

August 2010

Banking Sector Security

Annual Research Review

.....
An MWR Labs White Paper

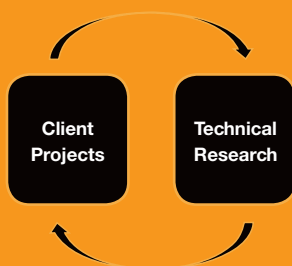
Foreword

As a security analyst I have worked extensively with the banking industry and have first-hand experience of many of the challenges that are currently faced in the financial sector. As a person with a responsibility on securing and protecting your organisations assets, you are no doubt highly dependent on the technology that runs your business processes. This dependency means you are exposed to a number of different risks.

My team at MWR Labs take an innovative yet practical approach to providing solutions to the major information security risks identified in the banking industry. This review highlights key issues including:

- Cyber Attacks
- Data Loss Prevention
- Identity and Access Management

These risks include key banking technologies and the manner in which they are used at the front line of your businesses.



For the challenges to be solved it requires a combined approach of fresh groundbreaking research in the relevant technology areas, alongside the testing of solutions that are currently in development or have already been adopted.

The ability to provide solutions to these challenges requires both testing projects for clients and research to feedback into the other. We have had considerable success using this approach and as a result the output from this work has enabled the identification of solutions across a number of key technology areas.

Ultimately, this engagement model has been highly effective at lowering the level of information risk and provided proven solutions to some of the critical challenges that you might currently face.

I hope the value of this approach is demonstrated in the results of this paper. I would like to thank you for your support with these projects and enthusiastically encourage you to continue to input into them. If you would like to comment on any of the work discussed here or to highlight research areas for the future please do not hesitate to contact me directly.

Martyn Ruks

Technical Director
MWR InfoSecurity Ltd

Introduction

MWR Labs welcomes you to its 2010 review of research undertaken into technologies in use in the banking sector.

MWR Labs is the research and intelligence arm of MWR InfoSecurity which performs all technical investigations into new and emerging threats. The Labs team provides a focal point within MWR InfoSecurity through providing research into key technology areas that interface with all client projects.

To undertake these projects, MWR Labs utilises the talents of some of the World's leading Information Security researchers, who adopt a flexible and novel engagement model that enables the provision of practical solutions to the major risks identified across various industries.

This review focuses on the banking sector and summarises various research projects completed in the past 12 months. Specifically we have worked closely with global banking organisations to solve the challenges they have faced. Generally these threats can be categorised into 3 areas:

- **Cyber Attack** – A slightly clichéd term but one that does a good job of summing up the continued onslaught of targeted malware and custom exploitation techniques. How can you ensure that your assets are protected against all possible types of electronic attack?
- **Data Loss Protection** – How can you protect against the loss or theft of sensitive information whether it is your information or that of your customers?
- **Identity and Access Management** – How you validate the identity of individuals accessing your systems when they are customers, suppliers and employees?

The review provides an overview of seven research projects conducted by MWR Labs. In each case, it provides a summary of the key challenges in the technology area, the research objectives, the threats identified, and MWR's findings.



MWR Labs would like to thank the following organisations for their support in research projects that have been conducted within the banking sector:

- **Visa Europe**
- **Thales**
- **Barclays**

In addition, it should be noted that MWR engages with UK Government authorities, such as the Centre for the Protection of National Infrastructure (CPNI), to help its understanding of threats to national security. This is used to guide the focus of specific research projects.

Where it is relevant or appropriate MWR will release public advisories related to specific technologies. A list of advisories and other publications related to the projects that are summarised within in this document are included with each finding.

Contents

| | | | |
|------------------|---|---------|---|
| Project 1 | Insider Threats: ATM Devices | Page 4 |  |
| Project 2 | Middleware: The Heartbeat of an Organisation | Page 5 |  |
| Project 3 | Cyber Warfare: Targeted Malware | Page 7 |  |
| Project 4 | New Attack Vectors: Mobile Banking | Page 8 |  |
| Project 5 | Privileged Access: USB Devices | Page 9 |  |
| Project 6 | Security Technology: Smartcards | Page 10 |  |
| Project 7 | Banking Applications: Threat Modelling | Page 11 |  |

Insider Threats: ATM Devices

Key Challenges: Cyber Attack

In March of this year Andrew Ashley and Nimesh Bhagat were convicted of offences relating to the creation of false betting slips. This particular scheme became unstuck after a cashier noticed that a winning slip for £600 for a £10 bet at odds of 35-1. The two individuals involved worked as IT contractors at the casino that was involved and had compromised the casino's systems to produce the false betting slips.

The case illustrates an area of growing concern; employees and contractor's with privileged access to systems that directly provide an opportunity to commit theft or fraud. Often the risk has been considered in terms of those that have system level access, however privileged access should also be considered in terms of physical access to interfaces or ports.

The ATM estate of many banks is now considerable and often ATMs are not located on company premises but in public locations such as railway stations or shopping centres. As such any compromise will highly impact the reputation of banking firms providing this service.

ATM Threats

This research was designed to examine whether the technical controls implemented within current ATM types present the potential to circumvent many of the inherent security features.

What are the threats?

A number of threats to ATMs currently exist including the following:

- Attack by a user of the system from the perspective of a customer
- Compromise of the system by a user with a legitimate level of physical access (an engineer or support person)
- A network based threat agent such as a worm or malicious attacker

What did we find?

The findings highlighted that technology that is deployed in security critical environments is not immune from security vulnerabilities. When the full range and potential sophistication of threats is considered it is important that all vectors of attack are assessed and tested. Solutions that are currently deployed are either incomplete and do not consider all relevant types of attack or they are not sufficiently robust to resist the threats that are facing them.

It was demonstrated that scenarios exist where ATMs are not able to resist all relevant threats resulting in significant risk being exposed to an organisation. It is important that organisations test their solutions to ensure that all viable attack vectors are protected by appropriate controls including a secure underlying platform and vendor supplied software product. As our findings highlighted even when appropriate controls are included in the design they do not provide the protection that is expected of them.

What is the Evidence?

The issues that have been identified in ATM technologies are currently being resolved by the relevant vendors. Further details will be published once the issues have been addressed by the vendor and affected organisations have been provided with the opportunity to upgrade affected systems.



Middleware: The Heartbeat of an Organisation

Key Challenges: Data Loss Prevention

What have you done today that involved middleware? You may be forgiven for giving the answer “nothing”. In reality if you have done anything that involved an electronic transaction then almost certainly middleware will have played a part in it. If you checked the balance of your bank account, looked at the availability of flights, booked a theatre ticket or bought a sandwich in a supermarket in the background messages would have moved between computer systems through the middleware. Some of the most important uses of middleware occur within the financial sector where it handles everything from money transfers to share transactions.

These examples highlight the fact that all businesses in the financial sector need information to be transferred between different systems and applications efficiently and securely. To do this a range of technologies that are collectively known as Middleware are used and are a fundamental component of a company's ability to conduct business. An attack against this component could have a significant impact owing to the fact that high volumes of critical data are often processed by these systems.

Middleware Attacks

This study examined the risks that are associated with Middleware and investigated key technologies that are used within the sector. The focus of the investigation was on methods that can be used to attack these technologies and the risk that this can expose.

What are the threats?

It is no surprise that given the importance of the information that passes through the Middleware layer that there are a number of threats associated with it:

- The technology is unfamiliar to security testers which results in security issues not being identified
- The ability to intercept messages being processed by these components results in exposure of sensitive data
- The methods of storing data within these components can result in the alteration of transactions
- The availability of multiple key systems could be affected where systems are not subject to appropriate controls

What did we find?

The findings revealed that the wide range of risks that are associated with Security issues in middleware technology are not being addressed by organisations resulting in excessive risk being exposed. This was determined to be primarily due to a lack of understanding about the importance of middleware technologies and the methods through which they can be attacked. It is important that Middleware technologies are subject to review by specialists with knowledge of their operation and business impact and that the results of testing are used to drive risk mitigation plans that accurately reflect the criticality of these technologies.



What is the Evidence?

The issues that have currently been identified in one key Middleware technology, namely IBM WebSphere MQ can be viewed at the following location:

<http://labs.mwrinfosecurity.com/projectdetail.php?project=5>

Specific vulnerabilities that have been published are as follows:

http://labs.mwrinfosecurity.com/files/Advisories/mwri_websphere-mq-ziiVSendReceiveAgent_advisory_2010-03-04.pdf

http://labs.mwrinfosecurity.com/files/Advisories/mwri_websphere-mq-rridecompress-advisory_2010-03-04.pdf

http://labs.mwrinfosecurity.com/files/Advisories/mwri_websphere-mq-rrilookupget-advisory_2010-03-04.pdf

http://labs.mwrinfosecurity.com/files/Advisories/mwri_websphere-mq-rriacceptOAMUserAuth-heap-overflow-advisory_2009-10-02.pdf

http://labs.mwrinfosecurity.com/files/Advisories/mwri_websphere-mq-getmem-heap-overflow-advisory_2009-01-12.pdf

http://labs.mwrinfosecurity.com/files/Advisories/mwri_websphere-mq-tcpreceive-heap-overflow-advisory_2009-01-12.pdf

http://labs.mwrinfosecurity.com/files/Advisories/mwri_websphere-mq-authentication-bypass-advisory_2008-03-26.pdf

http://labs.mwrinfosecurity.com/files/Advisories/mwri_websphere-mq-mcauser-setting-bypass-advisory_2008-03-26.pdf

Cyber Warfare: Targeted Malware

Key Challenges: Cyber Attack

With the advent of Internet Banking came the arrival of malware and Trojans whose purpose was to facilitate stealing money from customers. This is a widely publicised issue facing the banking sector and one for which there are now solutions on the market to address this. However, there is a much wider issue about protecting against targeted malware on key components that are used in the business process.

Whilst attacks against banking customers are usually conducted remotely across the Internet, other components may be at risk from trusted sources. In a much publicised case this year Rodney Reed Caverly pleaded guilty to installing malware on Bank of America ATMs and using it to fraudulently obtain money. These examples clearly highlight that the presence of malicious programs on computer systems whether they are owned by the bank or its customers can cost significant sums of money.

It is therefore important that any system that handles sensitive data such as an ATM or a customer's PC is protected against malware or other applications that might seek to intercept it. This is not a new challenge but one that requires both general and specific solutions to address and there is no shortage of claims from companies claiming to have achieved this.

Attacks on Security Solutions

This study examined whether a range of 3rd party solutions designed to protect retail banking systems such as ATMs or user systems could be subverted or nullified by an attacker.

What are the threats?

There are a number of threats associated with the installation of malicious software such as malware on systems handling sensitive data:

- Recovery of sensitive information from key presses, the system's display or network traffic.
- The collection of information and continued access to systems by the attacker through a covert communication channel.



What did we find?

The findings revealed that the use of 3rd party products to protect systems against the techniques commonly used by malware targeting the financial industry can be a key component in a security model. However, 3rd party software itself is not immune from the types of security vulnerability seen in other products. In addition it is important that the actual protection mechanisms that are claimed by a vendor should be understood to ensure that they are designed to provide the required protection against all the identified threats to a system. It is important that these solutions are subject to testing and that vulnerabilities in the software are addressed by the vendor. Whilst this sounds like a straightforward solution it is commonly observed that these relationships are not managed effectively. Often vendors will apply the letter and not the spirit of their contractual obligations and can result in additional cost and delay in ensuring that the software they provide is secure. Having an effective plan to manage these issues prior to purchasing is essential in ensuring good vendor relationships and secure software.

What is the Evidence?

The issues that have been identified in malware protection technologies are currently being resolved by the relevant vendors. Further details will be published once the issues have been addressed by the vendor and affected organisations have been provided with the opportunity to upgrade affected systems.

New Attack Vectors: Mobile Banking

Key Challenges: Cyber Attack / Identity and Access Management

Who hasn't got a smartphone? The adoption of smartphones amongst consumers has been rapid and many businesses including banks have looked to developed ways of interacting with consumers through these platforms. We have already seen smartphone apps for online banking, albeit with features limited to viewing balances or mini-statements. For example, Bank of America have developed a mobile application that allows bill payment and fund transfers if they have been setup through another channel. However, consumer pressure is growing to be able to use smartphones for a wide variety of financial transactions.

The reason for this is that as technology evolves, financial organisations need to keep up to date with the latest technology in order to meet customers' needs and provide easy access to services. However, the challenge is that smartphones have different security models to standard user PCs and this is what needs to be factored into the risk assessment around these technologies and solutions.

Smartphone Security

Our research was designed to explore whether client side software used by financial firms to facilitate customers' access and management of financial transactions, such as mobile phone applications, exposed organisations and customers to an elevated level of risk. This focused on both the manner in which the software and applications were designed and written but also the underlying security challenges in the wide variety of smartphone architectures that currently exist.

What are the threats?

Many of the threats faced on PC platforms extend to smartphones but with some further areas of specific concern:

- Interception of data submitted to a mobile financial application including usernames and passwords
- Alteration of the data displayed from financial applications, for example, stock market information
- Compromise of sensitive voice data including key tones and conversations

What did we find?

The threat profile is probably lower than that for PC based platforms, primarily as there are still plenty of opportunities for fraudsters on PC's. It is inevitable that smartphones will become a more attractive target as widespread adoption of the technologies and consolidation of market share increases the number of potential targets for each new attack. Security controls within mobile platforms are not all equally robust and all are potentially vulnerable to attack if not configured correctly. In addition, the architecture of some mobile platforms make them easier to attack than PCs and should be included as part of an organisation's mobile technology strategy.

What is the Evidence?

The issues that have been identified in smartphone technologies are currently being resolved by the relevant vendors. Further details will be published once the issues have been addressed by the vendor and affected organisations have been provided with the opportunity to upgrade affected systems.

A preliminary advisory about vulnerabilities in a specific smartphone can be found here:

http://labs.mwrinfosecurity.com/notices/palm_webos_145_vulnerability/

Further details of security issues affecting mobile platforms will be presented at the T2 security conference in Helsinki, Finland:

<http://t2.fi/>



Privileged Access: USB Devices

Key Challenges: Data Loss Prevention

If you search for the terms “USB” and “security” the results will not be a surprise to those people who have been working in the IT security industry for the past few years. They will be a combination of horror stories telling of lost data, virus and worm outbreaks and a range of solutions claiming to protect you from both of them. It is little wonder that finding solutions to these problems are high up on the list of priorities for the majority of organisations. Data Loss Prevention (DLP) strategies are one of the key challenges right now and the management of the now ubiquitous USB device is a key component of them.

Any threat which potentially negates the investment in DLP should therefore also be viewed as a key area of concern. The mantra that user input should never be trusted is well rehearsed and replayed by security professionals around the globe; however, it is important that it is viewed as more than just a tired cliché and should be heeded more than any other advice when attempting to protect any type of asset. Owing to the manner in which they operate the solutions deployed to provide protection against data loss are not immune from untrusted user input.

As well as the desktops and laptops that are typically protected by these DLP solutions a wide range of technologies used in the banking sector including ATM devices and HSMs now have USB ports. In most organisations at least one group of users is provided with a level of access where they could plug a device into these ports.

Privileged Physical Access

Given these potential risks to an organisation this study set out to prove whether USB attacks could be performed on banking machines, whether it is a user’s desktop or an ATM, by simply plugging in a malicious USB device.

What are the threats?

There are a number of threats associated with access to peripherals including those supporting USB, including the following:

- Loss of sensitive data from USB devices
- Bypass of restrictions enforced by DLP solutions
- Attacks against the underlying Operating System through a malicious USB device



What did we find?

Traditional threats such as the recovery of data from USB devices and smartcards is well documented and well understood; however, other threats are less well protected by security controls. Any systems that allow USB devices to be plugged in are potentially exposed to security vulnerabilities that could allow the compromise of the underlying infrastructure. This has been proven through the identification of vulnerabilities in the driver software used by the underlying Operating Systems. It is therefore important that security models are constructed which acknowledge the threat posed from a user with access to a USB interface. These attacks can render the protective measures that are currently implemented ineffective and could therefore mean the investment of resources in implementing them is negated. It is therefore concluded that DLP solutions that are designed to protect against the risks that exist from the use of USB technology do not always protect against all threats and should be subject to testing and review.

What is the Evidence?

Details of the findings from the USB research conducted by MWR InfoSecurity can be viewed here:

<http://labs.mwrinfosecurity.com/projectdetail.php?project=12>

Specific vulnerabilities that have been published are as follows:

http://labs.mwrinfosecurity.com/files/Advisories/mwri_linux-usb-buffer-overflow_2009-10-29.pdf

A number of additional issues that have been identified in USB software are currently being resolved by the relevant vendors. Further details will be published once the issues have been addressed by the vendor and affected organisations have been provided with the opportunity to upgrade affected systems.

Security Technology: Smartcards

Key Challenges: Identity and Access Management

Smartcards will solve a wide variety of challenges that the IT industry is currently faced with. After all if we trust them enough to put on bank and credit cards then they must be secure enough. It is true that significant time and effort has been invested in developing secure smartcard solutions as well as research into its implementation. Whilst there have been bumps in the road and more and more ingenious attacks have been devised, a comfort level has been reached with regard to the technology. However, in this rush to protect the data on our smartcards we have largely forgotten to protect the systems that process the data stored on them.

When we consider where the data read from smartcards is actually processed we start to realise that we should only ignore this attack vector at our peril. Whether we use a smartcard to log onto our PC, use it to withdraw money at an ATM or use it to unlock keys on a HSM the data passes deep into the heart of the banking sector's most sensitive systems.

Malware Loaded Smartcards

This study set out to prove whether Smartcard attacks could be performed on banking machines, for the good of the attacker, simply by inserting a malicious card into the smartcard reader.

What are the threats?

There are a number of threats associated with access to peripherals including those supporting smart cards and USB, including the following:

- Recovery of sensitive information from a card or copying of data onto another card
- Bypassing controls enforced by software that processes data from smartcards
- Attacks against back-end systems through malicious smartcards

What did we find?

The protection of data on smartcards, whilst not always implemented correctly, is traditionally an area that is well documented and understood; however, other threats that exist due to these devices are not well researched or protected. Where physical access to the smartcard reader is provided to a user any vulnerability that is identified could easily be exploited by inserting a specially crafted card. We have identified that a limited subset of solutions are used to read data from smartcards and are not as robust against attack as we might like to think. It is therefore important that security models are constructed which acknowledge the threat posed from a user with access to a smartcard interface and that the solutions that we place so much trust in are subject to detailed testing and review.

What is the Evidence?

The issues that have been identified in smartcard technologies are still in the process of being investigated. Further details will be presented at the T2 security conference in Helsinki, Finland:

<http://t2.fi/>

Full details will be published at this time; however, further details will be provided once they have been addressed by the relevant vendors.



Banking Applications: Threat Modelling

Key Challenges: Cyber Attack

When we watch the movies we all know that wherever there is a wooden chest full of gold coins, there will be pirates close at hand, likewise if there is a bank vault there will be bank robbers. It comes as little surprise then that wherever there are banking solutions that rely on IT, there will be the Cyberspace equivalent of the more traditional thief. It is therefore no wonder that the banking sector invests heavily in security technologies and their testing to ensure these systems cannot be successfully attacked.

Given the value of the assets in banking environments it is important to ensure that all threats are considered as a malicious entity is likely to invest significant resources in attempting to gain access to them. The methods they can utilise to attack the systems should be assessed when defining the activities that are used to test banking systems and applications. Without this approach security testing cannot provide the level of assurance required by the business.

Threat Focused Approach

The aim of this study was to assess the threats to a commercial banking system and identify whether the risks that were exposed had been mitigated with appropriate security controls. The objective was also to identify whether security assurance activities were being targeted at the areas of greatest risk to the organisation.

What are the threats?

There are a number of threats associated with a complex business process that has reliance on IT components:

- Undocumented or unknown inputs to the system that are not protected by security controls
- Unintended levels of access being granted to legitimate users through attack vectors not considered within the security model



What were the findings?

The findings indicate that security testing of these environments do not necessarily identify attack vectors that could result in significant financial losses being incurred by the organisation. This can be due to the absence of detailed threat modelling processes not having been followed. This can result in an absence of security controls because no mapping between current threats and the techniques they utilise does not occur. It is therefore important that financial systems and processes are subject to appropriate threat modelling so that security testing and assurance activities can accurately identify where controls are required to protect the assets that are processed within the system.

What is the Evidence?

The findings that have been obtained from this area of research are specific to individual client environments. Once the findings have been sufficiently anonymised further details will be published.

About MWR Labs

MWR Labs is the research and intelligence arm of MWR InfoSecurity which performs all technical investigation into new and emerging threats and was a key component of the work undertaken here. MWR Labs is committed to undertaking research that will assist organisations in the prevention of business threatening security breaches by exposing vulnerabilities and the methods by which they might be exploited by attackers. To achieve this it utilises the talents of some of the World's leading Information Security researchers who are employed within the technical consultancy team at MWR InfoSecurity.

The research is driven by two areas: new technological advances, and client specific requirements. This focusing of research activities into relevant commercial streams enables highly relevant data to be collected and disseminated to the appropriate stakeholders.

To this end, MWR Labs is committed to:

- Identifying and communicating the risks that can be exposed through the adoption of new technologies
- Application of the mitigation techniques for these risks to meet specific client needs
- Working closely with key stakeholders including vendors to ensure issues that are identified are resolved

This approach and close working relationship between the research capability and consultants engaged on client projects allows the effective sharing of threat and intelligence information about emerging threats on client engagements. This provides clients with up to date and accurate information about this fast moving aspect of technology and enables them to more effectively deploy resources to mitigate the risks that they face.

For a list of the latest MWR Labs events or speaking engagements look at:

<http://labs.mwrinfosecurity.com/notices.php>

Follow MWR Labs on Twitter:

<http://twitter.com/mwrlabs>

MWR InfoSecurity

St. Clement House
1-3 Alencon Link
Basingstoke
RG21 7SB
UK

Tel: +44 (0)1256 300920

Fax: +44 (0)1256 844083

MWR InfoSecurity (South Africa)

Suite 277
Private Bag X51
Bryanston
2021
South Africa

mwrinfosecurity.com



This white paper is provided for general information purposes only and should not be interpreted as consultancy or professional advice about any of the areas discussed within it.

If you would like to have a conversation about the topics raised in this document, please contact:

Jonathan Care

Head of Practice; Fraud, Risk
and Compliance

jonathan.care@mwrinfosecurity.com

Martyn Ruks

Head of Practice; Technical Consultancy

martyn.ruks@mwrinfosecurity.com

Harry Grobbelaar

Head of Practice; Technical Consultancy,
South Africa

harry.grobbelaar@mwrinfosecurity.com

