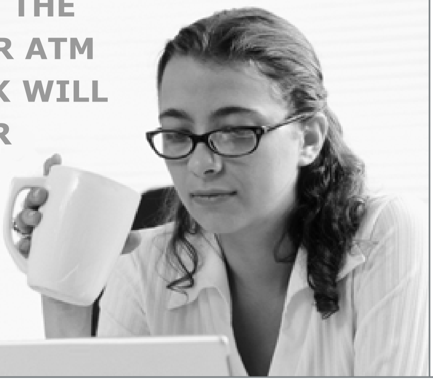
Software Security

NCR Webinar Series

CONTENTS



BY THE TIME SHE SEES THE **RISK,** HER ATM NETWORK WILL BE UNDER **ATTACK.**

SOFTWARE SECURITY IS NOT NEW

Bad news travels fast. Almost three years ago, the media picked up on two or three incidents where best practice ATM software security measures were not followed. This media attention focused on the risks to ATM security and the industry became nervous.

Much of this media 'hype' has now passed and there have been no further bad news stories. The risk profile of an ATM is now much better understood. Crucially, an ATM is not a PC, and is therefore not subject to risks associated with email or being on a shared drive, for example.

NCR has always worked to secure the software environment so that none of the bad news stories mentioned above could happen. NCR continues this work in today's Windows® environment with APTRA Security.

TOP OF MIND FOR THE IT INDUSTRY IS WHAT COULD BE CALLED **'TRADITIONAL THREATS'**. THIS INCLUDES **VIRUSES, WORMS, TROJANS AND SPYWARE**. HOWEVER, THESE ARE ACTUALLY SYMPTOMS OF THE PROBLEM, NOT THE PROBLEM ITSELF.

NCR SECURE™

The move away from OS/2 is an inevitable step forward for all financial institutions. The Windows environment brings new opportunities to offer value added services at the ATM and to efficiently integrate it with broader enterprise initiatives. To do this securely, there are best practice guidelines that all ATM deployers should follow.

Some of the key recommendations are: applying recommended patches in a timely fashion; designing- in 'least privilege' user principles; deleting services that are not being used; blocking ports that are not needed; and securing the broader network with appropriate firewalls and intrusion detection. Ultimately, it should never be forgetten that security in the 'trusted environment' is more than just technology. It is also about people and processes, and this is no different for Windows than in the old OS/2 environment.

THE REAL PROBLEM IS UNAUTHORIZED CODE

The ATM may be secure, but that is no excuse for complacency. The real problem for the industry is the introduction - from whatever source - of unauthorized code (whether malicious or not) and the harm it can cause.

Top of mind for the IT industry is what could be called 'traditional threats'. This includes viruses, worms, trojans and spyware. However, these are actually symptoms of the problem, not the problem itself. Point solutions have been designed by the IT industry, but they merely tackle these symptoms rather than address the real problem.

For instance, viruses were attacked with anti-virus solutions, worms gave rise to firewalls. Then there was intrusion detection for 'malware' that got past the other two. But the fact is none of these numerous ad hoc remedies was actually built on the others nor addresses the whole problem.

There is also a risk of unauthorized code from unknown threats. These are threats that today's solutions may not address.

Though patching is considered best practice, the environment remains exposed until the recommended patch is available, tested and deployed. Even automated patching is still a reactive process - and can bring other risks in itself. Only patches that are appropriate for a customer's application and network should be applied.

The industry has commented frequently on the determination and professionalism of today's 'hackers' and there is strong evidence of a link to organized crime. They are well funded, and are continually looking for weak links in the system and opportunities to exploit.

As with all fraud and crime, threats migrate and evolve to best hit their target. Currently, there is a move away from attacks on the operating system to the software applications themselves or to vulnerabilities in network devices such as routers or switches. Even vulnerabilities in some of the software security solutions that are deployed to protect the system could themselves be targets.

BY THE TIME THE **AUDITORS** ARRIVE, IT'LL BE **TOO LATE.**

THE REAL PROBLEM FOR THE INDUSTRY IS THE INTRODUCTION - FROM WHATEVER SOURCE - OF UNAUTHORIZED CODE (WHETHER MALICIOUS OR NOT) AND THE HARM IT CAN CAUSE.

INTERNAL THREATS

It is difficult to quantify, but analysts estimate that losses due to internal threats are growing faster than those from external threats. In essence any unauthorized change can potentially cause harm. Even a well-intentioned action can pose risks if there is a lapse in IT control. An example of this is a patch that is distributed with the best of intentions without proper testing. This could bring the ATM down.

In today's flexible environment, every application stack is potentially different. Although ATM software providers can recommend patches, customers still need to consider their own specific ATM software environment in case there are exceptions. All patches should be thouroughly tested before they are applied to make sure they do not affect availability.

The other internal threat comes from malicious 'insiders' - anyone who has access to internal systems - who may either want to cause harm or exploit opportunities for their own personal gain.

REGULATORY COMPLIANCE

These threats aside, it is regulatory compliance, not technology, that will likely be the biggest new challenge for IT organizations around the world.

The Sarbanes-Oxley (SOX) legislation in the United States applies to any entity doing business with the US, and requires a heavy investment in regulatory compliance. It may possibly be an even bigger financial commitment for many corporations outside, than within, the US. Though not directly affected today, many agree the ATM channel will inevitably be called into that audit cycle.

Other industry requirements are also starting to emerge. The Payment Card Industry Association (PCI), which includes VISA and MasterCard, is expected to introduce similar IT regulatory requirements for ATMs with its Data Security Standard. Other countries' banking associations and networks are also currently defining their requirements and that includes Interac in Canada and Cartes Bancaires in France.

The European Payments Council has published guidelines for ATM security, with the overall objective of avoiding "unauthorized software changes". It recommends that financial institutions have mechanisms in place that can detect any alteration to the software.

The ATM industry needs a solution that not only offers security through IT control, but also supports standards compliance. Many technology providers promote compliance, but this is not the same as regulatory compliance. While compliance may support internal policies and processes, regulatory compliance will demand significantly more rigor. ATM deployers will need to report on the security and state of all ATMs so all changes can be identified, reconciled against authorizations, remediated if necessary, or prevented. Deployers will need the capability to simply and easily provide real-time audit information on exactly what changes have been made to any ATM.

IDEAL REQUIREMENTS FOR ATM SOFTWARE SECURITY

Recent research from Deloitte highlights some interesting global trends.

Of the total number of financial institutions that experienced any kind of security breach in 2005, 72 per cent said the direct and indirect costs had totalled about US$1 million. Seventy-eight per cent experienced external attacks, mainly through 'phishing' and 'pharming', along with spyware and malware. Almost half, 49 per cent, had an internal breach of security, with insider fraud and theft of customer data being the main concern. And, overall, 91 per cent of the financial institutions surveyed are spending more in 2006 than in previous years on IT security, with the biggest spend being on logical access control products.

LOSSES DUE TO INTERNAL THREATS ARE GROWING FASTER THAN THOSE FROM EXTERNAL THREATS.

In light of these threats and business challenges, and in view of the solutions that exist today, what are the real requirements for software security on the ATM?

Since the security industry has typically created individual 'point' solutions to cover separate problems, a number of solutions may be needed to cover all scenarios. Further, each solution comes with its own associated inherent management and licence problems. Even if these issues were overcome, would any of these approaches cover tomorrow's problems or will we need new solutions?

The table below compares the characteristics of today's software security solutions to those of an 'ideal' solution.

SOLIDCORE FOR APTRA - TAILORED SECURITY AND COMPLIANCE FOR THE ATM ENVIRONMENT

In a shift from reactive defence to proactive control, Solidcore, an industry leader in IT control, has introduced an interesting new approach to securing systems. A growing number of companies in industries ranging from manufacturing to government are now deploying Solidcore technology to solve their security problems.

As indicated in the following table, today's anti-virus products are built around extensive lists of virus signatures that are used to try and identify threats as they come into the system and prevent those threats from executing on the device. While this can do a very good job of protecting a system from known threats, it requires constant updating and does not protect a system from threats that are unknown.

Today's security solutions	The 'ideal' solution
Define rules to find and stop bad code.	Defines (automatically, if possible) good code and only allows this to run.
Rule definitions are reactive, ad hoc and dependent upon "knowing the enemy".	Provides pro-active defence against known threats, and more importantly, unknown threats.
Managed through testing and deployment of updates to rules to defend against new threats.	Deployed once and left to get on with the job.
Rules-based security management is complicated and technically challenging. A slightly wrong rule can cause as much disruption as an attacker.	Automated and simple.
Regular updates lead to management pressure to test, verify and deploy patches quickly. If the process fails, there is downtime and the associated reputational damage.	Designed for maximum availability.
No reporting capability to verify what code is running on the ATM, and whether introduced by legitimate or illegitimate means.	Stops illegitimate methods of adding code, logs all added code through legitimate channels and creates a report for audit purposes.

The ideal solution is a single licence for today and tomorrow.

The last five years have seen a number of new technologies try to protect systems from unknown and complex threats. Most of these are based on developing rules either for what these threats or, conversely, good behavior should typically look like. However, all these 'solutions' have suffered from dramatic shortcomings around either effectiveness or performance impact. The reason is they can never model all of the possible threats or behaviors a system will experience given the wide variety of software that is running on a system.

The driving goal at Solidcore, right from the start, was to address the root problem with software security and not to create yet another point solution for today's problems. To achieve this, Solidcore consulted widely with leaders in the IT industry. The result was a unique security product based on control - one that knows exactly what code is authorized to execute on a device, and ensuring only that authorized code will ever be allowed to run.

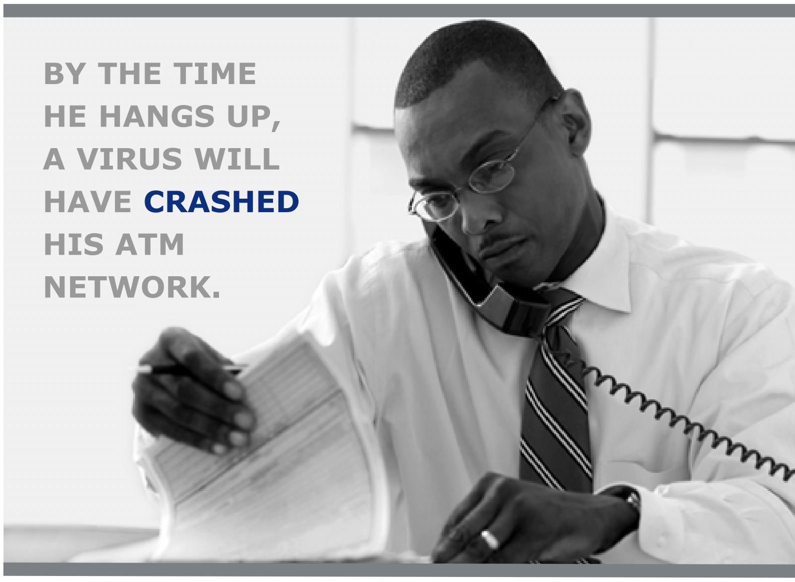
The unique benefit for the ATM industry of NCR's integrating Solidcore technology into its APTRA software suite is the way it will be able to address all potential categories of ATM channel risk. This includes traditional threats but most importantly unknown future threats, internal threats and the business risks associated with regulatory compliance. No other single technology or ATM vendor can do this today with one product.

Because it only allows authorized code to run and protects that code from being tampered with or hijacked, an ATM running Solidcore for APTRA behaves as if it were "cast in iron", completely shielded. There is no need to do real-time patching in a rush. It can now be done at the deployer's convenience, when it makes business sense.

Insider threats are nullified by control mechanisms that ensure any unauthorized or corrupted executable code that is placed on the disc of the ATM will not be loaded. However, the ATM system can be securely updated with authorized code.

The conventional approach to establishing and maintaining IT controls is to exhaustively document and review processes and policies. Though it may currently be acceptable, this approach, particularly in the face of challenging regulatory compliance requirements, will not only prove to be costly and inefficient but also error-prone. A sustainable compliance infrastructure must automate the verification and enforcement of IT controls with minimum overhead and reduce the need for documentation.

This would make it simple for an ATM deployer to provide auditors with real-time automated information on exactly what changes have been made to any ATM.



THE DRIVING GOAL AT SOLIDCORE, RIGHT FROM THE START, WAS TO ADDRESS THE ROOT PROBLEM WITH SOFTWARE SECURITY AND NOT TO CREATE YET ANOTHER POINT SOLUTION FOR TODAY'S PROBLEMS.

This approach was neatly summarized by judges awarding Solidcore for APTRA The Banker 'Fraud Prevention Innovation of the Year 2006':

"Through reducing the need for real-time patch updates and getting to the heart of the issue in fraud, whether perpetrated by internal or external parties, this was the best all-round challenge to the criminal fraternity we saw."

A SECURELY MANAGED ATM IN AN ACTIVE DIRECTORY ENVIRONMENT

As well as a secure ATM, there is also a requirement for a securely managed ATM; every secure environment needs a managed 'defence-in-depth' approach with complementary layers of security across the network to protect against attacks or inadvertent damage.

This is where Active Directory comes in. ATM deployers around the world are assessing the benefits of efficiently and securely managing the ATM channel through Active Directory.

Active Directory has two primary functions. First, it provides a central point to hold the accounts of users and computers so that both are authorized to function within the local environment. Second, it also provides a way to centrally manage Windows settings and configurations across an enterprise of servers, workstations or ATMs.

Given the prevalence of Active Directory, there are a number of deployers that see the value in integrating the ATM into their overall Active Directory strategy.

Using Active Directory means that each computer does not have to be configured individually. Instead it offers a central location to manage large groups of computers. This not only makes managing users and computers much more efficient, it offers the ATM deployer confidence that the entire estate has identical Windows configurations, removing the possibility that configuration errors be made on individual member computers.

Essentially, this is the most efficient way to make sure ATMs are configured to follow security best practice as the functionality of ATMs evolves over time. Active Directory allows a deployer to dynamically manage additional layers of defence in depth. This management includes:

- Dynamic administration of the Windows firewall, recommended to fully isolate the ATM from unwanted network traffic.
- Management of the other critical Windows security settings to provide a concise central summary of the Windows configuration of all ATMs.

BECAUSE IT **ONLY ALLOWS AUTHORIZED CODE TO RUN** AND PROTECTS THAT CODE FROM BEING TAMPERED WTIH OR HIJACKED, AN ATM RUNNING **SOLIDCORE FOR APTRA** BEHAVES AS IF IT WERE **"CAST IN IRON", COMPLETELY SHIELDED.**

- Grouping ATMs so that changes can be rolled out in a set of controlled releases across the ATM estate (this could include security changes or normal software updates that will occur over time as the ATM functionality changes).
- Centrally managing passwords so that only legitimate computers can become active ATMs and only legitimate administrators can make configuration changes. This removes the need to hold passwords locally on the ATM.
- Management of certificates that are sometimes used in the encryption and signing of messages as they travel outward from the ATM.

Though the technologies and skills sets to manage ATMs and PCs are the same (thus bringing cost savings), the two environments require different operational thinking and must be managed differently.

As an example, ATMs should be secured to prevent any users from logging on interactively to Windows. A second example is ATMs and their supporting servers should be as isolated as possible from other users, computers, and services available on the bank's internal network. A third is ATMs should be managed under very strict change control since they are public-facing, mission-critical computers.

Active Directory, through its ability to control and manage Windows configuration settings, can make it easy to manage security in the ATM environment. For example, the Windows configuration delivered to ATMs using Active Directory could be tightened to temporarily block all inbound network traffic and increase logging levels on the ATM during a period of suspected fraudulent network activity.

NCR has been working very closely with Microsoft®, from technical work at NCR's Research & Development labs in Dundee, Scotland through to live customer implementations. The output from this collaboration is a structure that allows the 800-plus Microsoft security settings configured locally today on an ATM to be securely, centrally managed using Active Directory.

This set of published guidelines can leverage the corporate investment in IT, while catering for the unique nature of ATMs.

NCR has a dedicated team of Software Security experts in its Global Fraud & Security Consultancy who can assist with Software Security including Active Directory and Solidcore for APTRA.

Now is the time to get secure and stay secure!

> **"THROUGH REDUCING THE NEED FOR REAL-TIME PATCH UPDATES AND GETTING TO THE HEART OF THE ISSUE IN FRAUD, WHETHER PERPETRATED BY INTERNAL OR EXTERNAL PARTIES, THIS WAS THE BEST ALL-ROUND CHALLENGE TO THE CRIMINAL FRATERNITY WE SAW."** THE BANKER

NCR

SECURE

NCR

NCR Corporation
1700 South Patterson Boulevard
Dayton, Ohio, 45479, USA
www.ncr.com

NCR continually improves products as new technologies and components become available. NCR, therefore, reserves the right to change specifications without prior notice.

All features, functions and operations described herein may not be marketed in all parts of the world. Consult your NCR representative for the latest information.