

Ten Immutable Laws of ATM Security

From a security perspective, ATMs have some characteristics that are unique to Information Technology 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.

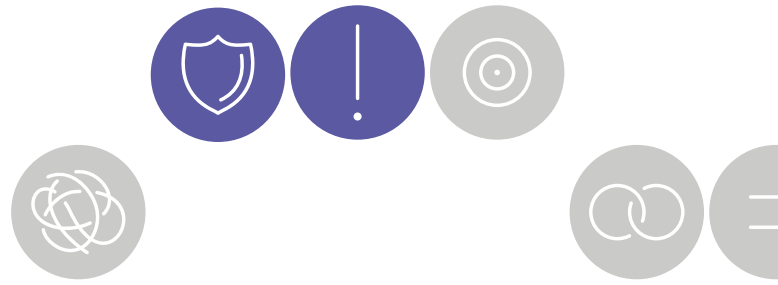
The components inside the locked ATM cabinet, but outside the safe, are also vulnerable to compromise from both hardware and software attacks such as plugging in a USB or even a DVD drive, replacing components inside the ATM – even removing the ATM computer and replacing it with an attacker's computer. 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.

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

Reprinted with the permission from the ATM Software Security Best Practices Guide, Version 2., published by the ATM Industry Association, October 2011. www.atmia.com. Authors: **Pat Telford**, Microsoft, and **Peter Kulik**, Vantiv.



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 is 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.

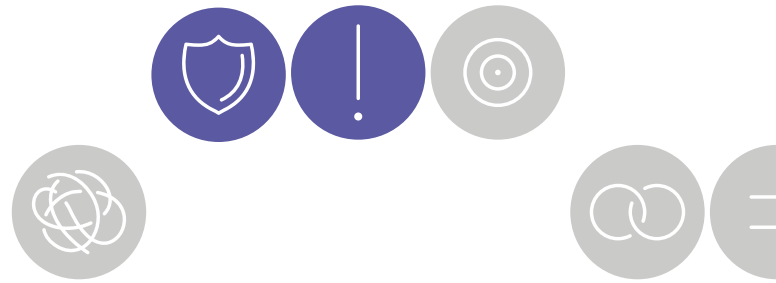
An untrustworthy administrator or developer can negate every other security measure – from uploading malicious software, to compromising encryption, to introducing a "back door" for access to ATM system files.

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 antimalware 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 of 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.