situations really possible?"

3.4. Threats to ATM Networks

You may have heard that the world is experiencing a paradigm shift regarding cyber-attacks. Worldwide criminal gangs are currently pursuing low risk, sustainable sources of revenue and it is a matter of time before many criminals in modern countries join this emerging criminal chain and target attractive assets in an organized manner. In this respect, there is no doubt that an ATM network is an attractive asset. ATMIA and other organizations have been tracking ATM attacks for a number of years. Early attackers were not well organized and tended to go for the easier physical attacks like ram raids, cash-in-transit attacks, cash/card trapping, and attacks on the ATM safe. Attackers became more organized and adopted better attack technology, which led to a rise in skimming attacks – which in turn led to deployment of EMV chip-and-PIN cards which has reduced skimming attacks and counterfeit card crime.



Source: EuropeanATM Security Team (EAST)

Figure 9: EMV Impact on European ATM Fraud

(European ATM Security Team, June 2011)

Attacks on ATM networks by well-organized and highly sophisticated criminal groups is a clear trend nowadays in Eastern Europe and Latin America, and will become an uncomfortable reality in the most advanced countries very soon.

As attacks to steal money and data become more and more common, there is an even newer trend emerging: groups of hackers who decide to attack some target because of publicity to promote their political agenda, or in pursuit of some other non-monetary gain. Recent examples include the Anonymous group's attacks or the Stuxnet malware.

Summary: Our ATM infrastructure is now under cyber-attack. Criminal gangs are currently pursuing low risk, sustainable sources of revenue and attacks against ATMs in a highly sophisticated way.

This is a reality today in many countries.

3.5. From Physical to Logical Fraud

Traditionally, much attention is paid to preventing thieves from stealing the most obvious asset in an ATM, cash. Many physical security controls are in place in modern ATMs to protect against known threats, such as ram raids and explosive attacks. Most ATM network managers have long believed that their ATM's network security is reasonably managed by implementation of these controls.

More recently, increases in card fraud have resulted in the appearance of an underground card data market. Today, criminals can easily sell card data over the Internet for a profit and thus it is only natural that they strive to obtain this data. Of course ATMs are an obvious source of PINs and magnetic stripe data. As ATM attacks shift to compromised card data, ATM security focus is shifting to ensure that proper security controls are also in place to prevent card and PIN data theft from the self-service network. However, in order to select the proper software security controls, it is necessary to understand the threat. Well known attacks such as card skimming are already being addressed (for instance through EMV initiative). Still, there are new threats which are far from evident and are also rapidly evolving.

ATM networks are rapidly becoming subject to emerging threats which are usually poorly understood by ATM network managers. Part of the problem is probably that theft of card data from an ATM does not immediately result in a loss for the ATM network itself, but for the financial entity behind the data. An ATM owner may not necessarily bear any part of the loss from a data compromise. Furthermore, recent evidence suggests that many security incidents in ATM networks are currently not detected and thus the rate of occurrence of breaches is generally underestimated. Surprisingly, what appears to be a new promising business for criminals is getting so little attention from ATM network managers.

In order to understand how this is possible, let us first discuss what would be the best strategy that a criminal could follow, for instance, to obtain card data from an ATM that he could later sell on the market. Criminals focus on three basic aspects:

- The effort must be worth the risk of being caught.
- This risk must not surpass some acceptable level.
- They prefer tactics that would provide sustainable revenue more than actions that would result in short-term profit. Sustainable revenue usually comes from a situation where assets (data or cash) are stolen regularly and without notice.

If criminals would come with a truck and steal a single ATM (or, less dramatically, install some hardware device on it like a dispenser trapper), they would obtain money and/or data. But this would require a great effort and would provide limited profit. On the other hand, if they could somehow, and without being noticed, get their hands on card data from an ATM on a regular basis, they would sell the data and thus have a source of sustainable revenue at a very low risk.

One could think of two ways to achieve this goal. If the criminal (or an accomplice) has periodic access to an ATM (say he is in charge of some sort of maintenance task), all that is needed is some knowledge and tools in order to obtain this data. This has been the main approach for some time. However this possibility is reduced to a limited number of people and therefore the associated risk of being caught is higher. At the same time, the card fraud market is becoming commoditized and the price of the stolen magnetic stripe data is decreasing. This, as in any other business, is demanding from the criminals a higher degree of sophistication in order to decrease risk (of being caught) and increase the amount of stolen data (or its quality, e.g., knowledge of customer profile associated to the data) and also decrease the effort to obtain it.

In this scenario, as in most technology-based businesses, the threat is rapidly evolving. For instance, if criminals just manage to have access to the ATM at a particular time (instead of on a regular basis), they can inject some malicious software and later collect the data using the ATM printer or send it over the network. The well-known Skimer malware that expanded in a few countries at the end of 2008 did just that. And, once you manage to introduce malware in the ATM, why not use it to withdraw cash? Indeed that is what Skimer malware is able to do; by means of a particularly built card you can instruct the infected ATM to dispense cash. The cash that disappears does not belong to a particular customer, and tracing the loss is sometimes difficult. Moreover, in the very near future this type of malware is expected to behave as a worm and be able to self-replicate in a network, thus reducing the exposure of the criminals and increasing their revenue expectations.

At a first glance it may seem that building this kind of malware is quite a sophisticated task, and it is indeed. However, most criminals do not build their malware; they buy it from organized criminal gangs just the same as they can later sell the obtained card data. These malware kits are available and are quickly becoming inexpensive. This criminal specialization is at the very core of the new threat model that we are facing.

Summary: Criminal gangs always look for less risky and more profitable business; ATM crime is evolving from high-risk, low-profit theft of cash to relatively low-risk, high-profit theft of card data through logical attack.

3.6. Basics on Vulnerabilities

The arrival onto the financial self-service scene of open operating systems, such as Microsoft Windows, together with the use of IP networks for communications services and standards like XFS, have brought lots of advantages to ATMs in terms of interoperability, reduced costs, reduced time-to-market and the sort. These changes have also resulted in considerable increase in security risks for ATMs as a direct consequence of the vulnerabilities which are common to all open systems.

Vulnerabilities are essentially weak points in the computer, its programs, or its concept which could be used to overcome the security of the ATM. The ATM includes a set of hardware and software products (the devices, drivers, operating system, application programs, etc.) which operate in an ordered manner following a chain of processes. The security of the ATM depends upon the security of the weakest link in the chain. In many cases, the operating system is this weakest link, both due to its design as well as its central control position in the ATM. On the other hand, if the operating system is properly hardened (secured) then there will be a different weakest link. Just as it is unrealistic to assume that any piece of software is completely free of bugs (except for very high quality and expensive software such as for the space industry), we have to assume that vulnerabilities exist and ATM deployers must adapt to this reality.

The nuts and bolts of how vulnerabilities are used by hackers in order to break into an operating system, penetrate a network, or compromise an application are technically sophisticated and a detailed discussion is out of the scope of this document. But regardless of the effort made by manufacturers or developers, it is unfeasible to achieve complete security. To make things worse, ATMs are usually accessed by personnel and securing a computer against someone with physical access and enough knowledge is essentially impossible.

So it is easier than one might think for an attacker to take control of an ATM device without proper software security measures from a remote user station with access to the ATM network. Without the protection of software security best practices as described in this document, it is uncomplicated for a knowledgeable criminal to introduce malicious processes in the ATM, relatively easy to download already existing files containing sensitive information to USB storage devices, and also easy to inject code that intercepts peripheral drivers and, for instance, dispenses cash.

Summary: Most attacks come from inside – employees, outsourced personnel, security, or operations.

3.7. Express ATM Security Policies and Defend ATMs

We can imagine an ATM-specific security product as software that is installed between the operating system and the resources of the ATM in order to ensure the use of resources conforms exactly to the expected use. The term resource includes files, peripherals, and everything controlled by the operating system. In this way, a large number of attacks may be detected as unexpected use and countermeasures are immediately taken to avoid damage and warn managers. It is this concept of conformance or compliance in the use of the resources which leads us to the quite interesting concept of ATM security policy.

A security policy is a set of rules, principles, and practices which determine the manner of implementing and managing security in a particular environment (in our example a financial self-service network). Once a security policy is established, it is possible to design and implement a well-reasoned set of security controls. Controls will be selected so as to ensure compliance with policy, and when this is not the case, detect and report on non-compliance.

The power of security policies is that they allow you to select the security controls that you need. A security policy should also be able to help in the selection of a balanced set of procedural, administrative, and technical controls for a particular scenario.

Specifying a security policy for your ATM network will enable you to select the proper security controls. This selection is an important task which is often disregarded. In many cases it is relatively common to introduce security controls into the information systems without having previously specified a security policy.

Sometimes one could argue a best practices reason, but quite often this is just a sign of the threat being poorly understood. In fact, it is not easy to define policies for complex environments because they intrinsically involve difficult cost-benefit analyses. In some cases, regulatory compliance poses a pressure on time, which combined with the lack of security incidents (or detected security incidents), could conceivably force managers to install some generic control which later is shown to be inadequate.

A final problem arises when, even with a good understanding of the threat, the controls required are too numerous and complicated. And this is indeed the case of ATMs where we have seen one should control execution, file access, peripheral access, communications, and a number of other subtleties which would imply the installation of several (four or more) generic security products. In turn this would result in a security management nightmare in terms of operational costs, products training, performance issues in ATMs, significantly more updates, and different management consoles.

Ideally, we would require just one ATM security product that would do three simple things:

- Provide for the generation and management of ATM-specific security policies which could automatically be translated into rules for security controls.

- Enforce these rules regarding execution, access, communication, or other security requirement using one single, low footprint security product in the ATM.
- Provide for centralized monitoring of compliance, including all required audit features.

The state-of-the-art security today that we have reviewed allows such a product. We have seen how an ATM is a stable environment where the use of resources is predictable. One could conceive a security product that would monitor the ATM, generate security policies based on its expected behavior, and then enforce that security policy embedding all necessary controls. For example, one could think of a security policy expressed as a set of rules that limit the access and usage of ATM resources, which could be structured and centrally stored in a file which is in turn securely sent to the ATM in order to become enforced.

A security policy should not be an abstract concept, but a very specific concept which enables delivery and enforcement of all aspects of security to ATMs in an understandable and manageable way. The rules admitted should have to be quite diverse; some examples could be no process except for xxx may modify file yyy, only Java class zzz may access the library for access to the dispenser, or no system outside of the ATM may access communications port 12345. These rules must be organized so as to cover all required security protections the ATM would require.

3.7.1. Case Study: Security Governance at a Financial Institution

A Spanish bank with thousands of ATMs distributed throughout Spain has implemented a comprehensive security governance program for its ATM network and equipment. The ATM network is composed of ATMs from several different manufacturers but the whole fleet runs uses Microsoft Windows operating systems.

An organizational structure was created and a team formed with both security and ATM administrators. Policies, standards and procedures were defined and security assessments performed regularly. Security controls at different levels have been progressively implemented, including device control to disable sensible keyboard keys or USB drive access, local network firewalling and access control, whitelisting of processes, resources permitted, hardening of ATM operating systems and applications, and many others.

The ATM network is a critical asset of the bank and is governed as such, with tight control of its configuration and changes. Operating security controls are a critical consideration for the ATM infrastructure. Most of the security controls introduced are centrally managed through the definition and distribution of low level execution policies and the recompilation of events and alarms that also enable continuous monitoring of an ATM's state.

Chapter 4. Mapping Software Operational Policy: Ensuring Confidentiality, Integrity, Availability

A powerful way for information security professionals to assess any IT system's overall security is to consider the three pillars of security:

- **Confidentiality** is the ability of the system to resist inappropriate disclosure of information. It requires protection against data being inspected.
- **Integrity** is the ability of the system to continue to function in the way intended. It requires protection against tampering with the system.
- **Availability** is the ability of the system to remain in operation during expected time periods and with acceptable levels of service. It requires protection against denials-of-service.

The PCI Data Security Standard has several requirements applicable to ATM deployment (see 2.3 PCI DSS Requirements on page 21), and each of these requirements is associated with one or sometimes multiple aspects of confidentiality, integrity, or availability. This chapter will explore strategies to implement more secure ATM systems by considering both the PCI requirements and the three CIA pillars.

4.1. Introduction

Good ATM security governance leads to good ATM security strategies.

This guidance is all about ATM software security, but before we dig deeper into how you should plan to secure your ATM software, there is one important statement that must be made.

When we wrote the first version of this guide in early 2009, the vast majority of successful attacks against ATMs had not exploited the software running on the ATM. The most common ATM attacks at that time were physical ones (card skimming, cameras to capture PINs, ram raids, attacks against the safe, cash-in-transit attacks, and muggings enormously outnumbered reported attacks) against the ATM software.

However, starting in the first quarter of 2009, attacks that involve compromising the ATM software started being reported. Because advances in defending against physical attacks have made them more difficult, attacks against the ATM software are emerging; worldwide criminal gangs prefer these low-risk, sustainable sources of revenue and we anticipated this trend continuing. We should expect more attacks against the computer, the networks, and the ATM software, and indeed, we are beginning to see evidence that criminals have begun to target ATM software and ATM-specific vulnerabilities to extract cash and harvest customer card data. Attacking ATM networks in a well-organized and highly sophisticated way is now a clear trend in Eastern Europe and Latin America, and will become an uncomfortable reality in the most advanced countries very soon. There have also been some recent high-profile compromises of back-end systems that process cards that contribute to subsequent fraud at the ATM, adding to the need to protect the ATM environment as a whole.

Also consider that the situation with logical fraud is completely different and potentially more dangerous than physical attacks. Software breaches are silent and if your ATM environment lacks the right security tools to monitor and protect you ATM infrastructure you may not even be aware of an ongoing logical attack.

The goal of this guide is to help you prevent and fend off potential ATM software attackers.

Summary: ATM Logical Fraud is all about cyber-crime.

To help you understand and prepare for ATM security, there are several fundamental suggested principles that we have found useful to help in selection of technology, process, and people for your ATM systems:

- **Complexity is the enemy of security.** More complex systems are harder to analyze and harder to operate; if you have to make a decision between a simpler technology or process and a more complex system, the simpler one is likely to be more secure in the long run.
- **Practical security involves a moderate number of defense-in-depth techniques.** The best security posture for a system is to apply a manageable number of well-proven security layers. More security measures or more settings tweaked does not equate to more security. Use a small number of powerful but proven security techniques to secure your ATMs. For example, using network isolation, tested operating system hardening, secure operating processes, and central monitoring/management tools offers a good core set of layered security without adding undue complexity.
- **Deploying, operating, and troubleshooting ATMs are essential elements of security.** Most guidance focuses on the technology aspects of securing ATMs, and many ATM projects focus primarily on technology. However, a lack of secure deployment, secure IT operations, or secure troubleshooting can severely weaken any technology.

- **Rigid change control is the backbone of ATM security.** Every configuration or software change on an ATM has associated risks to integrity, availability, and confidentiality. Minimizing change is ideal, but you will need to make periodic updates to the ATM to ensure it remains secure and functioning properly. When you make these changes, the better the control you have over the process, the less likely you are to suffer confidentiality, integrity, or availability problems. The three aspects of change control (testing a change, controlling the implementation of a change, and tactical change to assist troubleshooting efforts) all need attention.
- **Re-use proven security practices.** Your IT organization will have existing security technology and operational expertise. If existing practices are well-aligned to the unique aspects of securing ATMs, they should be reused; because of the detailed development needed and the operational excellence demanded to make a more secure system, re-using standard approaches will help ensure better overall security. There are also several well-established sets of guidance materials from vendors and independent bodies, such as this guide.
- **The fewer times an administrator has access to an ATM, the better.** Each person with full administrative access to an ATM is a threat to its integrity. With well-defined operational and troubleshooting processes, the number of times a user can interact with an ATM using full administrative access should move toward zero. When you can clearly articulate the management and troubleshooting processes you need to keep your ATMs running smoothly, these processes can be made into automated tasks that do not require administrative access.
- **Remember that physical access to the ATM computer can overcome all software security.** No matter what security measures are applied in software, an attacker with unrestricted physical access to the computer hardware of an ATM, reasonable knowledge, and sufficient time can compromise the ATM. Many ATMs do have hardware security measures that help protect against such attacks, but keep in mind that physical security also plays a part in IT security.
- **Security solutions must not impact the availability of the ATM.** Because ATMs may lack computing power compared to a modern desktop PC and the ATM is a public-facing device that may run unattended for weeks or months without a reboot, performance of any security or management tool is critical. Be sure to evaluate the resource requirements for each tool and thoroughly test the full combination of layered security tools to make sure that the ATM can respond crisply to customers and can run unattended for extended periods.

- **The ATMs and all associated security tools must be remotely manageable.** Good management tools and good security tools will provide capabilities to perform all management tasks remotely, securely, on a schedulable basis, and without undue performance impact upon the computer being managed. Look for capabilities to remotely manage each tool you select and look for monitoring, reporting, and alerting functions that can inform you of security breaches. The following table lists the sections of the PCI Data Security Standard, indicates which principles (confidentiality, integrity, and availability) apply to that topic, and lists the main recommendations.

PCI DSS Section	Main CIA Principle(s)	Key Recommendations
1. Install a firewall	Confidentiality Integrity Availability	Consider a firewall that can limit network access to expected processes only. Allow admin access to an isolated ATM environment using a jump server.
2. Do not use vendor default passwords	Confidentiality Integrity	Use a centralized directory service or security agent to manage local authentication. Randomize local administrator passwords.
3. Protect stored cardholder data	Confidentiality	Store truncated or no PANs if possible. Strictly control logical access to any PAN data. Limit the ability to use removable storage devices at the ATM. Full-disk encryption may add some value.
4. Encrypt cardholder data on open networks	Confidentiality	Use SSL, IPsec, or a VPN on open networks. Consider using this even on less open networks.
5. Use and update antivirus software	Confidentiality Integrity Availability	Consider an anti-malware solution based on whitelisting as an alternative to traditional antivirus. Be cautious of false positives and performance issues with traditional antivirus.
6. Develop secure systems and applications	Confidentiality Integrity	Build ATM-specific criteria for rating patches. Follow rigid change control. If using whitelisting, be detailed and specific about the allowed software actions on the ATM.
7. Restrict access to cardholder data by business need-to-know	Confidentiality	Eliminate storage of full PANs at the ATM. If not possible, limit access to the ATM's users, processes, and libraries.
8. Assign a unique ID to each person with computer access	Integrity, Confidentiality	Use a centralized directory service or a local security agent that can identify each service user that logs on.
9. Restrict physical access to cardholder data	Confidentiality	Use device control to limit the ability to use removable storage devices at the ATM.
10. Track and monitor access	Confidentiality, Integrity	Use a centralized directory service or a local security agent that can identify each service user that logs on. Include remote monitoring of unexpected access to ATM system components.

PCI DSS Section	Main CIA Principle(s)	Key Recommendations
11. Test security systems and processes	Confidentiality Integrity Availability	Vulnerability scanning may be helpful. Integrity control software/whitelisting may be of interest. Limit the ability to use removable storage devices at the ATM. Tools that monitor and alert on unexpected activity at the ATM are recommended.
12. Maintain an information security policy	Confidentiality Integrity Availability	See details in Chapter 3: ATM Security Governance on page 36.

Note: *Carefully consider the sections of the PCI DSS titled PCI DSS Applicability Information and Scope of Assessment for Compliance with PCI DSS Requirements when planning the management and security of your ATM environment. A goal when planning for PCI compliance is to ensure the scope of the environment includes as few systems as possible!*

Some examples of controlling scope could be:

- *If deploying a directory service to handle authentication for high-level administrators and ATM supervisor application functions, deploy a directory service that is dedicated to the ATM estate, not one that is shared with other parts of the business.*
- *Use network isolation or network encryption techniques to ensure that cardholder data cannot travel to systems outside the ATM system itself.*
- *If deploying a whitelisting solution, be sure that your ATM environment is remotely managed and monitored from the security point of view.*

4.2. Installation and Monitoring

This section describes how secure approaches to ATM installation and ATM monitoring contribute to the overall security of the system and align with the confidentiality, integrity, and availability principles.

4.2.1. Security Aspects of ATM installation

First, let us examine how ATM software installation contributes to security.

The primary pillar that installation security seeks to preserve is integrity. During installation, the installer(s) will have physical access to the ATM's computer. It is also very likely to allow people to have full administrative access to the computer while the initial software installation occurs. The goal of a secure installation should be to ensure that the software initially deployed on an ATM has not been tampered with or misconfigured in any way, either intentionally or accidentally.

A secondary consideration in ATM software installation is availability. The time taken to install the ATM software is time that the ATM is out of service to customers. This lost availability will come into play during an ATM's initial installation or when the ATM must be reinstalled due to hardware or software failure.

There is also a consideration of confidentiality when installing an ATM. Knowledge of the ATM software configuration of an ATM hard disk will be of interest to attackers. And a hard disk that has been in use in a running ATM will be of even more value to an attacker because it may contain more complete configuration information and, more importantly, it may contain customers' transaction information.

Recommendations to improve the security of the ATM installation include:

1. **Make the ATM installation as low-touch as possible.** This will reduce the chance of tampering and should reduce the time needed to reinstall ATM software after a fault. Consider that each ATM has a personality and unique configuration settings needed to distinguish each ATM in the field. If this personality is stored centrally ahead of time, it can be used during installation in order to reduce the manual configuration required to make the ATM operational.

2. **Limit the need for the installer to use admin-level access to perform manual configuration.** Again, automating the installation process and/or storing the ATM personality and retrieving it automatically can help reduce or eliminate the need for the installer to have administrative access to the ATM. Instead of allowing unfettered access to the ATM as an administrator, consider including specific configuration items to the supervisor interface so that only tightly-controlled configuration changes are allowed.

3. **Consider how to troubleshoot installation problems.** There are bound to be installation issues in ATM estates of any size; having good tools and techniques for troubleshooting installation issues at the ATM or through central management can dramatically reduce the need for the installer to attempt to correct the ATM using powerful local privileges. For example:

    - Using centralized monitoring tools to retrieve detailed troubleshooting information about the ATM operating system and the ATM application stack can help pinpoint issues.

    - Troubleshooting actions available to the installer at the supervisor interface of the ATM will help reduce the need to log into the ATM with full administrative access.

    - The ability to reinstall the ATM software back to a known-good base image gives the installer the ability to have a 2nd (or 3rd or 4th) try to install smoothly. This is especially important if power or other environmental problems interrupt an installation.

4. **Stay away from hard-coded passwords that are part of the ATM disk image or are known to the installers.** Passwords that are hard-coded into the image would be visible and usable to attackers that obtain a copy of the ATM hard disk. A wider audience than intended will inevitably come to know standard administrative passwords that are known to installers. Some practical advice about administrative passwords that will both increase security and address PCI DSS items regarding vendor-default passwords include:

    - If you need hard-coded passwords to automate the install process, store the passwords somewhere on the network instead of in the image itself. This will mean that without network access, there are no passwords visible to an attacker who has possession of an ATM hard disk.
    - The user accounts and passwords for powerful administrators must be non-local to the ATM. Instead, administrators should use accounts from a central directory service. For example, Windows-based ATMs can be a member of a domain where centralized administrator accounts can be tightly controlled.
    - If an administrator password needs to be entered by the installer at some point during the ATM installation, change the password at the end of the installation so that the well-known password is no longer usable at the ATM.

5. Consider adding as much installation verification information as is practical to the supervisor panel of the ATM. For example, a verification function could include:

    a. The TCP/IP networking information about the ATM

    b. Whether crucial remote systems are visible on the network

    c. Whether the management tools or agents have been successfully installed

    d. Whether these tools/agents have communicated to their central servers successfully

    e. A summary of patches applied and their versions

    f. Most recent activity for software updates, antivirus libraries, and similar

    g. Status of the local firewall on the ATM

    h. Any other configuration items that would be problematic if they were misconfigured

4.2.2. Monitoring Will Make a More Secure ATM

The primary purpose of ATM monitoring is to maintain the best practical level of ATM availability. Tools and techniques allow you to attend to the health of ATMs when needed to help make sure that the ATMs are available when your customers want to use them.

In addition, more sophisticated monitoring can help ensure the integrity of the ATM, alerting you to threats to its software state or unusual activity that could represent an attack, such as unexpected communications or the connection of unexpected devices.

Both of these points lead to the recommendation that an ATM needs proper monitoring to stay secure. This section will describe the main considerations for monitoring your ATMs.

First, keep in mind there are three parts to monitoring: ATM application monitoring, general ATM health monitoring, and ATM security monitoring. A well-running ATM needs to have a healthy operating system and set of management capabilities as well as an ATM application that is running and serving customers. Poor health in either of these aspects can result in an ATM that is unreliable or insecure. And an ATM that is under attack or has already been compromised is a threat to the integrity and confidentiality of customer data; it must be discovered and acted upon quickly.

Secondly, understand that there is a sweet spot in alerting where the number of alerts is small enough to be manageable and actionable by operational staff, but not so small that significant events are missed. Either alerts should be resolved or they should self-clear if a problem disappears. This means that all alerts should be actionable and have associated procedures; there is nothing more frustrating in an operational environment that an overwhelming flood of alerts or alerts that are beyond one's control to take action on.

So, the most important part of monitoring is what you do when you get alerts about a condition that threatens availability or integrity of an ATM. A good monitoring system includes both problem remediation and determination.

You should be able to resolve the top ten most common ATM issues centrally, using your ATM monitoring and management tools to perform predefined and well-scoped tasks. Some ATM deployers have found that about half of all visits to an ATM to perform troubleshooting involved a reboot and no other action; a central reboot of an ATM is likely the most effective problem resolution technique available to you. Just be careful that this is a graceful reboot using an ATM-application-specific command to wait for the current customer to complete transactions and receive his card back before the reboot is allowed to begin.

The following are examples of appropriately-scoped problem determination and resolution tasks that you should consider for central management of ATMs, all of which can be performed remotely with good ATM monitoring and management tools:

- Gracefully reboot the ATM; allow current transactions to finish before rebooting!
- Retrieve log files and security events.
- Retrieve performance information about memory, disk space, CPU usage, process lists, network ports, etc.
- Restart critical services on the ATM.
- Log all of the verification information available to local service personnel using the supervisor panel.
- Validate and enforce security tools and policies.

Ideally, a task list containing the top 20 or 25 correctable items that can be resolved remotely using central monitoring and management tools should be maintained. This list should be reviewed on a regular basis for accuracy and validity.

The administrators authorized to use ATM monitoring and management tools should not be able to do so directly from their desktop PCs or from laptops especially. Allowing such direct communication to ATMs creates a potential attack vector for attackers or malware. Instead, it is recommended that all direct access to the ATM for problem determination and remediation is performed via a management/monitoring server with controlled access.

Consider carefully the lists of people involved in managing and maintaining the ATM and exactly what they need to accomplish to provide support to the environment. Administrative role segregation is a very well-known security concept that allows a security team to define appropriate roles to the people that will have access to the ATM. A well-defined role-based access model and tools to implement and manage this should result from a well-developed set of security policies, as described in Chapter 2: Understanding the PCI Framework for ATM Software on page 18. For example, the person responsible for defining the security policy should not have the right to deactivate the security controls.

For diagnostic tools that normally run from an administrator’s computer with direct access to an ATM, a common technique is to set up firewall rules that force the administrators to first connect to a central terminal server. The central terminal server should have controlled access and allow authorized administrators to use a well-defined set of tools to monitor and manage the ATM. This approach allows for stronger auditing of activities and better control over the tasks the administrator is allowed to perform. This central terminal server is often referred to as a jump server or an admin server. This technique allows for more robust network isolation of the ATMs from the rest of a TCP/IP network and can dramatically reduce the scope of a PCI audit.

Summary: The foundation for ATM software security is set at time of installation. Proper monitoring maintains the integrity of this foundation.

4.3. Integration with Existing IT Systems

In many ATM implementations, additional standard IT systems can play a role in ATM security. Management and security tools that have been used successfully in ATM systems include:

- Directory services such as Windows Active Directory. Active Directory allows for:
  - Management of security settings on the ATM using Group Policy.
  - Central authentication of user accounts used at the ATM. This can include the automatic logon user, the users that perform routine supervisor functions at the ATM, or the administrator accounts that may be used occasionally for troubleshooting unexpected ATM issues.
  - Seamless authenticated access to other systems across the network, such as servers providing marketing content or financial-related functions that lie outside the core financial switch. This authentication takes advantage of the Kerberos authentication protocol inherent in an Active Directory deployment.
  - Credentials for authenticating and encrypting network traffic using IPSec (see 4.4 Role of Encryption: Hardware and Software Perspectives on page 58 for more information).
  - Other management tools can take advantage of the Active Directory structure. For example, software distributions can target specific geographies, specific ATM model types, or be deployed in waves such that no two ATMs at the same branch are updated at the same time.
- Inventory systems to track information about ATM hardware and software.
  - Configuration Database that stores the personality information for each ATM so that streamlined ATM software installation can occur with little or no interaction from the installer. This would be part of ATM install automation techniques and reduces the likelihood of software misconfiguration and can reduce the opportunity for introducing unauthorized software changes to the ATM build.
- Multi-factor authentication implementations for administrative access that use a token or similar device as part of authentication.
- Network monitoring systems to analyze the network performance of the ATMs. Access to Network Monitoring systems needs to be carefully controlled because network monitoring tools can be used to capture sensitive transactional data, including the customer PAN.

- Testing automation tools to assist in the rigorous test cycles that should be part of all ATM change control. Disk imaging tools to assist in the construction and deployment of the ATM software build to the ATM's hard disk.

Summary: Leveraging enterprise-wide IT systems can be cost effective and result in stronger ATM security.

4.3.1. Case Study: Active Directory at a Large US Financial Institution

Starting in 2000, a large US financial institution with 5,100 ATMs in 19 states plus Washington, D.C., began introducing a small number of Windows® XP Professional–based ATMs as stand-alone units locked down locally with security policies and firewalls. These ATMs were setup without remote access so a technician was dispatched to troubleshoot or reinstall the software onto an ATM whenever problems were reported. This was an expensive and time-consuming process.

With Active Directory, the financial institution uses centrally managed Group Policy to distribute consistent security and configuration changes to ATMs without the need to visit the sites. Group Policy also provides the financial institution with reporting capability so that IT administrators can examine and review all of its ATM configurations from a central point.

One of the challenges that the financial institution faced was to define the relationship between its ATM network and the rest of its enterprise infrastructure, which was already based on Active Directory. On one hand, the financial institution stood to benefit from connecting its Active Directory–based ATM network to the rest of its infrastructure, but on the other hand, traditional best-practice ATM security recommended complete isolation of the ATM channel from any other network.

To balance these security requirements, ATMs were isolated from the rest of Active Directory infrastructure in a separate network to minimize the possibility that a threat in one network would affect the other. Windows XP Firewall was also deployed to block unwanted traffic into the ATM network.

The financial institution's Active Directory architecture then went through four months of testing, followed by a series of rollout phases. The Active Directory–based design was first rolled out to ATMs at the financial institution's headquarters, giving the company's technical professionals a microcosm of an end-to-end deployment to evaluate. The deployment has continued in a series of increasingly broad rollouts.

When the financial institution's technicians restart a machine, it obtains the up-to-date security settings for the ATM automatically so the financial institution has a consistently secure ATM network. Using secure remote access capabilities, the financial institution avoided more than 200 site visits and gained more than 600 hours of ATM availability for just one update.

4.4. Role of Encryption: Hardware and Software Perspectives

Data encryption in an ATM system is implemented in three distinct ways:

1. **Data at rest on the ATM.** There are two main reasons for encrypting your data while it is stored on your ATM's hard drive. Firstly, any cardholder data that may be stored on the hard disk of the ATM should be protected from inappropriate inspection. Also, it is imperative to protect the hard disk from manipulation in order to avoid offline attacks.
2. **Data in transit to/from the ATM.** The network traffic from the ATM may contain sensitive information, and should be protected as described in 4.7 Interface with Communications Link on page 74.
3. **The encrypted PIN and secret keys associated with the financial transactions.** There are several well-established requirements for PIN and transaction cryptography and key management.

4.4.1. Encrypting Data at Rest

Like any computing asset, the data stored on an ATM is at risk if the ATM falls into the wrong hands (physically or logically). Customer and transaction information can be stored on hard drives by ATM applications in logs and temporary files used by the operating system. It must be ensured that sensitive data, such as PANs or track 2 data, are not stored on the ATM's hard disk. Compliance with PCI SSC directives might in some cases be achieved using encryption technology (see 2.3 PCI DSS Requirements on page 21 for details on when encryption is allowed and when data cannot be stored even if encrypted). Until recently, this has been the major use case for encrypting the ATM hard drive or some files in it.

In recent years, full hard disk encryption (FHDE) has become more relevant in order to prevent ATM offline attacks. These attacks involve booting the ATM from an operating system on a CD or USB drive and manipulating your ATM hard drive in order to disable your defense systems. These defense systems are described in 2.6 Cryptographic Hash Functions on page 30 and could include anti-malware solutions or firewalls, among others; all of which can easily be disabled in an offline attack.

In principle there are several ways to prevent this manipulation, including password protecting the BIOS so that booting from alternative media cannot be done without a password. However this requires cumbersome password management procedures and might have an undesirable impact in operations and maintenance. It can also be relatively easily bypassed. Other solutions, such as modifying the BIOS, are even less convenient. On the other hand FHDE technology has been around for years and provides a suitable solution to this threat.

4.4.1.1. Overview of Full Hard Disk Encryption (FHDE) technology

There are essentially two FHDE technology flavors: software-based and hardware-based. They were both derived to solve the need of data confidentiality in portable devices and laptops, so some caution is needed to extrapolate their use to ATMs.

Software-based solutions have been in use for a number of years and have a solid track record. These solutions implement the encryption algorithm in software, although they usually make use of some hardware acceleration capabilities in modern processors.

More recently, the Trusted Computer Group (TCG) developed standards to protect data based on hardware. One of such standards is OPAL, initially released in 2009. Hardware-based protection is achieved by means of self-encrypting drives (SED). SED technology includes the encryption functionality embedded within the hard drive itself.

Software-based or hardware-based, each technology has its own advantages. Essentially SED technology provides better performance at the expense of requiring specific hardware. This could be important in a laptop where performance is always demanded, but it is unclear that performance by itself would be a fundamental criterion in an ATM scenario, since software-based solutions are also quite good.

To complicate things more, full disk encryption on a computer where no user is present at boot time, such as an ATM, needs to tackle the problem of acquiring the decryption key material without halting the boot process and waiting for human interaction. This situation is the same regardless of the encryption type: software or hardware. There are several possible solutions to this problem, each with its pros and cons. The first standard of the TCG was actually for a Trusted Platform Module (TPM), a piece of hardware that stores the required key, provided your computer is equipped with one. The key can also be stored in an external hardware device such as a USB stick.

If you want to avoid dealing with new hardware, it is also possible to store the key in an unencrypted partition of the disk where it would be accessed at pre-boot time. Here the key material can be obfuscated but not encrypted, since then yet another key would be required and this would add further complications. However, obfuscation is a poor security solution. A better possibility is to compute the key at pre-boot time using identification information extracted from various ATM devices. Some manufacturers happen to use the same id numbers in all ATMs for some devices but there are some values – such as the MAC address of the network card – where these must be unique. This solution would reach the same goal as the TPM; the drive would be useless in case it is removed from the ATM.

Another possibility is to store the key material in an external server and access the key at pre-boot over the network. This can be achieved using PXE technology. Acquiring the key over the network would prevent decrypting the drive even if the whole ATM is stolen.

Finally, it is possible to combine several of these techniques in order to achieve the desired balance between security, availability, and deployment cost.

It should be evident by now that all these solutions have varying degrees of security and complexity. Due to the diversity of approaches and technologies, some guidelines are needed in order to select the best FHDE solution for each particular case. The next section discusses several aspects that should be considered in making the correct choice.

4.4.1.2. FHDE considerations for ATMs

This subsection discusses a number of aspects of interest regarding ATM FHDE and although discussed separately, these aspects will relate to one another. The following aspects should help to select the appropriate technology to deploy FHDE technology in an ATM network by identifying which requirements should be fulfilled.

1. **Diversity of your installed base.** New ATMs are likely to include hardware that can be used for FHDE. In some cases they might include SED drives or a Trusted Platform Module (TPM) which can be used to store the decryption key. On the other hand, old ATMs might not provide a TPM or SED and might even be incapable of running some software-based solutions in case it uses heavy resources. You must consider whether you want one common solution for your network, which means you must accommodate the low end ATMs, or you are prepared to manage more than one solution and accept the inherent complexities. You should look at multivendor solutions when possible.
2. **Key management.** One of the most critical aspects of FHDE for ATMs is how the keys are managed. Recall that this particular aspect of the solution is new since there are no relevant precedents for drive encryption in unattended platforms. Communicate with the manufacturers. Obtain all of the insight you need for your preferred solution. As usual with upcoming technologies, the devil is in the details. Do not deploy a solution that you do not understand.
3. **Performance.** There are two separate performance aspects to consider. The first is the performance loss from accessing an encrypted drive. An ATM application is not very demanding and you should not expect that encrypting your drive would be noticeable for your users. However, it is advisable that you do some testing to confirm this. The second aspect is the encryption process if you select a software solution. A poorly designed solution could take several hours to encrypt the full drive which could result in an availability issue. Again, actual testing is recommended. There are also solutions that keep the ATM operational while it is being encrypted and these should be preferred. Hardware solutions such as an SED should not present any performance issue.

4. **Deployment.** The deployment process might vary considerably from one technology to another. The main difference resides in whether the solution requires hardware. Deployment is much simpler for software-based solutions. Some software-based solutions even include a console where encryption can be commanded and managed remotely. You need to verify that your solution is resilient to abrupt interruptions of the encryption process. On the other hand, if your preferred solution includes hardware deployment, there will be logistics considerations and costs involved that you have to take into account. There are solutions that require deploying USB devices or even specific central appliances. Make sure you understand whether your solution is fully software-based or if hardware is involved.
5. **Reliability.** Some software solutions are designed so that a password must be obtained from a USB device plugged into the ATM during boot. Usually, this results from the adaptation of a general purpose FHDE solution to the ATM scenario. If you select this type of solution, the ATM would not be able to boot if the USB stick is removed or fails.
6. **Disk recovery.** In a laptop scenario, it is imperative that you have a method to recover your unique data in case you lose the password: regular backups, centralized password management, or another method. All disks in ATMs have the same content and, therefore, this is not a problem. However there are situations where you might want to decrypt the disk in order to analyze it in a laboratory, for instance for forensic purposes. Make sure that your solution supports this option.
7. **Centralized management.** ATM security should be centrally managed. Make sure disk encryption is also centrally managed. For instance, solutions should be preferred where encryption can be commanded remotely from a console. It must be possible to know the status of disk encryption all over your network. Another situation where a central control is convenient is when the key is derived from hardware devices in the ATM and one or more devices are changed. In these cases the ATM should be able to boot and the new devices should be approved from a central server. Key rotation and recovery are examples of other features that should be managed from a central server.
8. **Factory encryption.** In some cases the ATM drives are delivered to field ATMs from a location or factory and it is desirable that these drives leave the factory already encrypted. This way, even if a drive is intercepted while being transported to the ATM, no information can be obtained from it and no reverse engineering of the application is possible. Another scenario is where drive deployment is carried out by a third-party and drive encryption ensures the confidentiality and integrity of the contents. Specific requirements for this situation should consider the extent to which this party is trusted and the level of IT security in place in the factory.

9. **Suitability for ATMs.** Your chosen solution must be prepared for ATMs' scenarios. The FHDE is an old market. It is only logical that traditional FHDE solution manufacturers try to adapt their solutions to ATMs. This is good news, since these companies have the most expertise. However, keep in mind that the number of PCs in the world is many times greater than the number of ATMs. It is unlikely that general purpose products will be re-engineered for the particular needs of ATM networks and will most likely be adapted instead. Beware of general purpose solutions unless they have been extensively proven in ATM networks. Remember: FHDE key management for unattended devices, such as ATMs, is a recent and challenging scenario. Select a solution specifically designed for ATMs when possible.
10. **Security.** Lastly, the level of security provided by the solution must be assessed. Unattended FHDE cannot be made fully secure from a conceptual point of view. Do not look for a perfectly secure solution. It is better to understand how your preferred solution could be attacked and to understand that trust is required from all parties involved in operation and maintenance of your ATM network. Security is generally obtained at the expense of availability risk. Your preferred solution does not need to be completely secure, but instead the result of a trade-off considering the aspects mentioned above. It just needs to be secure enough.

Encrypting the ATM drive might be mandatory due to the most recent offline ATM attacks. The important thing to remember is this: You must understand exactly what you are trying to achieve with hard drive encryption. Perform a risk assessment: Are you just trying to prevent offline attacks or also to prevent reverse engineering of the software? Is there a risk that your drives could be manipulated during deployment from the factory? Do you want to prevent the disk from being decrypted when removed from the ATM or do you also want to prevent it in case they steal the complete ATM? Do you trust the third-party that operates or maintains your ATMs? Make sure you understand your goals. Then consider all aspects above and see that you reach your goals.

4.4.2. Cryptographic Key Management for ATMs

This section provides guidance for key management within the context of ATM transactions, more specifically key management associated with financial transactions and the encrypting PIN Pad.

The very essence of protection in an encrypted environment is the secrecy of the key. The role of key management is to ensure that the key remains secret through its lifecycle. The principles of segregated roles and access, along with maintaining high levels of integrity through all stages are enforced using strong key management processes. These principles are generally referred to as dual control and split knowledge.

With regards to an ATM environment, key management lifecycle and related secure processes include:

- **Generate:** Generating the Terminal Master Key and other keys as defined in the data in transit requirements. Most ATMs function on a single, symmetric encryption key known as the Terminal Master Key. It is used as a key transport key to protect the PIN encryption key during its transit from the host to the ATM. While others employ dual encryption, symmetric key distribution over a PKI channel is not uncommon. The keys are generated as multiple components, usually 2 or 3 components and each component is managed by a nominated key custodian.

  Refer to PCI PIN Security Requirements for additional information; for the latest documentation, see http://usa.visa.com/merchants/risk_management/cisp_pin_security.html

- **Store:** The key components are stored for future reference and for distribution to the ATM (for provisioning). Care needs to be taken that the storage repository for each component has a named owner and the following conditions are met:

  - No storage repository shall store more than 1 component of any key.
  - No key custodian shall have access to more than 1 component of any key.

  The medium of storage shall be in accordance with ISO 11568 (Cryptography Key Management standards for banks), ISO 11770 (Cryptography Key Management Lifecycle), and PCI PIN security requirements 9 and 21.

- **Distribute:** Sending the key(s) for provisioning of the ATM and reloading the ATM if the key(s) becomes corrupted. This stage is by far the most vulnerable of all the stages in the ATM environment. Recommendations for best practices include employment of multiple, trusted personnel for provisioning the ATM, or the best practice of deploying remote key technology where the key(s) and their components are not revealed to the user provisioning the ATM. This stage also includes electronic/physical transfer to a backup site for future recovery, if applicable. Refer to PCI PIN security requirements 8 to 11 for additional information.

- **Load:** The encryption key must be loaded using the principles of dual control and split knowledge and the correctness of the key must be verified before use. Refer to PCI PIN security requirements 12 to 16 for additional information.

- **Use / Rotate:** The encryption key(s) should be in active use for a limited and predefined period of time, unless known or suspected to be compromised.

  For single-level encryption keys, the refresh frequency should be 2 to 4 times a year. For multi-level encryption keys, each key should be refreshed at least twice a year.

- **Revoke / Suspend / Terminate:** At the end of the key's defined life or as a result of a known/suspected compromise, the encryption keys will be suspended. A business impact analysis should be completed for a compromised key to define the urgency of the key suspension.

  Where the encrypting PIN Pad (EPP) of an ATM accepts remote key distribution, whether or not the keys are stored in the EPP, the following practices should be followed:

  - Key usage must be restricted following the EPP vendor's approved approach and in conformance with PCI-PTS requirements for key bundling to enforce that the key is only used for the intended use.
  - Remote key distribution techniques for working keys (e.g., PIN, data, MAC) may only be used where key usage is restricted as described above.
  - Devices supporting asymmetric techniques for remote key distribution shall only support the use of such techniques for the loading of terminal master key(s).
  - Downloaded data key types must not be accepted by the device unless enciphered by a different terminal master key than sensitive keys such as the PEK or MAC key types.

  For reference, note that required hardware capabilities of EPPs include, but are not limited to, the following:

  - The addition of a new key type (slot) subsequent to the initial configuration of the device causes the zeroing of all other secret keys.
  - The device does not provide any support for decrypting data or other similar functions.
  - The device must ensure that keys with different purposes can never have the same value; this requirement must be maintained until the device is decommissioned (or until the applicable terminal master key(s) change).

4.5. Reference to Standards

The following best practice standards/guidelines apply to key management:

PCI DSS – Technical Guideline – 3 (PCI DSS TG – 3)

PCI PIN Security Requirements – Version 2.0, January 2008 and subsequent editions

ISO 11568 – ISO standards for Cryptography Key Management for banks

ISO 11770 – ISO standards for Cryptography Key Management Lifecycle

NIST Recommendations for Key Management: SP800-57-Part1, SP800-57-Part2

ISO / IEC 9564-1: Banking - Personal Identification Number (PIN) management and security - Part 1: Basic principles and requirements for online PIN handling in ATM and POS System

X9.24 Part 1: Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

FIPS 140-2 –Specifications for security of Hardware Security Modules

It is recommended that ATMs are audited frequently (once every 6 months) against key management standards and defined processes.

Summary: Following key management best practices and using an automated key distribution (remote key) system will maintain the security of encryption keys.

4.6. Software Defense System

The particular security technologies selected must be well-suited to ATMs and be selected using an ATM-specific software security governance process. This imposes a number of management, performance, and reliability requirements. The overall solution should consist of a combination of firewalls, integrity controls, whitelisting/blacklisting approaches to malware protection, patching, monitoring, and a hardware device control.

Best industry practice is to apply several layers of defense to provide better security for ATMs. This way, when a fraudster discovers a type of system vulnerability, your system is not immediately exposed; layers of security provide a set of checks and balances against attacks and fraud. However, the balance between adequate layered security and unneeded complexity should be kept in mind.

This section describes how a number of security-related software layers contribute to overall ATM security. Some or all of these components will make sense for your ATM solution, but be conscious of the following:

- Having more security tools does not equal more security. Make sure that you have a system with security tools that can be effectively operated and not just a system with a large number of security tools. A smaller set of tools that provide the same capabilities as a larger set would reduce complexity in both deployment and management.

- All tools that can prevent something bad from happening also have the ability to deny service to your solution. Be careful to weigh the benefits of ATM integrity against the possible impacts to the availability of the ATM because the security landscape is continually changing and most security tools will evolve and change over time. Be very conscious that each additional software tool may introduce its own mechanism for updating the configuration and software of that tool. This will increase the amount of work needed for overall ATM management, change control, and testing.
- The whitelisting approach has a clear advantage over traditional anti-malware tools due to its lack of needing to be updated.

The tools discussed briefly in this section include the following: firewalls, antivirus/anti-malware, device control, software patching and system management, vulnerability scanners, integrity control, intrusion detection/prevention, backup/restore, and remote control.

4.6.1. Firewalls and Network Isolation

When an ATM communicates through a shared or outsourced network which may also be used by other devices such as servers or workstations, a local firewall is advisable. Good desktop/endpoint firewall rules can prevent malware from reaching the ATM. For example, a firewall rule that says to only accept incoming traffic that is a response to traffic initiated from the ATM will prevent unwanted inbound connections; if all traffic to the ATM occurs in response to messages initiated from the ATM, then no other traffic will be allowed in. This also prevents a person with access to the network from attempting to breach the ATM through the network interface. However, exceptions should be allowed for legitimate ATM management tools.

Firewall rules are static and do not have the overhead of antivirus/anti-malware solutions. Firewalls can be implemented in software as part of the ATM's operating environment or in a hardware device located in or next to the ATM. A software-based firewall has the most security as it cannot be compromised through physical access alone. Some software network interfaces have a built-in firewall, which can simplify management and deployment.

4.6.2. Preventing Malware: Whitelisting and Blacklisting Approaches

Anti-malware/antivirus (AV) can complement a strong firewall system and therefore are an important layer of software security. AV benefits include:

- Protecting against vulnerabilities in firewall rules.
- Meeting regulations and/or corporate standards for AV.
- Safeguarding against the risk that software patches, updates, or even content could include viruses or malware.

There are also two philosophies for anti-malware. A blacklisting approach relies on a library of known virus types and variants to look for and protect against. A whitelisting approach allows only known-good executable code on a computer to execute. The whitelist can be generated in a few ways, normally one of the following:

- Examining code on a known-good computer and declaring all of it as safe to execute.
- Accepting digitally signed code from a list of trusted signers.
- Accepting code from a predetermined secure network location.
- Accepting updates from a predetermined updater, such as your internal software distribution tool.

Whitelisting technology locks down the operating system so that only known applications can run and known system calls can be made. A whitelist can also protect memory to prevent malware from performing buffer overflow attacks. The main advantage of this approach is that it will not need to be updated as frequently as blacklisting approaches and the approach is also well-suited to ATMs where the list of applications and tools that need to execute is limited and rarely changes. Unlike desktop and laptop PCs where users expect and require frequent changes in what should be allowed to execute, ATMs are aimed at providing a specific purpose and only need to be updated infrequently and in well-controlled ways.

Because whitelisting is well-suited to the rigid operating environment that a well-defended ATM lives in, this is the recommended approach to anti-malware for ATM.

Care should be taken when selecting a whitelisting strategy to ensure that the whitelist covers these three areas beyond the code that may be on the ATM when it is first deployed:

- Only appropriate Java content should be allowed to execute within the Java runtime process. Disable blanket permissions allowing other Java content. This is important since Java drives many ATM applications.
- Your software updating tool must be allowed to install new code on the ATM and have the new code automatically update the whitelist. Because you will need patches from time to time, the change to the whitelist should be low maintenance.
- Any management tools and agents that you require to securely operate your ATM environment must also be included in the whitelist. A whitelist has the power to block legitimate tools or scripts as well as malware.
- While blacklists are long and grow with each new malware variant, a whitelist for a specific-purpose computer like an ATM can be dramatically smaller. It also requires minimal updating.

The reasons that whitelist-based anti-malware is preferred to blacklist anti-malware for ATMs includes the following key considerations:

- Installing a blacklist anti-malware tool on an ATM has the overhead of dealing with updates, which are released daily.

- Due to the size of the blacklist, continuous malware scanning can slow performance and will consume too many resources. This can be an issue in low specification computers and can cause noticeable customer impact.
- Blacklist anti-malware detects known malware variants. Because malware that specifically targets ATMs may not be widely distributed, blacklisting approaches will struggle to detect it.

There are also several common reasons for an ATM deployer to select a blacklist-type anti-malware tool. Carefully consider the reasons for selecting a blacklist tool before deciding to use it instead of a whitelisting tool. A few of the common reasons for selecting traditional blacklisting antivirus are described below. The identification of security policies described in Chapter 2: Understanding the PCI Framework for ATM Software on page 18 can help in the decision-making process.

If you are selecting a traditional blacklisting antivirus because of its lower cost per ATM, you also need to factor in operational cost related to ongoing updates of the blacklist library and the potential impact of undetected ATM-specific malware.

If you are selecting a traditional antivirus tool because antivirus is specifically mentioned in the PCI DSS standard, keep in mind that whitelist approaches to anti-malware are also considered to be valid antivirus tools by the PCI.

If you are selecting a traditional antivirus because you have previously experienced examples of PC viruses on your ATMs, remember that whitelisting would also have protected against this malicious code since it would not be on the whitelist.

And if you are selecting a traditional antivirus because you already use it in your desktop and server environment and are familiar with it, perform a risk assessment that takes into account the reduced costs of using a familiar tool but also the risk of it causing availability problems or failing to prevent inappropriate code from running on the ATMs.

If the risk assessment does point you in the direction of a traditional antivirus tool, make sure you include the following in your operational plans:

- Perform very thorough performance testing of the tool, particularly on ATMs with lower-spec PCs. This should include antivirus behavior during updates to the ATM or to the antivirus library, and ATMs that remain running for periods of weeks or months without a reboot.
- Before promoting any new antivirus library to production, introduce it into a pre-production environment and perform a full virus scan of a production-identical ATM to ensure that the new engine is not generating false positives. There may be cases where a new library falsely identifies the ATM application as malware and prevents it from running. You may be the first to discover this in your production ATM network!

- If you have a number of other compensating controls against the introduction of malware, you should consider delaying the introduction of new antivirus libraries into your environment (so other people can discover false positives or performance issues) and lengthening the interval between updates (reducing the churn of changes on ATMs makes for better-running ATMs).

4.6.3. Protection from Reverse Engineering

Modern virtualization technologies give new opportunities for reverse engineering of ATM software and development of malicious software to carry out attacks on ATMs.

Unprotected applications can easily be reverse engineered by even an intermediate level hacker. Reverse engineering involves tracing execution of software code to map out a program's algorithms; once these algorithms are understood, they can be modified to accomplish the hacker's objectives. In this way, a reverse engineered program can become a powerful tool that serves a hacker's needs. For example, by reverse engineering the algorithms that control the cash dispenser, a hacker could create specially designed attack software that takes direct control over the dispensing of cash.

To prevent reverse engineering attacks, best practice is for ATM software vendors to introduce the following anti-reverse engineering technologies:

- Obfuscation
- Program code virtualization
- Integration of behavioral analysis
- Process isolation technologies in application software

Such technology and techniques have been widely used in other industries, such as computer games, and have proven their value in prevention of reverse engineering.

4.6.4. Software Patching and System Management

Every piece of software of any significant size has bugs. And most software products will be enhanced over time, because of business drivers, support reasons, or changes to other parts of the system infrastructure. Software changes (patches) are inevitable, even in relatively static systems such as ATMs.

Strict and orderly change control is the secret to applying patches and upgrades in an environment where availability, integrity, and confidentiality are so important. This section describes the most important factors to take into account when planning for software patches.

First, a manual approach to patching ATMs (sneaker-net) will work only in the smallest ATM estates. Visiting ATMs to apply patches is costly, time-consuming, and can be error prone. It also allows the installer highly-privileged access to the ATM operating system, which is best avoided if possible. Once the number of ATMs in an estate reaches any significant number, a central software distribution tool will reduce expenses while protecting the integrity of the ATMs and preventing downtime.

The most important considerations for people, process, and technology aspects of a software distribution tool include:

- The more software products that are installed on an ATM, the more patching will be needed. At a minimum, there will be an operating system, device drivers (such as the XFS layer), and an ATM application. There may be additional pieces of software, including management agents, tools like Acrobat Reader, Java runtimes, Flash graphics engine, and more. These items will all likely need software updates over time.
- The process of deciding which patches are needed and how important they are to apply is critical. Some patches that are critical for desktops may not be critical for ATMs. Your organization should have a distinct set of criteria for patch decision making, particularly to identify critical security patches as required by PCI DSS.
- You should always be able to answer the question, which of my ATMs has received and applied this patch? This could become critical in a breach response situation where an ATM estate suddenly becomes vulnerable or comes is under attack for a specific software vulnerability.

Newly-provisioned ATMs may be installed using a software image that is at least a little bit out-of-date with respect to patches and updates. This has several implications:

- Often, the initial patch-to-current process can be difficult. Consider an installation tool or an approach which automatically verifies whether a patch has been applied to an ATM and determines which patches are needed (e.g., using a catalog) so that no necessary patches are missed when a new ATM is introduced.
- The patch-to-current process also applies when ATMs are re-installed in the field or are restored from a backup.
- In some cases, it may be acceptable to bring an ATM online without all patches. For example, perhaps a subset of mandatory patches needs to be applied before an ATM can be brought online, with remaining patches installed after the ATM becomes operational. If so, technology and procedures should allow for this.

- Experience has shown that rigid change control and good testing will protect you from many security problems, but it can be time-consuming and resource intensive! The best practice is to strike an acceptable balance and define a standard patching rhythm. Monthly is generally considered the best practice today, though it may be an aggressive timeline for some ATM deployers. A patch rhythm that is longer than quarterly is generally thought to be too long in today's constantly evolving threat landscape.

Patching of ATMs usually requires that the ATMs are removed from service while patches are installed. Planning is needed to minimize customer impact from ATM downtime. Some customer service considerations include:

- Where a significant number of ATMs are to be patched, the best practice is to minimize customer impact by installing the patches in waves. The first wave, for example, might include half of the off-premise ATMs; the second wave might include half of the branch ATMs, and so on. Waves are timed such that the majority of the ATM base remains active at any given time. This approach also minimizes the risk of issues with patch installation and maintains availability of ATMs across the base when issues might occur.
- Patching an ATM should not impact the customer using the ATM at that time. Many ATM applications have the ability to wait to run a command until there is no customer using the ATM. This approach is recommended to be used (or included in the software update itself) before any change to the ATM software are triggered remotely.
- When two ATMs located side-by-side are to be patched, the patching schedule should ensure that these ATMs are not updated at the same time to prevent impact to customers; in other words, they should be updated in different distribution waves. For example, this logic could come from a single central roster of ATMs, such as a directory service, so that multiple update tools can use the same scheduling logic.

Some management or security tools such as AV tools, centrally-managed firewalls, security configuration tools, or integrity control tools may have their own mechanisms for applying updates. Consider all methods of updating the ATM when planning the procedures and schedule for applying regular ATM updates.

Most software distribution tools also include the ability to perform some remote administrative tasks. A few important considerations for these aspects of systems management are:

- Ensure proper dual-custody controls so that no single administrator can both develop a change and implement it. Systems management tools can allow for changes to be made to a large number of ATMs by central administrators. However, such systems management capabilities should always be used within a tiered administration structure where only top-tier administrators can perform the most powerful operations.

- Because availability of the ATM to customers is important, make sure that remote administration tasks do not affect the ATM's performance. For example, if particularly heavy diagnostic operations can be triggered remotely, these may need to be preceded by a command to make the ATM unavailable to customers.

4.6.5. Other Security Tools of Interest

It is best practice to take a snapshot of the key files on an ATM's hard disk at a point in time when the ATM is known to be clean and not infected by any malware. That snapshot should be stored securely and compared regularly to the ATM's hard disk snapshot over time. Proper selection of the files to be included in the snapshot will identify changed files as exceptions from the original snapshot, highlighting review for malware infection not caught by other methods.

Some other security tools that may have value in a layered security approach to ATM security include the following:

- **Port protection tools/Device Control:** ATMs operate like any desktop and have interface ports. If a person has access to the ATM, such as a hardware maintenance outsourcer, they also have access to the ports. A savvy user can use the ports to insert malware or gain access to the device. Port control tools can prevent this access, or only allow specific users to gain access based on authentication. Endpoint security tools that include firewalls or anti-malware often provide port protection options as well.
- **Tools that validate the integrity of executable files, libraries and drivers.** This is a complement to the protection against unauthorized software execution by allowing only code or software updates signed by trusted vendors or by your own organization to be installed and executed. In this way malware is prevented from running or interfering with authorized software.
- **Vulnerability scanners** can provide a good profile of the security of your ATM network from a software and systems perspective. Network vulnerability scans are a required part of the PCI DSS for internet-facing environments and must be performed at least quarterly. Though ATM networks are not public-facing, vulnerability scans performed using a scanning tool will provide valuable information about the security of an ATM network.
- **Intrusion detection may have a place in layered security.** However, intrusion detection aimed at desktop/laptop PCs may not be suitable for ATMs, since ATMs are more similar in function to a server with a fixed role sitting on an isolated network than a multi-function device like a PC. Be conscious that it may result with false positive identifications of threats.

- **Remote backup/restore functionality** can restore ATMs to a known-good state in the event of a widespread security incident. The tool can provide the best way to recover an ATM or group of ATMs after a virus outbreak, a catastrophic software update, or a suspected ATM software compromise.

As software protection systems converge towards more complex all-in-one solutions, it will be difficult to attribute anti-malware software to one of the above-mentioned types. For example, some host-based intrusion prevention systems (HIPS) encompass both application whitelisting and can provide protection from memory exploits within approved applications.

In general, we recommend that all remote control tools should only be used after other predefined troubleshooting tasks have been exhausted. Further, remote administrative tools should have very strong controls in place to protect them.

Summary: Whitelisting is a powerful anti-malware technique for use in ATMs.

Layers of security systems protecting your ATMs will always provide greater security than any single technique, however advanced or secure that product may be.

4.6.6. ATM Software Security Solution Example

The following diagram shows an example topology for an ATM solution that includes a number of the components suggested in this document. Because the recommended approach to security here is to include an appropriate number of layers of security, a real solution may not include all of these elements. The diagram is intended to simply provide a sample of what a well-secured ATM solution could look like.

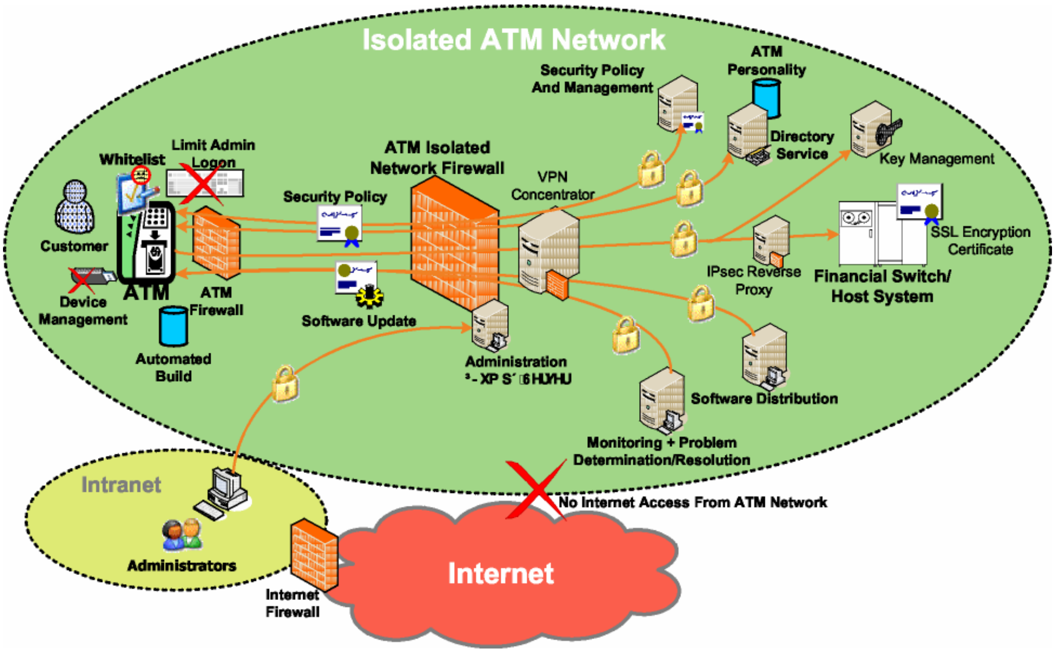


Figure 10: Sample ATM environment with PCI DSS requirements and other recommended options

4.7. Interface with Communications Link

Finally, as ATMs require a network to operate, a discussion of ATM software security best practices would be incomplete without mention of techniques for securing communications. While communication security could itself be the subject of a best practices guide, the PCI Data Security Standard includes requirements for securing communications applicable to ATMs. In addition, ATMIA is currently preparing a guide on telecommunications security best practices.

While the use of encrypting PIN Pads (EPPs) ensures that the PIN is always encrypted during communication, the risk of a criminal tampering with transactions during transmission over the communications link is of concern for ATM security. This is a concern for the integrity of the communication. This concern also applies to management traffic reaching the ATM; an attacker who can compromise the integrity of management traffic may be able to manipulate the ATM for criminal purposes.

Another concern is ensuring the confidentiality of the communication to and from the ATM. In an ATM transaction there is more information than just the PIN considered confidential. For example, account numbers, balances and transferred amounts are sensitive personal data and need to be secured. Some of the data may be considered to be personally identifying information (PII) and is subject to local regulatory or statutory requirements. Exposing this data as it is transmitted by the ATM may be a violation of these regulations or statutes.

Traditionally, ATMs have been networked using private networks (or dialup connections for low volume ATM installations). Although there was still the risk of someone directly tapping the network in the middle or at the network cable attached to the ATM, the risk was considerably lower than exists today. The reason for the increased exposure today is that cost reduction and increased availability have pushed many ATMs onto multi-purpose TCP/IP networks, outsourced to third parties, or in some cases onto wireless networks. When ATMs are on the same network as other computing equipment, ATM communications traffic can more easily be intercepted by employees and others who may be able to decode PII. Also, in most cases there will be parts of the ATM network operated by a third-party telecom carrier. The carrier's IT staff will need access to the network for operational and troubleshooting reasons, so there will always be someone able to observe network traffic to and from the ATM. Confidentiality is even more of a concern with wireless traffic like Wi-Fi, cellular/GSM, or traffic that passes across the public internet. The PCI DSS explicitly addresses these types of traffic.

Although this is especially true of wireless traffic like Wi-Fi, cellular/GSM, or traffic that passes across the public Internet, it is also true for private, wired communication. There will always be a number of people that can inspect your wired ATM traffic. It can be an attacker that taps a cable close to an ATM, someone at the telco that carries your WAN traffic, or internal IT staff that has access to the network.

There are three fundamental recommendations for increasing the integrity and confidentiality of the communications link to the ATM:

- Protecting the integrity of transactional traffic should be an essential part of your ATM solution. Many ATM deployments use a standard integrity control, the message authentication code (referred to as MACing transaction traffic). This technique uses shared secret keys known to the financial switch and the encrypting PIN Pad in the ATM to protect against tampering with transaction data between the ATM and the financial switch. This is very important even if no other communication protection is implemented because an attacker who could adjust transaction amounts on transactions in flight could easily perform fraudulent activity against an ATM.
- ATM transactional traffic should be encrypted. Even when the transactional traffic is protected from tampering, the traffic should be encrypted. There is still considerable value to just inspecting the communication from an ATM, even if it cannot be tampered with. Transactions will contain the cardholder PAN and details of transactions. Singly, this information is interesting to an attacker; in bulk, the information is very valuable to criminals and the risk of fraud is high.
- Whenever possible, ATM management traffic should be protected with integrity checks and encryption. Being able to tamper with management traffic could allow an attacker to mismanage an ATM. Even inspecting management traffic may give an attacker an idea of how to exploit the ATM’s software stack. Most management tools today offer some ability to protect the integrity and/or confidentiality of the management traffic.

Summary: Communication security, including encryption of both transactional and management traffic, is part of the holistic approach for ATM security.

Chapter 5. Preventing Insider Fraud

"Both insider and outsider threats are serious problems. However, the insider threat is much more common. It makes sense since employees have more access. It comes down to access to information. The outsider threat is still a serious problem but it's just not as common."

Jim Ratley, CFE and president of the Association of Certified Fraud Examiners (ACFE). "Going Broad on Fraud" by Scott Berinato, CSOonline.com

5.1. The Nature of the Problem

Security experts worldwide recognize the seriousness of the threat posed to the integrity of financial services by insider fraud. A 2006 Financial Services Authority (FSA) report titled "Firms' High-Level Management of Fraud Risk" stated that "internal fraud and associated organized crime activity is recognized as one of the main threats to firms in financial services and is growing fast... Major firms and law enforcement consider insider fraud, whether arising from coercion, collusion, infiltration, or existing employees' own initiatives, to be one of the most serious fraud threats faced by financial institutions." Focusing purely on external threats without taking steps to protect systems from insider fraud would be like locking the front door to secure a property while the back door is standing wide open.

Insider fraud can be carried out by employees at all levels of the corporate ladder from bank managers to low-level employees, sometimes connected to organized gangs, who have access to account sensitive data. For example, staff may be approached by criminals nearby their place of work (whether a branch, call center, or other operational area) and offered money to sell confidential customer information, such as account numbers and balances, details of dormant accounts, threshold levels for check inspection, or more. In this way, organized crime can infiltrate an organization by targeting individuals open to criminal influence. Such infiltration can also involve planting an individual in an organization. There is increasing evidence that organized criminals are placing so-called sleepers within organizations with the objective of identifying possible security weakness and opportunities. Sometimes employees, turned fraudsters, even act alone.

At its simplest, insider collusion could involve the theft of information on paper from an institution's premises. On a bigger scale, internal fraud could also be committed via access to a company computer system. The scale of the fraud and data theft is likely to escalate when there is electronic access to customer data. Criminals typically sell and share stolen customer data on the black market. The rise of electronic banking and mass database marketing has increased the scope for large-scale insider fraud of this kind.

Dr. Donald Cressey developed the well-known fraud triangle for white collar crime:

- opportunity
- financial need
- rationalization

This is a useful model for understanding insider fraud. It is possible for companies to control or modify the first two factors in Dr. Cressey's fraud triangle for white collar crime, the opportunity and the financial need. It is probably not possible to have any measure of control over how fraudsters rationalize their crime to themselves.

It is important to monitor or review underpaid employees who have access to customer data and to provide incentives in the organization for staff to advance their careers. It is also important for management to be aware of staff that may have significant debts they are struggling to pay back.

For more information on the fraud triangle, see http://www.examiner.com/financial-fraud-in-national/financial-fraud-101-understanding-the-fraud-triangle.

5.2. Towards Best Practices for Preventing Insider Fraud

Part of the problem of insider fraud is that managing control over customers' personal information is a challenge, whether such information is stored on paper or a computer system.

That is why reviewing best practices for information security is an essential part of preventing insider fraud. But it is only one step among a very comprehensive, corporate-wide strategy required to beat back this growing threat.

In recent years there has been an increase in staff turnover within financial institutions – one major bank has reported that one in three teller staff leaves within a year – and a greater emphasis on short term or temporary appointments.

In an era of outsourcing and high staff turn-over, recruitment policies are more critical than ever. In addition to the financial losses involved, banks have suffered reputational damage[3] when high profile cases involving customer accounts have been published in the media. These best practices for preventing insider fraud are focused on reducing the risks of both financial and reputational losses.

It should be noted at the outset that Payment Card Industry – Data Security Standards (PCI – DSS), provides a security template and best practice standard for all processors of customer data. It delivers a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.[4]

5.2.1. Integrating the Strategy to Prevent Insider Fraud

Insider fraud is an issue for management, HR, IT, and security staff. Thus, senior-level central coordination is needed to combat this threat. An interdepartmental (or interdivisional) team at strategic level should be set up to develop and implement the corporation-wide policies, procedures and technologies needed at recruitment, staff monitoring, and data protection levels.

The Financial Services Authority (FSA) concluded in their 2006 report that although there is a high-level of executive sponsorship of fraud management in financial services in the UK, the approval of anti-fraud strategies and plans was in some cases informal with unclear lines of authority and ownership or accountability. There is a deep need for an integrated, comprehensive approach to fraud management, including fraud awareness training, accurate and detailed fraud data, and analysis. The FSA recommended more sustained fraud risk identification, assessment, mitigation and reporting, and the adoption of more formal fraud risk assessment processes in order to be proactive about fraud prevention.

[3] The respected 2002 King Report on Corporate Governance for South Africa stated, “Reputation is a function of stakeholder perception of a company’s integrity and efficiency, derived from many sources such as customer service, employee relations, community relations, ethical conduct, and safety, health, and environmental practices. Increasingly, the investment community builds an ethical premium in its valuation of companies, based on the perceived integrity of an enterprise and its management. Once blemished, this aspect of reputation is often hard to recover, a fact reflected in the share price.”

[4] Source: https://www.pcisecuritystandards.org

5.2.2. Implement a Corporate Governance Structure using Global Standards Business Ethics

Corporate ethics and governance are essential for protecting a sound reputation in the marketplace. Corporate Governance (CG) can be summed up by the acronym GAS: Governance (exercise of control), Accountability (being answerable to a system and to seniors), and Stakeholder Relations (those with vested interest in the company's performance).

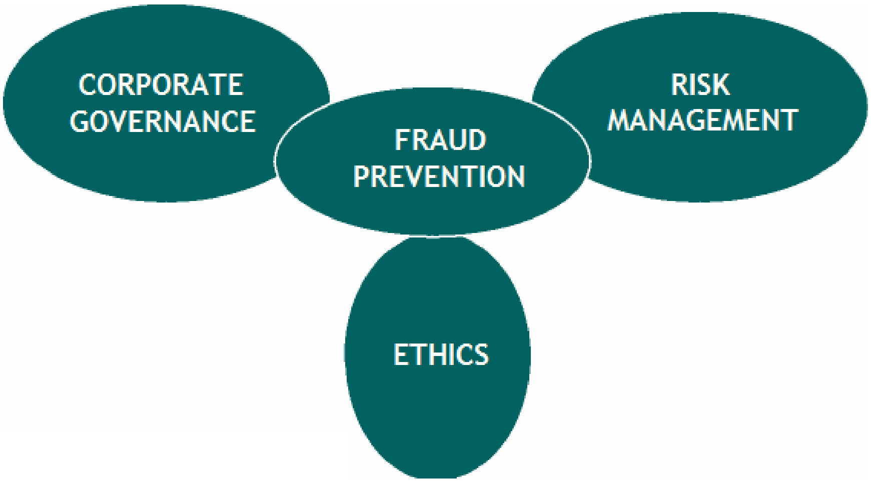


Figure 11: Insider Fraud Prevention Linkages

The Harvard Business Review of December 2005 outlined its impressive Global Business Standards Codex, which includes these 8 core principles:

1. **Fiduciary Principle**

   Fiduciary is a trustee, a person bound to act for another's behalf. Act as a fiduciary for the company and its investors. Carry out the company's business in a diligent and loyal manner with the degree of candor expected of a trustee.

2. **Property Principle**

   Respect property and the rights of those who own it. Refrain from theft and misappropriation. Avoid waste. Safeguard the property entrusted to you.

3. **Reliability Principle**

   Honor commitments. Be faithful to your word. Follow through on promises, agreements and other voluntary undertakings, whether or not embodied in legally enforceable contracts.

4. **Transparency Principle**

   Conduct business in a truthful and open manner. Refrain from deceptive acts and practices. Keep accurate records. Make timely disclosures of material information while respecting obligations of confidentiality and privacy.

5. **Dignity Principle**

   Respect the dignity of all people. Protect the health, safety, privacy and human rights of others. Refrain from coercion. Adopt practices that enhance human development in the workplace, the marketplace and the community.

6. **Fairness Principle**

   Engage in free and fair competition. Deal with all parties fairly and equitably. Practice nondiscrimination in employment and contracting.

7. **Citizenship Principle**

   Act as responsible citizens of the community. Respect the law, protect public goods, and cooperate with public authorities. Avoid improper involvement in politics and government. Contribute to community betterment.

8. **Responsiveness Principle**

   Engage with parties who may have legitimate claims and concerns relating to the company's activities. Be responsive to public needs while recognizing the government's role and jurisdiction in protecting the public interest.

Governance and ethical principles should be integrated into the culture of an organization. It is relatively easy and inexpensive to set up a corporate governance system:

- Commitment to CG system.
- Define stakeholder universe.
- Outline stakeholder value system.
- Set up communication channels for each level of stakeholder.
- Develop information security policy.
- After business process review, process owners are allocated and assigned responsibilities.
- Review of board structure to check independence and establish audit committee.
- Establish discipline code and reward system as part of corporate code of conduct.
- Set up whistle-blowing system.

5.2.3. It Starts with Recruitment

A robust recruitment policy is a necessary step in the prevention of insider fraud. Failure to properly screen during recruitment can result in increased costs later to the organization through loss recovery, investigations, and prosecutions.

The purpose of pre-employment screening should be to prevent infiltration and re-employment of offenders, as well as identifying employees susceptible to fraud. It is important that all banks have the correct procedures and background checks in place as well as establishing on-going monitoring of staff. The other purpose of screening is to find gems: people of proven integrity.

Summary: Employee recruitment checks are a first line of defense against insider fraud!

Pre-employment screening is vital and may require use of a specialist agency to perform thorough background checks and profiling.

Recruitment checks should be at least as stringent as the checks required to open bank accounts. CIFAS has identified the following best practice recruitment checks:

- Confirmation of previous employment details, sometimes going back 10 years or more
- Confirmation of all qualifications
- Confirmation of identity (name and address)
- Credit reference agency checks
- Fraud prevention checks (shared information)
- Taking up references
- Checks against own internal fraud databases
- Police/criminal background checks (essential for prospective employees)

Note: *Intensify background checks for all temporary staff!*

At a minimum, pre-employment checks must verify applicant ID and confirm previous employment and performance/conduct.

Profiling is increasingly being used to vet staff. How is this done?

- Highlight any gaps, inaccuracies, and discrepancies in the information provided by the recruit. Any negative information discovered could lead to automatic rejection of the candidate after an investigation is carried out as to why the discrepancy exists.
- Work with police to develop profiles of typical inside fraudsters. Compare candidates against insider profiles.
- Perform police/criminal background checks on all prospective employees.

- In terms of the application process, evidence suggests that Curriculum Vitaes (CV), or resumes, are not always a good indicator of either a candidate's suitability or their full employment history. A better approach than simply requesting a CV would be to use an application form with specific questions designed to obtain information not usually included on CV: convictions, bankruptcies, gaps, reasons for leaving, proceedings pending, etc. It has been shown that lying on CVs is fairly endemic in today's high-turnover job market.

5.2.4. Ongoing Vetting/Staff Monitoring

Although pre-employment screening will hopefully ensure the suitability of those appointed, employees' circumstances may change over time. Ongoing vetting of people in key roles should include annual background and credit checks on employees. This acts as a deterrent and reveals employees who may have a financial motive to sell information or steal from the bank. Though it would be an individual bank decision, one response could be to offer counseling and financial assistance to staff in difficulties.

Each promotion and change of job within an organization should be treated almost as seriously as a new appointment with rigorous checks, tests, and interviews accompanying the promotion or shift to a different position.

In addition, management needs to keep aware of changing circumstances in employees' lives such as divorce, debt, psychological problem, and so on. It is during traumas and big changes in employees' job or life situations that they may become vulnerable to temptations to commit fraud.

Some insider fraudsters became corrupt for the first-time after assuming a more responsible management position giving them access to greater levels of information with increased temptations. It is therefore desirable to implement a system of on-going monitoring of staff. Insider profiles show that fraudsters are often over-qualified for their role and that a majority are not registered on any electoral roll.

- Have stringent interviewing for promotions which are as extensive as for new recruits.
- Build in regular interviews and testing aimed at checking loyalty, trust, and integrity with all staff as part of performance appraisals.
- Beyond a whistle-blowing system, a company could set up trust managers with whom employees can discuss their difficulties (financial, personal etc.) within a confidential-sealed environment without fear of repercussions.

5.2.5. Tightening Security Access

- Strict visitor access system. Installation of a vigilant visitor access/departure policy.
- Ban mobile phones in sensitive locations.
- Security and information policy for systems access (deployment of need to have access control policy)
- Introduction of a company-wide clean desk and secure data storage and filing policy.

It is recommended that levels of authorization for access to the company's systems be underpinned by an authorization matrix. The matrix looks at risks involved in certain combinations of authorized access for staff and then blocks or bans those combinations that may create opportunities for potential insider fraud. Special approval procedures can be implemented for these risky combinations of authorized access. This can significantly reduce the risk of insider fraud.

5.2.6. Introduce a Whistle-Blowing Procedure

One pillar of corporate governance is setting up a confidential whistle-blowing system which allows employees, who suspect that transgressions of the corporate code of conduct are taking place within a company, to securely report such transgressions without fear of being victimized.

Whistle-blowing[5] is when an employee reports a suspected case of serious misconduct, irregularity, or non-compliance to an authority. The content of such a report could range from health and safety risks, potential environmental problems, fraud, corruption, cover-ups, to many other problems. It is recommended that companies set up a single, protected and anonymous whistle-blowing line for reporting suspected serious non-conformances of the corporate code of conduct as well as suspicious staff activity.

This line of communication should be independent of corporate management structures and needs to be administered fairly and objectively. The whistle-blowing function and system could report through to an audit committee.

The key elements of a whistle-blowing system are:

[5] The UK organization Public Concern at Work describes the difference between making a complaint and whistle-blowing, "When someone blows the whistle they are raising a concern about danger or illegality that affects others (e.g. customers, members of the public, or their employer). The person blowing the whistle is usually not directly, personally affected by the danger or illegality…. For this reason, the whistleblower should not be expected to prove the malpractice. He or she is a messenger raising a concern so that others can address it….When someone complains, they are saying that they have personally been poorly treated. This poor treatment could involve a breach of their individual employment rights or bullying and the complainant is seeking redress or justice for themselves. The person making the complaint therefore has a vested interest in the outcome of the complaint and, for this reason, is expected to be able to prove their case."

- Develop a company whistle-blowing policy, including proper management structures, methods of protecting whistleblowers, and a feedback and follow-up mechanism.
- Specify built-in protections for the anonymity or confidentiality of the whistleblower.
- Keep whistle-blowing system separate from the grievance procedures. Whistle-blowing systems are for reporting serious suspected cases of misconduct of significance to the whole company, while grievance procedures are for processing complaints from individuals rooted in personal grievances.
- Communicate the whistle-blowing policy to all staff as part of the corporate handbook.
- Educate staff on how to use the system, on the dos and don'ts of whistle-blowing, and create awareness that whistle-blowing functions positively as a company safety valve and early warning system. Whistle-blowing alerts employers or the public to danger or illegality while there is still time to address the problem; whistle-blowing can save lives, jobs, money, and reputations.
- Include overseeing the company whistle-blowing system as a responsibility of the audit committee with an annual audit of the system.
- Appoint a manager or director with several years of experience in business and a record/reputation for integrity to head up the whistle-blowing system.
- Create a secure phone line manned by trusted and senior advisors from within the company or outsourced to a trusted third-party.
- Create a secure system for recording the calls, documenting, and storage.
- Train senior and trusted staff to man the secure whistle-blowing line.

5.3. Information and Data Security Polices

Financial institutions should review their information and data security policies and procedures in the light of the specific threats posed by the rise of insider fraud.

5.3.1. Protecting Data

Best practice protection against theft of paper data will include strict enforcement of a clean desk policy, a clear policy on physical security to include access, and the shredding of documents and disposal of data. There will also be a review of processes and governance to ensure adequate supervision of staff at all times and reduction of the amount of customer information available to staff to a need to know basis. In some banks and card companies, the use of mobile phones has been banned in sensitive areas.

Whatever format the data is in, no single individual should have access to all of a customer's data (see PCI – DSS standards). It is important to define and separate roles responsible for key business processes and functions. Dual control means that two custodians must be involved in a task for it to be completed successfully.

Access rights, management solutions, and more secure employee authentication are recognized as key to securing computer data from internal attack. Access to data files should be restricted, controlled, and monitored so that any changes can be traced back to the person who made them. Password policy needs to be secure, strong, and require periodical changes. Employees should be trained to protect passwords. It is now recognized that password access only is not acceptable as many passwords can be easily broken. As a solution to this, two factor authentication involves the use of passwords with security tokens (something you know and something you own) or more recently biometric security measures such as thumb print or retinal scan (something you are).

These techniques are now being combined into three factor authentication: something you know, something you own, and something you are. Introducing two and three factor authentication makes it easier to change passwords on a regular basis. Other major technology projects taking place across financial institutions include investment in detection tools to monitor unauthorized or suspicious movements and access to data and systems.

Random auditing of all transaction involving an individual employee is a further deterrent to insider fraud. Data audits typically involve manual processes such as comparing electronic data modification history to paper records or examining electronic records for suspicious discrepancies.

It is essential that the bank has in place an acceptable computer usage and security policy. Without the former, computer forensics will have difficulty proving any wrong-doing. Security policy should include acceptable use of memory keys, hard disk, iPods, PDAs, and any other form of removable storage. There is a need to define what devices can be used and whether they are read only. There also needs to be an acceptable usage policy with regards to e-mail. In order to test their security, banks may employ a company to carry out approved penetration testing on their IT infrastructure. Using the same techniques as a hacker, an ethical hacker will test for discrepancies in the bank's security.

In the event of any attack on a bank's system, the backup system will be required. It is important that backup tapes are encrypted if stored off-site.

5.3.2. Detection and Prevention Measures

Remote video viewed over a networked PC provides the ability to access video footage of a particular event to determine culpability and can be used to detect theft of paper data, for example.

Note: *This is not true of all countries. Check the laws of your country regarding this issue.*

Cases of theft or manipulation of computer data require specific techniques to ensure the successful capture and prosecution of those responsible. Computer forensics involves the examination of computers to obtain potential legal evidence. Analysis of data can be difficult and many log file analysis tools are not designed for this purpose. Employing a computer forensics expert at an early stage removes the possibility that inappropriate handling of logs may render them unacceptable in evidence.

Computer forensic software can be used to examine employees' computers, even as they are using them, to ensure there is nothing to indicate any fraudulent activity. Using computer forensics, investigation times can often be shortened by the improved capabilities of these tools. They provide court admissible evidence and have a history of acceptance in court. However, to ensure an employee cannot claim that their privacy rights are infringed upon by such forensic analysis, companies must notify employees that this type of activity could be conducted at any time. This is also usually part of a company's corporate security policy statement.

Computer forensics should be used as a tool whenever a company has suspicions of fraud. In this way the computer can be viewed to confirm suspicions prior to a thorough investigation.

In the case of stored information, it is now possible to employ cryptographic solutions to render information tamper proof. Rather than perimeter security (e.g., passwords) controlling access to data, one alternative is to embed integrity at the data level, rendering information immutable, and securely logging and storing it in an independent registry. This deters, detects, and proves manipulation. Combined with existing encryption and access control technology, company data can be kept secure at the source. Solutions of this kind are already used in electronic voting environments where it is critical to secure the audit trail and can be implemented for any application that requires high level security for stored data.

5.3.3. Information and Data Security Policy

A company's information[6] security policy needs to be reviewed in the light of specific threats posed by the rise of insider fraud. Industry cryptographic standards need to be applied for all customer and transaction data.

5.3.3.1. Defining Information Sensitivity

These guidelines define the minimum security recommendations for classifying and securing an organization's information in a manner appropriate to its sensitivity level. This helps employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of the company without proper authorization.

[6] The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually, such as telephone and video conferencing.

For the purposes of these guidelines all company information is categorized into two main classifications:

- **Public Company Information:** Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to the company.
- **Confidential Company Information:** Confidential information contains all other information. Some information is more sensitive than other information and should be protected in a more secure manner. It includes information that should be protected very closely such as trade secrets, intellectual property, development programs, potential acquisition targets, and information integral to the success of the company. Also included in this category is information that is less critical, such as telephone directories, general corporate information, and personnel information which require a less stringent degree of protection. A subset of confidential information is third-party confidential information. This confidential information belongs or pertains to another corporation which has been entrusted to a company by another under non-disclosure agreements and other contracts. Examples of this extremely sensitive type of information include everything from joint development efforts, vendor lists, customer orders, and supplier information.

A company must be consistent and enforce its confidential information policies. Any employee uncertain of the sensitivity of a particular piece of information should seek clarification from their supervisor or manager.

5.3.3.2. Categorizing Confidential Company Information

The sensitivity of information should conform to a single corporate standard though it may remain the prime responsibility of the owner of the information. Labels are useful to indicate the level of sensitivity (e.g., Restricted, Internal Only, Confidential, and Strictly Confidential). Also, the labels could be used with the additional annotation. However, even if no labels are present, company information should be presumed to be confidential unless explicitly determined to be public by someone with the authority to do so.

Access to levels of information should be on a need to know basis.

5.3.3.3. Minimal Sensitivity of Information

Access to the information is allowed to:	Company employees, contractors, and people with a business need to know.
Distribution of the information **inside** the company is by:	Standard interoffice mail, approved electronic mail, and electronic file transmission methods.
Distribution of information **outside** the company is by:	National mail service and other public or private carriers, approved electronic mail, and electronic file transmission methods.
Electronic distribution	No restrictions, except that it should only be sent to approved recipients.

Storage	The information should be kept from the view of unauthorized persons; erase whiteboards and do not leave open on desks and tables. Machines used to store this information should be administered with security in mind; electronic information should have individual access controls where possible and appropriate. Protect data from loss.
Disposal/Destruction	Deposit outdated or unwanted paper information in specially marked disposal bins on company premises or shred using industrial strength shredder if available. Electronic data should be expunged or cleared; reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure:	Up to and including termination of employment. Possible civil and/or criminal prosecution to the full extent of the law.

5.3.3.4. More Sensitive Information

Access to the information is allowed to:	Company employees and non-employees with signed non-disclosure agreements who have a business need to know.
Distribution of the information **inside** the company is by:	Standard interoffice mail, approved electronic mail, and electronic file transmission methods.
Distribution of information **outside** the company is by:	National mail services or private carriers.
Electronic distribution:	No restrictions to approved recipients within the company, but should be encrypted or sent via a private link to approved recipients outside the company.
Storage	The information should be kept from the view of unauthorized persons; erase whiteboards and do not leave open on desks and tables. Individual access controls are highly recommended for electronic information. Protect data from loss.
Disposal/Destruction	Deposit outdated or unwanted paper information in specially marked disposal bins on company premises or shred using industrial strength shredder if available. Electronic data should be expunged or cleared; reliably erase using DoD compliant software or physically destroy media.
Penalty for deliberate or inadvertent disclosure:	Up to and including termination of employment. Possible civil and/or criminal prosecution to the full extent of the law.

5.3.3.5. Most Sensitive Information

Access to the information is allowed to:	Company employees and non-employees with approved access and with signed non-disclosure agreements.
Distribution of the information **inside** the company is by:	Direct delivery: signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution of information **outside** the company is by:	Direct delivery: signature required with approved private carriers.

Electronic distribution:	No restrictions to approved recipients within the company, but is highly recommended that all information be strongly encrypted.
Storage	The information should be kept from the view of unauthorized persons. Individual access controls are highly recommended for electronic information. Physical security is generally used and information should be stored on a physically secured computer. Protect data from loss.
Disposal/Destruction	Deposit outdated or unwanted paper information in specially marked disposal bins on company premises or shred using industrial strength shredder if available. Electronic data should be expunged or cleared; reliably erase using DoD compliant software or physically destroy media.
Penalty for deliberate or inadvertent disclosure	Up to and including termination of employment. Possible civil and/or criminal prosecution to the full extent of the law

5.3.4. Defining Security Vulnerabilities

In the past, software and hardware solutions addressed intrusion protection, antivirus, spyware, and adware. New approaches consider these and also the content and security of remote users.

Until recently, network security for the financial services sector has been based on content filtering. A proprietary messaging system, such as an SQL based email server, would filter electronic communications. Now, products exist that can automatically filter content based on text patterns in messages such as social security numbers, bank account numbers, security keys, and other sensitive information.

Modern networks must take a broader view of security. Any port, internal or external, is vulnerable.

When performing due diligence and product analysis of products from different vendors, it is best practice to do a proof of concept with your data and environment. This will help to identify obvious shortcomings in a product's capabilities.

5.3.5. Managing Outsourcing of Operations

When the storage or destruction of data is outsourced, the owner of the customer relationship retains responsibility. The delegating firm retains ultimate responsibility for duties undertaken in its name.

The management of such operations should entail constant auditing and receive the highest level of security. Contracts between parties should include security issues.

5.3.6. Fraud Records

Maintaining records of internal fraud cases is good practice and could help to form the basis of a predictive system. This could form part of a central Risk Register.

Sharing fraud records across the financial services industry through an industry fraud blacklist of known fraudsters is advisable in today's environment. Sharing fraud records greatly increases the chances of identifying potential and actual fraudsters. An industry-wide blacklist of known fraudsters could be created and kept in a fraud database.

5.4. Technology Considerations for Preventing Insider Fraud

Technical progress gives new opportunities for ATM deployers to improve the reliability and functionality of services they deliver through ATMs. At the same time, technology offers cybercriminals additional opportunities for illegal actions. Response by the IT security units of ATM deployers spans system administration, protecting the ATM end-points and software updates, to software development and deployment practices including protection from reverse engineering and multi-vendor software considerations.

Technologies for preventing fraud, both from insiders and from outsiders, are discussed in detail in Chapter 4: Mapping Software Operational Policy: Ensuring Confidentiality, Integrity, Availability on page 47.

5.5. Conclusion

Along with tight recruitment and staff vetting policies, an information security policy is the most important element of an integrated strategy for preventing insider fraud. New technology and approaches to security are available to help implement this information security policy. Matched with a corporate governance system and an anti-fraud culture in the organization, these are our most powerful weapons in the fight against insider fraud.

Chapter 6. Service Interface Protection for the ATM

6.1. Background

To maintain an ATM, authorized service personnel will have some access to the system. Service personnel requiring access will include field engineers for hardware and software maintenance, armored car personnel for cash replenishment, and branch or other service staff for consumable replenishment (e.g., receipt paper).

Any and all staff managing ATM procurement, deployment, installation, monitoring, and servicing must have the appropriate guidance, certification/technical expertise, and level of security awareness. The ATM deployer is responsible, and sometimes required through regulation, to ensure that security procedures are defined and followed for service staff. Some companies rely upon third-parties to perform all or some of the ATM service activities while others use in-house or contract staff. Independent of the choice of staffing, the information contained in this chapter outlines the best practice guidelines for the following people aspects of security:

- Servicing/Maintenance Interface
- Insider Fraud Prevention
- Fraud Investigation

6.2. Defining Best Practices for Servicing ATMs

With the growth of the ATM industry, ATM deployers often outsource all or part of the servicing responsibility to ATM manufacturers, ATM deployment organizations, independent service organizations, or others. While ATM deployers are able to directly implement security processes for in-house staff, greater diligence is needed in outsourced ATM servicing to maintain security from a people perspective.

For ATM deployers using both internal resources and outsourced services providers, the following best practices should be employed to ensure the safety and security of ATM transactions:

1. Establish physical security of the ATM to ensure only authorized personnel have access to ATM internals. Physical security, though outside the scope of this guide, is vital to ensure software-based and operational security practices cannot be bypassed.

2. Ensure all personnel are properly trained to manage/service the specific ATM model and types that are being serviced.
3. Third-party service agreements for servicing and maintaining ATMs should explicitly assign liability for fraud, including fraud that might be perpetrated through the software service interface of the ATM or by installing illicit software on the ATM.
4. Not all personnel need access to all parts of the ATM and therefore it is best practice to have role segregation and limit access for each role. For example, the individual replenishing receipt paper does not need access to the cash vault or hard drive; cash replenishment personnel may not need a passcode for an ATM's service interface.
5. Software security processes to access an ATM's service interface should always control segregation of functions and access to sensitive data based on a user's security level. Additionally, security processes should prevent sensitive or confidential data from being removed from an ATM's hard disk, except in the case where data should be removed for maintenance or end of life when the hard disk should be wiped clean.
6. For remote ATM access where allowed, there should be role separation for maintenance, debugging, or resetting the ATM between having read-only or write access. For example, a system administrator would have write access and a report generator would have read-only access. There needs to be a clear definition of each role; it is fundamental to maintain a system security.
7. Audit in-house staff and third-party providers at least annually to ensure compliance with lifecycle security processes.

Summary: ATMs can be vulnerable while being serviced; diligence of people, process, and technology is necessary to maintain security.

6.2.1. Case Study: Denomination Fraud in the US

In the US, ATMs for merchant locations are either leased or sold directly to the merchant with cash loaded directly by the merchant customer or provided as a service by the Independent Service Organization (ISO) utilizing a cash courier. Placement locations are normally owned by the ATM ISO or an agent of the ISO, such as a distributor. The location in these cases typically has no interaction with the ATM itself. The ISO handles all ATM performance or cash related issues and provides the placement location with a portion of either the surcharge or advertising revenue.

The majority of off-premises ATMs deployed in the US contain two or more passwords used to access a variety of menus. Most off-premises ATM models in the late 1990s came with a default password setting for both the master and administration access codes. The default settings were typically generic and constant with every ATM manufactured. The master (primary) password is used to access higher functions on the ATM, such as password maintenance, encryption key maintenance, terminal ID settings, denomination settings, troubleshooting, and surcharge data. Administrative or secondary passwords are typically used to access diagnostic menus, closing and balancing options, cassette configuration, and journal print and clear functions.

In these types of ATM deployments the master password is typically controlled by the ATM owner and the merchant uses the administration or secondary password to perform close functions, load cash, perform service diagnostic tests, and print/store journal data. ISO's utilized generic master passwords specific to their company or unique to each ATM, but the merchant normally did not have knowledge of this password. The master was provided to third-party service organizations or subcontractors to make adjustments and perform service in those higher-level menus.

Denomination fraud emerged when knowledge of the master password or default password setting on several models of off-premises ATMs allowed access to ATM denomination settings. Some off-premises ATMs could be set to dispense denominations as low as $1. Fraud occurred by accessing the management level menus and resetting the denomination setting from the $20 value of bills actually in the cassette to a lower amount such as $5 or $1. The perpetrator would then perform one or multiple transactions. For example, they could withdraw $20 and receive 20 bills that the ATM thought were worth $1, but were actually worth $20 – almost a $400 gain! Such a fraud cost the owner of a bowling alley ATM in Shawnee, Kansas $18,000 in just one week. See http://atmmarketplace.com/article.php?id=9602.

6.3. Fraud Investigation

In all cases, ATM deployers, financial institutions, and independent deployers who experience fraud need to report the incident to the local authorities immediately and retain the police report number or equivalent. This allows local and regional law enforcement to identify patterns across a geographic region and find those responsible for the fraud.

Summary: People need to be trusted, but ATM deployers cannot assume that all people are trustworthy.

Chapter 7. Emerging Technologies and ATM Integrated Payments Security

7.1. ATM Integrated Payments Security

ATM integrated payments includes all possible transactions that could be performed at an ATM. With the emergence of mobile infrastructures (cardless and NFC – near field communication), especially over the last few years, and the evolution of payment services (see ATMIA Best Practices for Mobile Device and Contactless Transactions https://www.atmia.com/best-practices/), the real questions are: Who plays what role is the payment transactions? How and what must be taken into consideration so that these transactions can be performed in a secure fashion?

Regardless of country or region, ATMs offer a similar experience to the customer. Business and financial services tend to include similar functions: checking account status/balance, withdrawal, deposit (cash/check), bill payment, etc. All of these functions are supported for different types of accounts: savings, checking, credit. A simplistic view of the customer interaction includes:

1. Insert/swipe card.
2. Enter PIN.
3. Choose transaction.
4. Account selection.
5. Enter transaction specifics (insert cash/check(s), amount to withdraw, etc.).
6. Complete transaction and take card.

Being able to perform the transaction revolves around two key elements: 1) a card (debit, credit, voucher-prepaid, etc.) being present, and 2) the customer entering a valid PIN for the card. With emerging technology, two questions could be posed:

- Do people using ATMs really need to have a card or can something else be used?
- Do people really need to enter a PIN at the ATM or can they use some other means for identification?

To be able to answer these questions and understand current and upcoming trends within the ATM environment, you need to understand the current status quo and movements within the current ATM integrated payments environment.

7.2. Current Status Quo

ATMs, irrespective of vendor, consist of a similar basic infrastructure. From a hardware perspective, a majority of ATMs run on an Intel-based computer using between 256MB and 4 GB of memory. Hard disk size is a prerequisite with a minimum of 1 GB free space while the majority is taken with the operating system and backups. With the jump in technology and fall in prices, hardware is not the problem it used to be.

From a software perspective, ATMs consist of a multi-layered software stack:

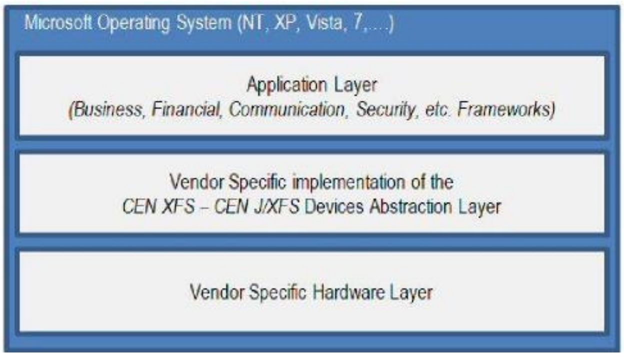

Microsoft Operating System (NT, XP, Vista, 7,....)
Application Layer
(Business, Financial, Communication, Security, etc. Frameworks)
Vendor Specific implementation of the
CEN XFS – CEN J/XFS Devices Abstraction Layer
Vendor Specific Hardware Layer

Figure 12: ATM Software Stack

- **Operating System:** Microsoft Windows® is the current de facto standard and most widely deployed operating system. While much has been spoken about the use of Linux, it has not been used to create a truly fully functional ATM for wide spread usage.
- **Hardware (Interface) Layer:** All ATMs contain hardware devices and their respective vendor specific driver software.
- **Device Abstraction Layer:** This layer is either CEN XFS (extensions for financial services) or CEN J/XFS (Java extensions for financial services) in most cases and delivers an abstraction layer between the underlying vendor specific hardware driver interfaces and the ATM application. Founded originally by Microsoft™ and later handed over to the European Committee for Standardization, the standard has the support of all major ATM software and hardware vendors (core members) as well as end users of this standard (associate members).

- **Application Layer:** The ATM payment application layer controls most activities and interactions including displaying a request for users to enter their PIN or choosing between different financial services. It also controls tasks such as communicating with a hardware device via the device layer to accept the PIN using the ATM's encrypted PIN Pad, writing to log/journal files, and more. The default transaction protocol is either NCR NDC or the Diebold 911/912.

With this in mind, one could say that while the rest of the world's IT environments have evolved from a fat client-server based architecture to a thin client web services architecture, the typical ATM environment has remained predominately a fat client-server architecture.

7.3. A Shift in the Sands

A recent gradual movement towards a more web-based architecture for ATM software has materialized. An increasing number of ATM deployers are investigating how they can implement new financial and business services (cash, check deposit, bill payment, transaction pre-authorization, one-to-one marketing) into their ATM environment using web services.

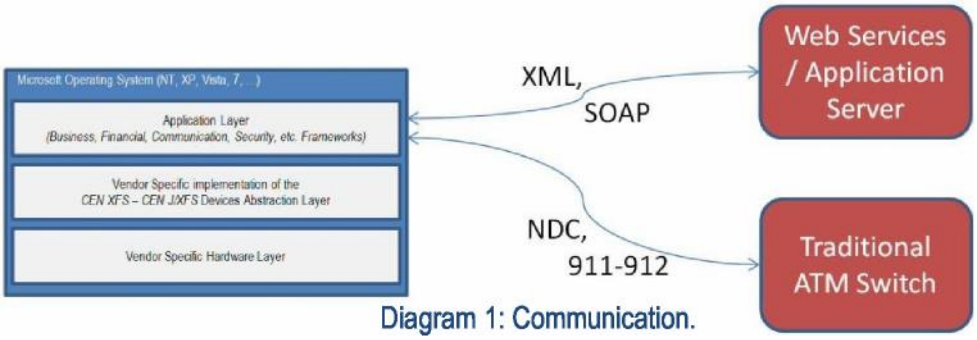

Microsoft Operating System (NT, XP, Vista, 7, ...)
Application Layer
(Business, Financial, Communication, Security, etc. Frameworks)
Vendor Specific implementation of the
CEN XFS – CEN J/XFS Devices Abstraction Layer
Vendor Specific Hardware Layer
XML,
SOAP
Web Services / Application Server
NDC,
911-912
Traditional ATM Switch
Diagram 1: Communication.

Figure 13: Communication

Taking advantage of web services and its underlying architecture (software components that communicate using standards-based Web technologies: HTTP, SOAP, XML-based messaging), ATM deployers have realized that they can design, implement, and integrate new web services to access customer/transactional data while keeping their traditional communication lines (NDC, 911/912) for transactions such as cash dispensing, account status, and PIN authorization. By using this technology, ATM deployers are receiving an improved time-to-market while at the same time satisfying their customer needs.

As with the introduction of web services, alternatives to the NCR NDC and Diebold 911-912 transaction protocols have also materialized. Interactive Financial eXchange (IFX)[7], an XML-based messaging protocol, was developed and released with the help of representatives from the retail, financial, ATM manufacturing, and servicing industries. While promising greater flexibility and interoperability, IFX installations are uncommon among ATM deployers.

[7] IFX Internet Site: http://www.ifxforum.org/home/

With the evolution of the ISO 20022[8] (the universal financial industry message scheme) in 2004, a new standard was released. Unlike IFX, NCR NDC, and Diebold 911/912, the ISO 20022 delivers a so-called recipe proposed by the ISO organization for the developing message standards for the different domains of the financial industry. The key ingredient of ISO 20022 is the development methodology which decouples the business standard from the physical message formats, a registration process, and a centralized repository. The ISO 20022 recipe offers a better, cheaper, and faster way of developing and implementing message standards. As with IFX, ISO 20022 is an evolving standard and one which has up-to-now not reached mass endorsement.

The future may look completely different. As we write this document, some recent events which may have a major impact on the future of payments include:

- Google announced Google Wallet in partnership with Citigroup, VeriFone, and MasterCard.
- Softcard payment wallet, supported by relationships with Visa, MasterCard, Discover, and American Express.

A business model scenario may be emerging where mobile devices can be used to initiate a payment transaction, such as paying for groceries. One can envisage that these payment services could be used to initiate and authorize payment transaction at an ATM, though an ATM with its specialized cash dispenser system will still be required to deliver actual cash to consumers.

7.4. New Security Requirements

Regardless of a traditional or more modern web services architecture, the communication protocol, and the schema being used, the vulnerabilities and security issues are actually very similar. Protection of cardholder information (e.g., PIN, PAN), the transaction communication, and transaction processing integrity must be upheld.

It all starts with the initiation of the transaction. To start an ATM payment transaction, a plastic card must be inserted or swiped into a card reader. Even if the plastic card is a smartcard (e.g., chip-and-PIN EMV), if a skimming device is present, the cardholder information can be stolen; remember all plastic cards still process a magnetic stripe. This vulnerability would also apply to contactless cards and NFC based cards. Currently predominant in the retail sector (MasterCard: PayPass; Visa: payWave; American Express: ExpressPay) and seen by the industry as delivering a safe alternative to the standard plastic with magnetic strip card, these too can also be skimmed, eavesdropped or are vulnerable to man-in-the-middle attacks depending on the type of transaction (NFC).

[8] ISO 20022 Internet Site: http://www.iso20022.org/

The answer to these problems has already been specified. The EMV contactless specifications describe how secure contactless transactions can be delivered. For EMV environments, processor-based contactless cards can be used delivering challenge-response authentication.

With regards to the ATM hardware, software stacks, and indeed the respective payment process, here the PCI SSC (Payment Card Industry Security Standards Council) with their PCI PA - DSS (Payment Card Industry Payment Application Data Security Standard) and PCI DSS (Payment Card Industry Data Security Standard) standard have created a good, if not comprehensive, set of security standards which if implemented and upheld will help mitigate potential risk and vulnerabilities.

With regards to security, all ATMs and their hardware and software stacks must deliver support to given international security standards as discussed in this document – especially the PCI DSS, PA-DSS, and PCI PTS standards as discussed in Chapter 2: Understanding the PCI Framework for ATM Software on page 18. These standards all influence how ATMs and the modules are manufactured, staged, operated, run, and in some circumstances decommissioned.

In essence the key security requirements with regards to ATM integrated payments security are consistent with the ATM software security guidelines discussed in previous sections of this document:

- Protection of cardholder information during initiation for the payment transaction regardless of source (e.g. contact, contactless, pre-authorization)
- Protection of cardholder information during all forms of communication: device to device, device internal communication (within hardware and software stacks), external communication (end-to-end).
- Protection of customers' identification.
- Protection of integrity of systems against manipulation and malicious software: code injection, code integrity, malicious software attacks, and incorrect configuration.
- Protection of systems against unauthorized and/or malicious access.

Security is only delivered when both systems and governance are combined. If only system or governance protection is being used, protection may be ineffective.

Chapter 8. Detecting and Mitigating Malware and Black Box Attacks

8.1. Overview

Over the last few years there has been an increase in incidents of ATM fraud involving both malicious software (malware) and sophisticated electronic (black box) devices. The primary objectives of such attacks is either to compromise data (including cardholder information) or force the ATM dispenser to deliver cash (jackpotting and cash-out attacks) without the need to use a genuine card and PIN to perform a transaction.

Attacks have been successful against various ATM models from different suppliers running different versions of ATM software. ATMs running Microsoft Windows operating systems appear to be better understood by the perpetrators and have been specifically targeted by most of the malware identified to date. This chapter explains the type of attacks that have been identified globally, indicators that can be used to detect such attacks, and highlights some key recommendations for mitigation. As different ATM models have been targeted, this chapter is intended to be generic and ATM vendor independent and is based on our knowledge of global attacks to date.

8.2. Black Box Attacks

Black box is the term commonly used to describe technically sophisticated electronic devices that are attached directly to an ATM in such a way as to allow the perpetrator to exert control over the functioning of the ATM. Black boxes that have been identified have ranged from simple form factor devices with electronic input and output sockets, LED indicators and rudimentary toggle switches to devices based on modified laptop computers, smartphones, and tablets.

While some black boxes have had the ability to intercept information such as cardholder data, administrator codes, passwords, and encryption keys, others have had the ability to inject malware on to the ATMs hard drive (see 8.3 Malware Attacks on page 102). The focus of this section is on black boxes that directly control ATM functions.

The most commonly targeted ATM module for black box attacks is the dispenser. Black boxes designed to control the dispenser allow the perpetrator to dispense cash without any need to perform a transaction using a card and PIN. Attached directly to the dispenser electronics or indirectly via the ATMs internal communications sub-system, a black box can operate in association with the genuine ATMs software or can completely replace the genuine ATM software which is, in effect, similar to replacing the genuine ATMs PC core with the perpetrators system.

To attach a black box, internal access to the electronics within the ATM cabinet or top box is required. It has been known to be achieved by:

- Use a genuine (or a copy of) the physical key to open the cabinet.
- Sabotage (or pick) the lock to open the cabinet.
- Cut a hole in the ATM fascia or cabinet.
- Impersonate a service technician to obtain access to the cabinet.
- Cabinet maliciously accessed by genuine staff of ATM owner or service company.

Execution of a black box attack is normally directly achieved by switches or keyboard input on the perpetrators electronics rather than via the genuine ATM card reader or keyboard. This can include commands issued remotely to a smartphone enabled black box pre-installed and connected to the dispenser within a compromised ATM.

Black boxes that are designed to take control of a module, such as to direct the dispenser to dispense cash, are known to overcome basic obfuscation methods intended to protect messages between the genuine ATM core and the dispenser.

As black box attacks on the dispenser effectively isolate the fraudulent activity from the transaction authorization and ATM monitoring systems, detecting attacks in progress can be difficult.

For attacks that involve physically opening the ATM cabinet or top box, it is possible to use alarms or, if the ATM is fitted with an auto-supervisor switch, monitor for the ATM entering supervisor mode unexpectedly. When the black box is designed to be connected directly to the dispenser or to be installed between the genuine ATM core and the dispenser module, it is sometimes possible to detect the dispenser being temporarily disconnected and disappearing from the list of active modules configured. In some ATM architectures, disconnecting an active module, such as the dispenser, can cause the ATM to reset or system escape. However, some attacks overcome this potential detection indicator by simulating the continued presence of the dispenser within the compromised ATM. The feasibility of using each of these indicators to act as a method of detection also depends on the ATM remaining powered on and in active communication with the remote monitoring system.

Perpetrators wishing to avoid allowing such indicators being used as detection methods are known to power down the ATM before commencing their attack. Also, some black box electronics require the ATM to be powered off and on or rebooted before the black box is able to be used to control the dispenser. For environments that normally have reliable power supplies and communications, an ATM disappearing from the network and restarting unexpectedly could be used as a potential method of detection.

After a black box has been installed (either left in place for a future attack or used and subsequently removed), well trained staff and service personnel can inspect the ATM for evidence of foreign electronics or if the internal cables have been disturbed. This can include cables being unclipped or untied from their normal fixing positions, rerouted, or left in a loose or not fully secured state in relation to being connected to the ATMs internal communications subsystem.

When a black box attack has successfully dispensed cash from the ATM, the ATM will often not balance correctly with transaction records at the host. Inspection of ATM maintenance logs (stored locally on the ATM) can sometimes provide evidence that the dispenser has been activated. However, it is not uncommon, particularly when a large number of notes are dispensed in a short time period, for operational problems to occur. For example, the dispenser may fail to pick some of the notes and this may be recorded as an event in the ATM's maintenance logs. Correlating the date and time stamp of such events with the central transaction authorization records at the host can be used to determine that the dispenser was actively dispensing at a time when no actual transactions were being authorized.

Indicators for detecting that a black box attack is occurring or has occurred can include the following:

- ATM cabinet opened (alarm or auto supervisor state activated).
- Dispenser module removed from the list of available modules.
- ATM system reboot including system escapes indicating a module was disconnected.
- ATM powered down then powered up when power supply is normally reliable.
- Inspection reports of black boxes or foreign electronic devices within an ATM.
- Inspection reports that internal ATM communications cables were untied, rerouted or loose.
- Inspection of local ATM logs showing pick fails or other dispenser operational errors without corresponding host records of cash dispense transactions being authorized.

8.3. Malware Attacks

There are a growing number of variants of ATM malware with different levels of functionality. Similar to black box attacks, a common purpose of ATM malware is to force the dispenser to deliver all or some of the cash held within the ATM. Other purposes include interception and storage of cardholder data and other sensitive information:

- Force dispenser to deliver all or some of the cash within the ATM (jackpotting/cash-out).
- Intercept and store card data (full magnetic stripe information or equivalent information such as track 2 data).
- Intercept and store in-the-clear PINs or encrypted PIN blocks.
- Decrypt encrypted PIN blocks by exploiting an insecure encrypting PIN Pad (EPP).
- Intercept and store initial ATM encryption key values and subsequent key change values.
- Intercept and store ATM administrative codes and passwords.

ATM malware is known to be installed in different ways. Examples of how confirmed malware attacks have been perpetrated include:

- Boot or auto-run using a USB device or CD / DVD disk which installs the malware on the ATM hard drive.
- Boot using a USB device or CD/DVD disk containing an operating system and application which allows control of the ATM directly.
- Access the Windows desktop and install malware onto the ATM hard drive from the command line.
- Use of a composite USB human interface and storage device to copy malware onto the ATM hard drive.
- Remote maintenance network system compromise.

With the exception of network compromise, physical access is required to place components within the ATM top box or cabinet, such as the ATMs PC core and internal communications subsystem. Access has been known to be achieved by the following methods:

- Use a genuine (or a copy of) the physical key to open the cabinet.
- Sabotage (or pick) the lock to open the cabinet.
- Cut a hole in the ATM fascia or cabinet.
- Insert a device via the card reader slot to interface with USB connectors or solder points.
- Impersonate a service technician to obtain access to the cabinet.
- Cabinet maliciously accessed by genuine staff of ATM owner or service company.

Once installed, ATM malware is known to be executed as follows:

- Using a specific ATM card to trigger the malware.

- Entering a specific sequence of numbers on the PIN Pad.
- Commands issued via a mobile phone connection previously installed within the ATM.
- Switches (buttons) on a composite USB human interface and storage device.

Characteristics vary between different types of malware which means that detecting the presence of malware during installation or after execution can be difficult and may require a thorough forensic examination of the ATM hardware and software. Some versions of malware are designed to securely delete themselves after a specific time period or after execution which can further impede an investigation. Indicators can include:

- ATM cabinet opened (alarm or auto supervisor state activated).
- ATM powered down then powered up when power supply is normally reliable.
- System reboots including system escapes without a recognized cause or error condition being recorded in the ATM logs.
- Logs including Windows event logs missing from the ATM hard drive.
- Indication that anti-malware software including whitelisting solutions were disabled.
- Malicious files with the same name as genuine files being present in incorrect directories on the ATM hard drive.
- Unexpected and unauthorized software updates were installed.
- Known malware files and signatures being present on the ATM hard drive.
- Inspection of local ATM logs showing pick fails or other dispenser operational errors without corresponding host records of cash dispense transactions being authorized.

8.4. Malware Examples

This section provides a summary of some of the known ATM malware variants that have been identified since 2008. This should not be considered to be an exhaustive list. Where a particular name has been regularly used to describe the malware this is mentioned for reference, but that does not necessarily mean that the actual executable is named as such.

8.4.1. Skimer-A

Discovery: 2008
First Location: Russia
Primary Purpose: Card and PIN compromise, Cash dispense
Infection Method: Physical access, Windows desktop

The Skimer-A Trojan was first reported as being used to target ATMs in Russia in 2008; although there is some indication that the malware was created in 2007. Variants were later detected in Ukraine and elsewhere in Europe. Physical access to the ATM cabinet is required to load the malware via the Windows desktop. The malware has the ability to intercept and store card data and PIN information as well as dispense cash. It has the ability to encrypt the compromised data and later print out the data using the ATM receipt printer and possibly write the data to a special ATM card. Activation is via a specific magnetic stripe card which when entered, opens a window on the ATM screen with a list of options, including one to remove the malware from the ATM and another to print out captured data. Another of the options opens a further window and prompts for the user to enter numbers on the PIN Pad. If specific numbers are entered then there is an option to dispense cash.

8.4.2. Unknown

Discovery: 2009
First Location: USA
Primary Purpose: Cash dispense
Infection Method: Bank employee

Malware permitted withdrawals from selected ATMs without a link to a valid account.

8.4.3. Scrooge

Discovery: 2010
First Location: Black Hat Security Conference
Primary Purpose: Card and PIN compromise, Cash dispense
Infection Method: Remote Administrator Network Connection and USB

The Scrooge root kit created by the late Barnaby Jack was demonstrated at the Black Hat security conference in 2010. Two different models of ATM were exploited: one via a dial-up remote administration network and the other by accessing a USB socket. Card, PIN, and Administrator information was compromised and the ATMs were made to dispense cash (jackpotted).

8.4.4. Siberian Malware

Discovery: 2010
First Location: Russia
Primary Purpose: Account compromise
Infection Method: Bank employee loading malware on ATM systems

The malware was capable of compromising consumer account details following ATM transactions. Funds were then transferred to another account under control of the perpetrators.

8.4.5. Dump Memory Grabber

Discovery: 2013
First Location: USA
Primary Purpose: Card compromise (track 1 and track 2)
Infection Method: Likely insider

Scans memory of infected device (ATM and POS) for card data and stores the data in a text file. There is POS variant known to use (FTP) or email to retrieve the compromised data.

8.4.6. Backdoor Ploutus

Discovery: 2013
First Location: Mexico
Primary Purpose: Cash dispense
Infection Method: CD/DVD drive

Ploutus is known to be loaded via a bootable CD/DVD Drive. Once installed on the ATM hard drive, it is activated by entering a specific set of numbers on the PIN Pad or via an external keyboard attached to the ATM. The numbers include the date of activation which time limits the ability to exploit the malware. If the numbers entered are valid, a graphical user interface (in Spanish) is displayed on the ATM screen which includes an option to select how many notes to dispense.

8.4.7. Backdoor Ploutus, Version B/Ploutos

Discovery: 2013
First Location: Mexico
Primary Purpose: Cash dispense
Infection Method: CD/ DVD drive

Ploutus (B) is known to be loaded via a bootable CD/DVD Drive. Once installed on the ATM hard drive, it is activated by entering a specific set of numbers on the PIN Pad. The numbers include the date of activation which time limits the ability to exploit the malware. If the numbers entered are valid, a window (in English) is displayed on the ATM screen which displays how much cash is available and logs activity as cash is dispensed. There is not an option to select how many notes to dispense.

8.4.8. Trojan.Skimer.18

Discovery: 2013
First Location: Russia
Primary Purpose: Card and PIN compromise
Infection Method: Infected application

Trojan Skimer 18 which when present on an ATM is activated by a special chip card which causes a window to be displayed on the ATM screen and accepts input from the PIN Pad. The special chip card is also used to store card and compromised PIN data.

8.4.9. Atmh4ck

Discovery: 2013
First Location: Chaos Communication Congress, Germany
Primary Purpose: Cash dispense
Infection Method: USB via cutting cabinet

German researchers (names withheld by request) demonstrated malware that is loaded by cutting a hole in an ATM cabinet to access a USB port and rebooting an ATM from their connected USB stick. A specific set of 12 numbers (000507607999) entered on the PIN Pad activated a menu window on a second desktop of the ATM screen displaying (in Portuguese) the quantity and value of notes (labeled R$, Brazilian Reals) in each cassette. A further set of 6 numbers was required to actually dispense cash based upon the concept of challenge and response thus controlling the ability to exploit the malware. In addition to directing the dispenser to dispense cash, other options included clearing log files, completely removing the malware from the ATM using a secure delete function, and disabling the ATM network adapters. The malware demonstrated was reported as being based on malware recovered from genuine ATMs. The malware appeared to be specific to individually targeted ATMs as the ATM hard drive volume serial number must match the specific customized malware.

8.4.10. Backdoor Ploutus, version B/Ploutos (SMS)

Discovery: 2014
First Location: Unknown
Primary Purpose: Cash dispense
Infection Method: CD/DVD drive or USB device

Ploutus (B) is known to be loaded via a bootable CD/DVD drive or USB device. Once installed on the ATM hard drive, it was originally (2013) activated by entering a specific set of numbers on the PIN Pad. An updated version can now be activated by an SMS text message sent to a mobile phone tethered to a USB port. A second text message activates the cash dispense function.

8.4.11. Unknown

Discovery: 2014
First Location: Latin America
Primary Purpose: Cash dispense, Card and PIN compromise
Infection Method: USB device

In addition to dispensing cash and compromising card data and encrypted PIN blocks, the malware includes key logging of the maintenance keyboard. If the maintenance keyboard is used to enter initial DES encryption keys these are compromised as well as subsequent host initiated key changes.

8.4.12. Backdoor.Padpin

Discovery: 2014
First Location: Russia, UK
Primary Purpose: Cash dispense
Infection Method: CD/DVD drive

Loaded by rebooting the ATM from the CD/DVD drive, malware is copied onto the ATM hard disk and not prevented from running by certain whitelisting protection systems. Cash dispense is activated by inputting specific numbers on the PIN Pad. The malware can delete event logs and remove itself which can hinder incident investigation. Although there are some similarities, it is different malware from the various Ploutus versions.

8.4.13. Macau Malware

Discovery: 2014
First Location: Macau, Ukraine
Primary Purpose: Card and PIN compromise
Infection Method: USB interface via card reader slot

Believed to originate from Ukraine, a sophisticated electronic device is inserted via the card reader slot to make contact with USB solder points at the rear of the card reader. The device enumerates itself as a composite USB device (storage and human interface) and copies malware onto the ATM hard drive. The malware collects card data and encrypted PIN blocks which are then decrypted exploiting an unprotected EPP on the ATM. Control chip cards are used to harvest card and PIN data and delete the malware.

8.4.14. Unknown

Discovery: 2014
First Location: Unknown
Primary Purpose: Cash dispense
Infection Method: Network compromise

Malware installed on ATMs following external compromise of an ATM deployers internal network. An unknown method is used to initiate cash dispense. The malware is securely deleted after the attack to hinder forensic examination.

8.5. Mitigation

ATMIA members concerned about ATM malware and black box attacks are encouraged to consider the following mitigation options:

- Train staff and service personnel to be vigilant in detecting any changes to the ATM which may indicate that unauthorized access to the ATM cabinet has occurred. This includes inspection for holes cut in the fascia, damaged locks, or out of place internal cables.
- Engage ATM solution providers and other specialists for guidance on installing and correctly configuring any applicable hardware, firmware, or software to detect and prevent malware and black box attacks. Also ensure ATMs comply with the latest PCI standards where applicable.
- Perform a risk assessment of the whole ATM estate recognizing that different ATMs, even of the same model, can have different levels of software and firmware installed or configured.
- Ensure that firewalls and anti-malware protection are correctly configured, including whitelisting solutions that cannot be disabled without generating a remotely monitored alert and audit trail.
- Prevent unauthorized USB devices from being installed (USB whitelisting).
- Deploy full hard disk encryption (FHDE) and encryption and authentication solutions to protect internal communications between the genuine ATM PC core and ATM modules, including the dispenser.
- Disable in BIOS the ability to boot or auto-run software from USB sticks and CD/DVD drives.
- Set and maintain strong BIOS password protection to prevent settings from being changed without correct authorization.
- Disable access to the Windows desktop at the ATM and maintain a robust password management policy.
- Implement secure remote key loading for ATM encryption keys and prevent the entering of encryption keys via the ATM supervisor or administrator keyboard.

- Enhance the physical security of the ATM cabinet or top box, including the use of high security locks, keys, and alarm systems.
- Effectively monitor the operation of ATMs paying special attention to unusual patterns of power outages, resets, communication failures, and an uncharacteristic lack of transactions being performed at normally high transacting ATMs.
- Implement SSL encryption between the ATM and the host.
- Monitor CCTV coverage of the ATM location for unusual activity at and around the ATM.
- Ensure access to the ATM cabinet is restricted to verifiably authorized persons and that such access is electronically logged.

Chapter 9. Further Reading and Links

9.1. Useful Reading

PCI SSC Data Security Standards Overview:
https://www.pcisecuritystandards.org/security_standards/index.php

ATMIA Best Practices:
https://www.atmia.com/best-practices/

ATMIA alerts:
https://www.atmia.com/education/security/fraud-alerts/

ATMsecurity.com reports of ATM Malware:
http://www.atmsecurity.com/index.php?searchword=atm+malware&ordering=newest&searchphrase=exact&limit=0&option=com_search

9.2. Standards Documentation

PCI Standards documentation can be found at the following link:
https://www.pcisecuritystandards.org

- Data Security Standard (PCI DSS)
- Payment Application Data Security Standard (PA-DSS)
- PIN Transaction Security (PCI PTS) – formerly known as PIN Entry Device (PCI PED)

Guidance for development of web applications can be found at Open Web Application Security Project (OWASP):
http://www.owasp.org/index.php/Main_Page

- CEN XFS-J/XFS (Comité Europeen De Normalisation Extensions for Financial Services, or Java Extensions for Financial Services) device interface standards

ISO Standards:

- ISO 11568 – Cryptography Key Management for banks
- ISO 11770 – Cryptography Key Management Lifecycle
- ISO/IEC 9564-1: Banking – Personal Identification Number (PIN) management and security. Part 1: Basic principles and requirements for online PIN handling in ATM and POS System
- ISO 13491 – Banking – Secure Cryptographic Devices (Retail)
- ISO 7810 – Identification Cards – Physical Characteristics

- ISO 7811 – Identification Cards – Recording Technique
- ISO 7812 – Identification Cards – Identification of Issuers
- ISO 7813 – Identification Cards – Financial Transaction Cards
- ISO 7816 – Identification Cards – Integrated Circuit(s) cards with contacts

Other standards and best practices of relevance:

- X9.24 Part 1: Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques.
- FIPS 140-2 – Specifications for security of Hardware Security Modules
- NIST SP 800 57 – Recommendation for Key Management
- ANSI TR-31 – Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
- ANSI Technical Guideline 3 (ANSI TG-3) – Guideline for Financial Services
- EMV:
  http://www.emvco.comhttp://www.mastercard.com/us/merchant/support/ptsprogram.html

9.3. Relevant Links

The following links are provided for informational purposes only. Inclusion here does not represent an endorsement by ATMIA or the contributors to this Guide of any specific product or vendor.

- Center for Internet Security (CIS) (provides security benchmarks and templates to harden and minimize many popular operating systems):
  http://www.cisecurity.org
- Visa Inc.:
  http://www.corporate.visa.com
- Visa's Risk Management section:
  http://usa.visa.com/merchants/risk_management/index.html
- PIN Security documents and references, including auditor's guides:
  http://usa.visa.com/merchants/risk_management/cisp_pin_security.html
- Microsoft Security:
  http://www.microsoft.com/security
- Security Development Lifecycle:
  http://www.microsoft.com/security/sdl/default.aspx

Chapter 10. Checklist of Recommendations for Securing ATM Operating Software

Check these items, one by one, to ensure you are implementing these software best practices.

10.1. Checklist Recommendation Details

10.1.1. Lifecycle Approach to Software Security

Adopt a holistic, systematic approach to the operational security of ATM software. To infuse the ATM operational software lifecycle with a security focus, all processes should be examined, including: (a) development, (b) installation (for example, tamper prevention), and (c) monitoring. Cover all phases of the lifecycle as follows:

10.1.2. Definition of the scope of the software system

This definition covers all technologies, processes, and people that are part of the system and could be vulnerabilities. It includes the crucial interconnection of the ATM application to the switch.

10.1.3. Risk Assessment

Create a risk register or threat model of all potential vulnerabilities of the ATM system. For each vulnerability, rate both potential damage and probability of attack as high, medium, or low.

10.1.4. Policy Creation

Based on the risk register, develop an ATM system security policy and best practices.

10.1.5. Security Testing

Once ATM system security policies have been created and introduced, the ATM system should be tested to ensure that all identified vulnerabilities are mitigated and that all policies are being followed.

10.1.6. Intrusion Detection

Monitoring could be accomplished through automated detection systems or random audits of technology and process. Intrusion detection should have a documented process for response if an attack is identified, including tasks and personnel assignments.

10.1.7. Continuous Review

Gather information from testing and detection activities and feed this information into the risk and vulnerability assessment matrix, regularly reviewing and adjusting security policies. In addition, any changes or updates to the system should trigger an analysis of the security risks that are associated with these changes.

We have positioned our ATM software security policy and procedures within a framework of the security lifecycle of development, installation, and monitoring.

10.2. Layered Security

In addition to adopting a lifecycle approach to ATM software security, construct layers of security in the software system. For example, a good core set of layered security would involve using network isolation, tested operating system hardening, secure operating processes, and central monitoring/management tools.

Best industry practice is to apply several layers of defense to provide better security for ATMs. This way, when a fraudster discovers a type of system vulnerability, your system is not immediately exposed; layers of security provide a set of checks and balances against fraud.

We have provided a core of layered security for our ATM software system.

10.2.1. Software Compliance Best Practices

It is recommended that all ATM operators abide by PCI security standards, especially PCI DSS, PCI PA-DSS, and PCI PTS. I is important to follow implementation guides drawn up by ATM manufacturers and ATM software developers, where available.

We have taken the necessary steps to comply with current PCI standards for card and card data security.

10.2.2. ATM Software Development Best Practices

10.2.2.1. Source Code

The ATM software's source code should be parsed through code checking software that analyses the code for security flaws. Another best practice is to carry out peer reviews of source code prior to final production.

10.2.2.2. Third-Party Software

The ATM software developer should audit suppliers of third-party software integrated with the ATM software per the lifecycle security process and ensure that these third-party products are not tampered with prior to installation.

10.2.2.3. Development Process

The ATM software development process should include anti-reverse engineering techniques. The ATM software developer should have mechanisms in place to inventory and track changes to the system throughout the development process and a final QA audit should include a security assessment as well as quality assurance. This should include exhaustive automated testing of the whole software stack to uncover gaps and unwanted functionality.

10.2.2.4. Digital Signature for Executable Modules

A best practice by ATM software developers is to digitally sign their executable modules so that recipients can verify that the files originated from a verifiable source and have not been tampered with.

10.2.2.5. Final Virus Check

Additionally, the final output (gold disks) should be virus-checked before packaging.

We have followed the above five steps for securing the development of ATM software.

10.2.3. ATM Software Installation Best Practices

Installation gives people full administrative access to the computer while the initial software installation occurs. Installation processes should ensure that the code is not tampered with during delivery. This could be as simple using trusted installers and some form of protection of the software during transit such as verifying the digital signing of files.

Instead of allowing the administrator unfettered access to the ATM, consider including specific configuration items to the supervisor interface so that only tightly-controlled configuration change is allowed. Also, see 10.2.7 Servicing and Maintenance Best Practices on page 119 for more information.

If the software is factory-fitted, then the manufacturer's processes need to be examined to ensure that the software is secured during the manufacturing and storage process.

Consider adding as much installation verification information as is practical to the supervisor panel of the ATM (e.g., the TCP/IP networking information, status of the local firewall, or any other configuration items) that would be problematic if they were misconfigured.

A best practice by ATM deployers is verification of digitally signed installation packages so that recipients can verify the files originated from a verifiable source and have not been tampered with.

In all cases an audit should be carried out after installation to confirm proper installation.

We have followed best practices for installing our ATM software, including post-installation audits.

10.2.4. ATM Monitoring, Administration, and Software Updating

An ATM needs good monitoring to stay secure. This applies to both ATM application monitoring and general ATM health monitoring.

All alerts should be actionable and have associated procedures. A good monitoring system includes problem identification and remediation.

Develop the capability to resolve the top ten most common ATM issues remotely using your ATM monitoring and management tools to perform predefined and well-scoped tasks.

The administrators authorized to use ATM monitoring and management tools should not be able to do so directly from their desktop PCs or laptops. Instead, it is recommended that all direct access to the ATM for problem identification and remediation is performed via a management/monitoring server with controlled access.

The central terminal server should have controlled access and allow authorized administrators to use a well-defined set of tools to monitor and manage the ATM.

When updating system software:

- Authenticate patches and software updates before installation.
- Perform an impact analysis to provide information of all payment application modules affected by the change.
- Test and review the impact analysis prior to installation.
- Virus test all software patches and updates prior to installation.

Ensure proper dual-custody controls so that no single administrator can both develop a change and implement it.

Systems management tools can allow for changes to be made to a large number of ATMs by central administrators. However, such systems management capabilities should always be used within a tiered administration structure where only top-tier administrators can perform the most powerful operations.

We have adopted best practices for ATM monitoring and software updating. We have adopted procedures for dual-custody control for all administrative tasks associated with ATM software. Systems management tools are controlled with a tiered management structure.

10.2.5. ATM Software Defence System: Firewalls, Anti-Virus, Whitelisting, Port Protection, and Patching

For ATMs communicating through a shared or outsourced network, a local firewall is necessary. Good desktop/endpoint firewall rules can prevent malware from reaching the ATM. Firewalls can be implemented in software as part of the ATM's operating environment or in a hardware device located within or near to the ATM. A software-based firewall has the most security as it cannot be compromised through physical access alone.

ATMs operate like any desktop and have interface ports. If a person has access to the ATM, such as a hardware maintenance outsourcer, they also have access to the ports and could insert malware or gain unauthorized access. Port control tools can prevent this access and only allow specific users to gain access based on authentication. Anti-malware can also provide port protection options.

Antivirus/anti-malware (AV) can complement a strong firewall system. Further, whitelisting is well-suited to the rigid operating environment of an ATM and is a recommended best practice for anti-malware protection.

A system of patching ATM software is required. Once the number of ATMs in an estate reaches any significant number, a central software distribution tool will reduce expenses while protecting the integrity of the ATMs and preventing downtime.

Prior to installing any patch, an impact analysis should have been conducted on the patch to ensure all payment application modules affected by the change are compatible and updated if necessary.

Patching ATMs requires that the ATMs are removed from service while patches are installed. Planning is needed to minimize customer impact from ATM downtime.

Strict and orderly change control is the secret to applying patches and upgrades in an environment where availability, integrity, and confidentiality are so important. The more software products that are installed on an ATM, the more patching will be needed.

The process of deciding which patches are needed and how important they are to apply is critical. Your organization should have a distinct set of criteria for patch decision-making, particularly to identify critical security patches as required by PCI DSS.

You should always be able to answer the question, which of my ATMs has received and applied patch X?

Define a standard patching rhythm. Monthly is generally considered the best practice today, though may be an aggressive timeline for some ATM deployers. A patch rhythm that is longer than quarterly is generally thought to be too long in today’s constantly evolving threat landscape.

Where a significant number of ATMs are to be patched, the best practice is to minimize customer impact by installing the patches in waves. The first wave, for example, might include half of the off-premise ATMs; the second wave might include half of the branch ATMs, and so on.

We have installed a local firewall for our ATMs, plus antivirus (AV), whitelisting, and a Host Intrusion Prevention System.

We also protect the interface ports of our ATMs.

We have implemented best practices for patching of our ATMs by including a standard patching schedule and knowing which ATMs have received what patches.

10.2.6. Encryption and Key Loading Best Practices

Central management of an encryption system is necessary to handle key management, revocation, and assignment.

The best practice is to load encryption keys through remote key management. In the absence of such capability, keys should be provisioned under dual control and in the case of the master key, through the encrypting PIN Pad.

The very essence of protection in an encrypted environment is the secrecy of the key. The role of key management is to ensure that the key remains secret through its lifecycle. The principles of segregated roles, access, and maintaining high levels of integrity through all stages are enforced using robust key management processes.

10.2.6.1. Generation

Most ATMs function on a single, symmetric encryption key – the terminal master key. Others employ dual encryption (symmetric key encryption over a PKI channel is not uncommon). The keys are generated as multiple components, usually two or three components and each component is generated by a nominated key officer/custodian.

10.2.6.2. Storage

The key components are stored for future reference and for distribution to the ATM (for provisioning).

Care needs to be taken that the storage repository for each component has a named owner. These conditions should also be met:

- No storage repository should store more than one component of any key.
- No key custodian should have access to more than one component of any key.
- The medium of storage should comply with ISO 11568 (Cryptography Key Management standards for banks) and ISO 11770 (Cryptography Key Management Lifecycle).

10.2.6.3. Distribution

This stage is by far the most vulnerable of all the stages in the ATM environment. Recommendations for best practices include employment of multiple, trusted personnel for provisioning the ATM or the best practice of deploying remote key technology where the key(s) and their components are not revealed to the user provisioning the ATM.

10.2.6.4. Use/Rotation

The encryption key(s) should only be in active use for a predefined period of time. For single level encryption keys, the refresh frequency should be 2 to 4 times a year. For multi-level encryption keys, each key should be refreshed at least twice a year.

10.2.6.5. Revocation

At the end of the key's defined life or as a result of a known/suspected compromise, the encryption keys will be suspended.

It is recommended that ATMs are audited (once every six months) against key management standards and processes.

Any cardholder data stored on the hard disk of the ATM should be protected from inappropriate inspection. One option is full disk encryption which will encrypt the hard drive regardless of what is stored and is transparent to any applications. Full disk encryption can be implemented by software or in hardware. Software-based encryption can work on existing ATMs, while hardware-based encryption requires installing new hardware or hard drives.

Alternatively, a file and folder encryption system can encrypt the areas that are known to contain confidential information.

It is important to get rid of the unmasked PAN in all files. This includes transaction logs (including electronic journals) and diagnostic logs from XFS devices and from the ATM application itself.

The network transaction traffic from the ATM should be encrypted. Many ATM deployments use a standard integrity control, the Message Authentication Code (normally referred to as MACing transaction traffic). In an ATM transaction, there is more information than just the PIN that may be considered confidential.

For example, account numbers, balances, and transferred amounts are also sensitive personal data and need to be secured. Transactions will contain the cardholder PAN and details of transactions. Some of the data may be considered to be Personally Identifying Information (PII), and as such is subject to local regulatory or statutory requirements. Using shared secret keys known to the financial switch and the encrypting PIN Pad in the ATM will protect against tampering with transaction data while it is in flight between the ATM and the financial switch.

Whenever possible, ATM management traffic should be protected with integrity checks and encryption. There are several well-established requirements for PIN and transaction cryptography and also for key management.

All in flight transaction data is protected and encrypted on our communications links to and from the ATM. In addition, ATM management traffic is encrypted. Both transaction traffic and management traffic are subject to integrity checks. We have a robust key management system in place to ensure that the key remains secret through its lifecycle. The principles of segregated roles and access are upheld.

10.2.7. Servicing and Maintenance Best Practices

Third-party service agreements for servicing and maintaining ATMs should explicitly assign liability for fraud – including any fraud that might be perpetrated through the software service interface of the ATM or by installing illicit software on the ATM. Both in-house staff and third-party providers need to comply with security best practices.

Not all personnel need access to all parts of the ATM and therefore it is best practice to have role separation and limit access to that necessary for their role.

Where a security role includes access to areas which may contain confidential or sensitive information, the best practice is to require dual control of entry. Ensure proper dual-custody controls so that no single administrator can both develop a change and implement it.

Systems management tools can allow for changes to be made to a large number of ATMs by central administrators. However, such systems management capabilities should always be used within a tiered administration structure where only top-tier administrators can perform the most powerful operations. For remote ATM access (e.g., maintenance, debugging, or to reset the ATM), the best practice is to require multi-factor authentication of the credentials of the person accessing the ATM. Multi-factor authentication typically validates something you know plus something you have – for example, a passcode and a token.

Additionally, security processes should prevent sensitive or confidential data from being removed from an ATM's hard disk. The exception is the case where data should be removed for maintenance or end of life, and then the hard disk should be wiped clean.

For remote ATM access where allowed, there should be role separation for maintenance, debugging, or resetting the ATM between having read-only or write access. For example, a system administrator would have write access and a report generator would have read-only access. There needs to be a clear definition of each role; it is fundamental to maintain a system security. In general, we recommend that all remote control tools should only be used after other predefined troubleshooting tasks have been exhausted. Further, remote administrative tools should have very strong controls in place to protect them.

With well-defined operational and troubleshooting processes, the number of times a user can interact with an ATM using full administrative access should move toward zero.

Audit in-house staff and third-party providers at least annually to ensure compliance with lifecycle security processes. All staff needs to be trained in the defense against criminals acting as trusted personnel in order to gain access to the systems.

Log all service/maintenance activity performed at your ATMs and retain all resulting access logs.

Policies and procedures are in place for ensuring the security and integrity of the ATM software system during servicing and maintenance activities. Log all service and maintenance activities. The best practices for appropriate role separation, dual control, and multi-factor authentication are implemented. In addition, we have narrowed down administrative access to the ATM to a necessary minimum.

Staff has also been trained to be vigilant about individuals accessing the ATM system.

10.2.8. ATM Password Policy

ATM passwords need to comply with password security best practices. The best practice is to control access via unique passwords, user IDs, and multi-factor authentication.

ATM vulnerabilities for insider fraud arise from a weak password system, including the following:

- Leaving the passwords set at the manufacturer’s default.
- Allowing the same password to be used for multiple ATMs; in other words, not requiring unique passwords for each ATM.
- Accessing the service password prompt without additional layer of security.
- Resetting passwords without affecting the current programming.

The best practice for password security includes:

- If more than one entity/person services an ATM, establish a unique master password and then unique IDs and passwords for each role.
- Use a strong and unique password for all accounts, especially the administrator account.
- Change passwords every 90 days or within a reasonable period based on service timing – for example, immediately following ATM maintenance.

We implement an ATM password system requiring unique passwords for each ATM. Passwords are never left at the manufacturer’s default. Access to the system for the purpose of changing passwords follows a multi-factor authentication procedure. We abide by password best practices.

10.2.9. Physical Security of ATM Computer

An attacker with physical access to the computer can remove ALL software security from play simply by swapping in his own prepared hard drive. The ATM's PC needs to be physically secured. Therefore, protect the hardware housing the software!

We have implemented a policy of physical protection of the ATM computer to prevent unauthorized access.

10.2.10. Preventing Reverse Engineering

To prevent reverse engineering attacks, the best practice for software vendors is to introduce anti-reverse engineering technologies.

We have used technologies recommended for prevention of reverse engineering attacks.

10.2.11. ATM Integrated Payments Security

When extending the kinds of payments that can be made via the ATM, such as bill payments, check deposit, or contactless payments, we have ensured the continued protection of cardholder data through attention to PCI security standards when installing expanded payment services.

We have upheld the protection of cardholder data through checking PCI security standards during the expansion of our payments services on our ATMs.

10.2.12. System for Reducing the Risk of Insider Fraud

Along with tight recruitment and staff vetting policies, an information security policy is the most important element for preventing insider fraud. Matched with a corporate governance system and an anti-fraud culture in the organization, these are our most powerful weapons in the fight against insider fraud.

We have implemented a system for reducing the risk of insider fraud.

10.2.13. Best Practice for Reporting Fraud

ATM deployers who experience fraud need to report the incident to the local authorities immediately and retain the police report number or equivalent. This allows local and regional law enforcement to identify patterns across a geographic region and find those responsible for the fraud. And where possible, share this information with other ATM deployers via a centralized fraud reporting program or other means to prevent widespread fraud.

We have implemented a system of reporting incidents of fraud.

10.2.14. Monitor Intelligence of Malware and Black Box Attacks

ATM deployers should stay abreast of the latest intelligence and reports of both malware and sophisticated electronic devices (black boxes) targeting ATMs.

We are aware of the latest malware and black box attacks.

10.3. Summary of Checklist of Recommendations

□ Lifecycle Approach to Software Security

□ Layered Security

□ Software Compliance Best Practices

□ ATM Software Development Best Practices

□ ATM Software Installation Best Practices

□ ATM Monitoring, Administration, and Software Updating

□ ATM Software Defense System: Firewalls, Antivirus, Port Protection, and Patching

□ Encryption and Key Loading Best Practices

□ Servicing and Maintenance Best Practices

□ ATM Password Policy

□ Physical Security of ATM Computer

□ Preventing Reverse Engineering

□ ATM Integrated Payments Security (where applicable)

□ System for Reducing Risk of Insider Fraud

□ Best Practice for Reporting Fraud

□ Aware of Latest Malware and Black Box Attacks

Appendix A. Ten Immutable Laws of ATM Security

Adapted from "Ten Immutable Laws of Security," originally published by Microsoft in 2000: http://technet.microsoft.com/en-us/library/cc722487.aspx

Authors: **Peter Kulik**, Vantiv, and **Pat Telford**, Microsoft

From a security perspective, ATMs have some characteristics that are unique to IT systems – the presence of cash being the foremost. But ATMs also have much in common with other IT systems when it comes to strategies and tactics in protecting against fraud.

No software patch by itself will ever protect ATMs from the issues described below – security is a function of People and Processes, in addition to technology. As Microsoft stated in 2000, sound judgment is the key to protecting yourself against these issues, and ATM deployers who keep in mind these Immutable Laws and the best practices described in the ATMIA Best Practices guide will significantly improve the security of their ATM systems.

1. **If a bad guy can alter the operating system on your ATM, it's not your ATM anymore**

   The threat of malware on ATMs is real and becoming greater with each day that passes. Malware can alter screen flow, intercept card data – even PINs are at risk. Most ATMs systems are installed using a gold disk approach – which provides enhanced security but also a single point of vulnerability. Operating system files are the most trusted files in an ATM, and have almost complete control of an ATM's operation - if the operating system on a gold disk is infected, the ATM is compromised from the very first transaction it completes.

   The key to protecting the gold disk installation is primarily through people and processes – employee screening, strong access controls, and dual control for installations are all important. Creation and comparison of a hard disk snapshot can start by comparing a newly-installed ATM with a known clean system to monitor for tampering in the installation process.

2. **If a bad guy has unrestricted physical access to your ATM, it's not your ATM anymore**

   The computer components controlling an ATM typically reside partly inside and partly outside the ATM's safe. Unrestricted physical access to the safe makes the cash vulnerable as well as the technology components – but unrestricted physical access to components outside the safe introduces risk as well. The most obvious are the card reader and PIN Pad on the front of the ATM, which can be compromised by skimmers, false keypads, etc. The components inside the locked ATM cabinet, but outside the safe, are also vulnerable to compromise from both hardware and software attacks such as plugging in a USB or even a DVD drive, replacing components inside the ATM – even removing the ATM computer and replacing it with an attacker's computer. Physical access allows any software or hardware component to be replaced; protecting physical access to ATMs starts with security of the site and use of unique keys for ATM cabinets.

3. **If you allow a bad guy to upload programs to your ATM, it's not your ATM anymore**

   When a computer program runs, it will always do exactly what it's been programmed to do, even if the program is harmful. Harmful computer programs can be loaded onto an ATM at several points of vulnerability. With physical access inside the ATM cabinet, a USB key or CD/DVD can be loaded and install malware. The telecom interface to an ATM also provides an attack interface for malware. In addition, a remote service interface also introduces vulnerability, for example through software distribution or remote control access to the ATM system. Best practices for physical security, telecom data encryption and restricted access through firewalls and related controls – as well as service interface and people processes protection – are all necessary to safeguard ATMs from malware.

4. **If a bad guy can persuade you to run his program on your ATM, it's not your ATM anymore**

   ATMs do not allow users to open up a browser window and browse the Internet, a common threat vector in laptops and desktop PCs. However, even if the ATM manufacturer's recommendations and other best practices have been followed, the bad guys continue to get more sophisticated and may find ways to break into ATM systems. Best practices to prevent and detect changes to ATM software files include a whitelisting solution that controls ATM processes and libraries executed, file access rights, network communications control, and device access control; as well as archiving a snapshot of an ATM's hard disk and regularly comparing the ATM to the archived image as a failsafe approach to detect an infection. Having the ability to quickly, securely, and (where practical) remotely reinstall an ATM from a known-good source is the ultimate remediation for malicious code.

5. **Weak passwords trump strong security**

   As Ben Franklin once said, “three people may keep a secret – if two of them are dead!” His comment presaged today’s best practices for password protection; ATM passwords should always be changed from manufacturer’s default at the time of installation. PCI requires use of strong passwords that are changed regularly – for ATMs this includes passwords for both the service interface as well as the operating system. Some ATM manufacturers have begun to introduce more sophisticated controls for service interface access, such as logins requiring both a password and unique token, more securely establishing the identity of the person logging in and aiding in tracking and auditing ATM access.

6. **An ATM is only as secure as the administrators and developers are trustworthy**

   Every ATM has administrators – trusted people who can install software, configure devices, manage accounts and establish security policies, and handle the other management tasks associated with keeping the ATM operational. ATM administration tasks are often completed on the ATM itself through a physical service interface – but increasingly, these tasks are performed through remote management tools. By definition, administrative tasks require control over the ATM, which puts the administrator in a position of unequalled power. Further, the developers of the ATM software itself are in a position of great power to control the operation of an ATM, and could write software to change screen flow or content, capture PINs, or access other confidential information.

   An untrustworthy administrator or developer can negate every other security measure – from uploading malicious software, to compromising encryption, to introducing a back door for access to ATM system files.

   Best practice people processes – hiring honest people to begin with, and then keeping honest people honest – are the basis for maintaining the trustworthiness of ATM systems. Secure development practices such as keeping an audit trail of changes to code and isolating development and testing activities – and people – help to secure the development environment. Dual control and the other best practices discussed for securing the service interface help to ensure the honesty of ATM administrators.

7. **Encrypted data is only as secure as the decryption key**

   Like the front door of your house – or the combination to a bank vault – encrypted data is only as secure as the key or combination needed to unlock it. If a key is tucked under the doormat, or the combination written on post-it notes in the manager’s office, the strongest locks in the world will do no good in keeping bad guys out.

Triple-DES (3DES) and encrypting PIN Pads (EPPs) are basic building blocks of data encryption for ATMs. Remote key technology eliminates paper keys and is a best practice for keeping 3DES systems secure – and for passing key audits with flying colors. Hard-disk based journaling may seem convenient, but has proven vulnerable to compromise; disk encryption may seem like a solution, but in practicality has proven unworkable since the encryption key is by nature vulnerable in an unmanned application. The best solution is to use a remote journaling system which can be effectively secured, and store no journal data on the ATM itself.

8. **An out-of-date security system is only marginally better than no security system at all**

   Microsoft's Patch Tuesday has become a highly-anticipated monthly event, though security patches for software components and antivirus updates are released almost daily it seems. ATM operating systems are tightly controlled and locked down so that most of these patches are not applicable for ATMs – but some are. Further, some security components on an ATM need to be updated regularly by design, such as malware detection systems which function based on files that define known malware – and are always growing. An ATM which has not been updated with security patches and current definition files is vulnerable to attack; over time, this exposure increases.

   Good centralized software distribution systems are available today to economically administer ATM patch and definition file updates. Using Whitelisting technology for anti-malware will require fewer definition file updates than other approaches. There are fewer attack vectors on ATMs than on internet-connected laptops, for example, so the frequency of patch updates can be lower for ATM operators who consistently follow best practices for ATM security. Deploying updates every one to three months is a typical, proven practice today for ATM deployers who have addressed the breadth of ATM software security best practices in their ATMs.

9. **Absolute anonymity isn't possible, in real life or ATMs**

   Despite our best efforts, as long as ATMs have cash, bad guys will seek to steal it. Likewise, as long as we use cards to access the cash in ATMs, bad guys will find ways to steal that card data as a means to steal cash. Whether through low-tech approaches such as card skimmers and telecom sniffers, or high tech approaches such as malware that alters screen flow and interfaces with an embedded mobile phone to phone home stolen data, the bad guys will always be just as creative as the good guys.

As a first step to protect cardholder data, ATM deployers should complete a thorough review of their ATM configurations to make sure their ATMs are not storing full user Primary Account Numbers, or storing them for only a limited period. Further, ATM deployers should have a plan in place in case of compromise, including notifying authorities and working with the appropriate card associations and/or networks to identify compromised cards and notify their issuers. Issuers should be sensitive to compromised card reports from their processors, networks, and card associations, and block and reissue compromised cards promptly. By reacting quickly, we reduce the value of stolen data to the bad guys, which in turn helps reduce the attractiveness of ATMs as targets for fraud.

10. **Technology is not a panacea**

Perfect security requires a level of perfection that is unlikely to ever be achieved – as long as security depends on People, Processes, and Technology, the people component will keep us ever-striving for perfection. Technology continues to evolve in amazing ways, but as long as human nature is vulnerable, technology will remain necessary but not sufficient for optimum ATM security.

An emerging best practice is to leverage human nature – i.e. the human desire to safeguard our hard-earned funds – to protect ATMs. Including ATM users as part of the equation for ATM security ranges from educating them to be aware the ATM fascia and report anything that looks suspicious – to displaying a picture on the ATM screen of what the ATM should look like and asking them to check and report any discrepancies.

ATM security is a journey, not a destination – as Microsoft stated in 2000, a constant series of moves and countermoves between the good guys and bad guys who both continue to get better at what they do. Our best practices for ATM security have evolved considerably since the invention of the ATM, and will continue to evolve as long as ATMs provide a valuable service to consumers.