Infosec- Resources

Advanced ATM Penetration Testing Methods

By **BALAJI N** - November 26, 2017 7

Newsletter

ATM Penetration testing, Hackers have found different approaches to hack into the ATM machines. Programmers are not restricting themselves to physical assaults, for example, money/card catching, skimming, and so forth they are investigating better approaches to hack ATM programming.

An ATM is a machine that empowers the clients to perform keeping money exchange without setting off to the bank.

Utilizing an ATM, a client can pull back or store the money, get to the bank store or credit account, pay the bills, change the stick, redesign the individual data, and so on. Since the ATM machine manages money, it has turned into a high need focus for programmers and burglars.

Most Popular

Google Released Security Update for Android and Fixed 16 Critical Vulnerabilities

March 7, 2018

Now We Aware Who is the NSA Employee kept Top Secret...

December 2, 2017

Droidclub Botnet via Malicious Chrome

In this article, we will perceive how do an ATM functions, security arrangements used to secure the ATMs, diverse sorts of infiltration testing to break down ATM security and a portion of the security best practices which can be utilized to evade ATM hack.

Also Read **ATM Black box attacks – ATM Jackpotting**

ATM Work Function :

Most of the ATMs have 2 input and 4 output. The card reader and keypad are input whereas a screen, receipt printer, cash dispenser, and the speaker are output.

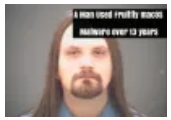
There are for the most part two sorts of ATM's which vary as indicated by the way they work. They can be called as

1.Rented line ATM
2.Dial-up ATM machines

Any ATM machine needs an information terminal with two data sources and four yield gadgets. Obviously, for this to happen there ought to likewise be the accessibility of a host processor. The host processor is important so that the ATM can interface furthermore speak with the individual asking

Extensions That Affect More Than Half...

February 2, 2018



A Man Used Fruitfly macOS Malware over 13 Years For Spying...

January 12, 2018

Fourth Fappening – Hacker Pleads Guilty to Hacking into iCloud accounts...

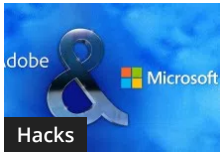
January 15, 2018

Recommended

4 Cybersecurity Risks We willl Face With New WhatsApp Status...

5 Methods to Secure Your Company's Data from Cybercriminals

A perfect way to Start and



Adobe & Microsoft

for the money. The Internet Service Provider (ISP) additionally assumes an essential part in this activity. They go about as the passage to the halfway systems furthermore the bank PC.

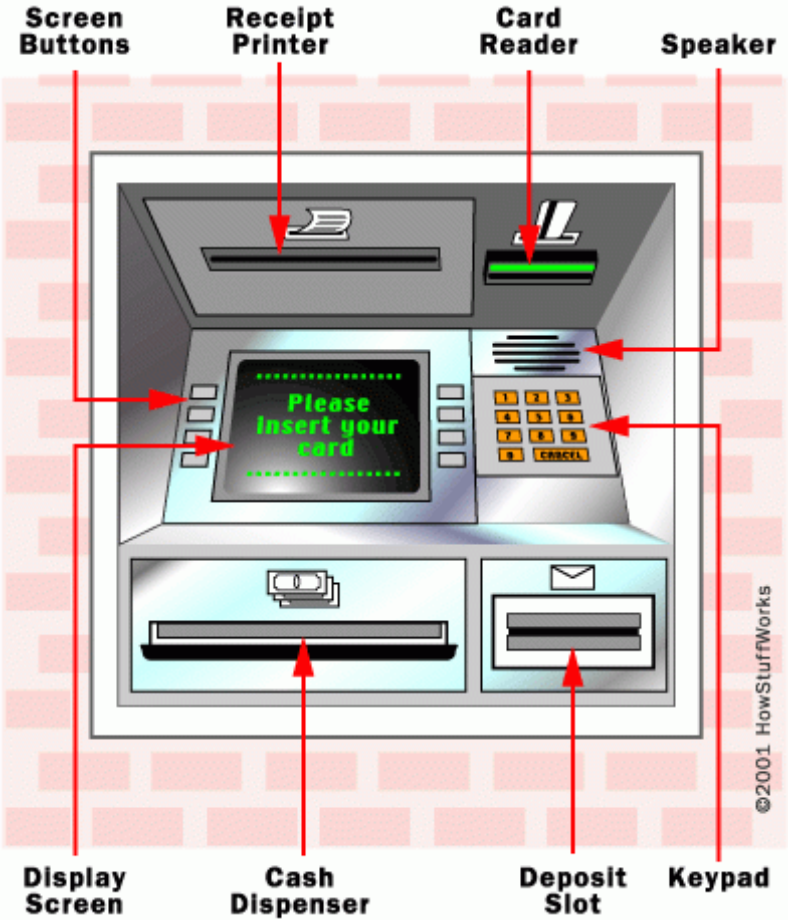
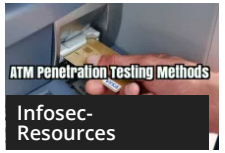


Image Credit : HowstuffWorks

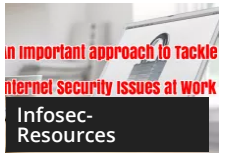
Strengthen your Cyber Security Career

released New Critical Security updates for software...

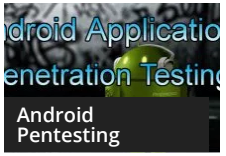


Advanced ATM Penetration Testing Methods

All that You Should Know About Bitcoins and How Does Bitcoin...



An Important Protection Approach to Tackle Internet Security Issues at Work



Android Application Penetration Testing – Part 1

Android Application Penetration Testing – Part 8

Android Application Penetration Testing – Part 9

A rented line ATM machine has a 4-wire, indicate point committed phone line which assists in associating it with the host processor. These sorts of machines are favored in spots where the client volume is high. They are viewed as top of the line and the working expenses of this sort of a machine is high.

The dial-up ATM machines just has an ordinary telephone line with a modem and a toll free number. As these are typical associations their underlying establishment cost is less and their working costs just turn into a small amount of that of a rented line ATM.

The host is primarily claimed by the bank. It can likewise be claimed by an ISP. On the off chance that the host is

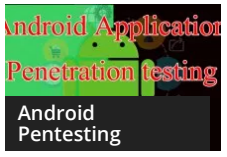
Android Application Penetration Testing – Part 10

Android Application Penetration Testing – Part 11 – Android Checklist

Android Application Penetration Testing – Part 12

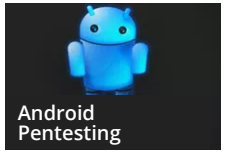
Android Application Penetration Testing – Part 5

Android Application Penetration Testing Part – 4



Android Application Penetration Testing Part 2

Android Application

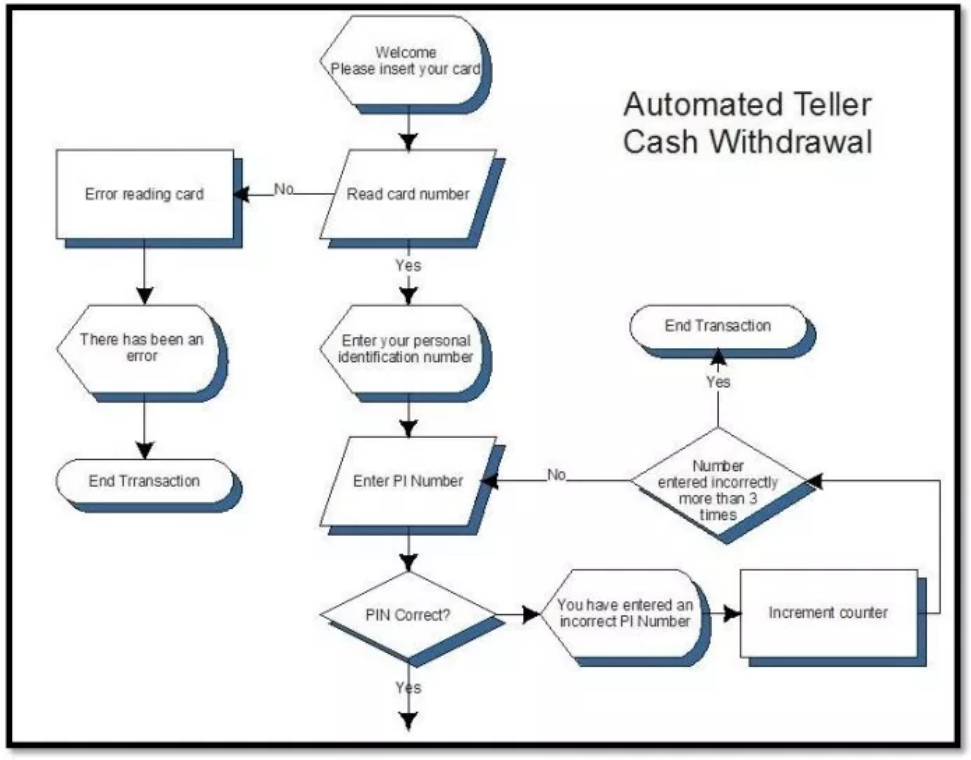


Android Application

possessed by the bank just machines that work for that specific bank will be upheld.

Aso Read **Undetectable ATM "Shimmers" Hacker's Latest Tool for Steal your Chip Based Card Details**

So what happens when a client embed his card to pull back the money?



Penetration testing Part 3

Penetration Testing Part 6

Android Application Penetration Testing- Part 7

APT Group Cyber Attack to Hack Various Companies Web Servers Using...

1.Client’s record data is put away on the attractive portion of the card which is situated posterior of the card. The client embeds the card in card peruser.

The card peruser peruses the data from the attractive portion of the card. The information from this card is sent to the host processor which advances the data to client’s bank.

2.After the card is perceived, the client is requested that give the stick. The client enters the stick utilizing the keypad. The stick is encoded and sent to the host server. The record and stick are approved by the client’s bank. Once approved by the bank, the host server sends the reaction code to the ATM machine.

3.The client enters the add up to pull back. The ask for goes to the host processor. The host server sends the exchange demand to the client’s bank which approves the sum, pull back cutoff, and so forth. At that point subsidize exchange happens between client’s bank and host processor’s record. Once the exchange is done, the host processor sends the endorsement code to the ATM which permits the ATM machine to administer the money.

4.The application running on the ATM teaches the money container to administer the money. The money container has a component which considers every charge it leaves the allocator. This information identified with the exchange like record number, exchange id, time, sum, charge group, and so forth is logged to the log document. This log record is normally known as EJ log.

5. Amid the administering procedure, a sensor sweeps every bill for its thickness. This is to check if two bills are stuck together or if any bill is torn or collapsed. In the event that two bills are stuck together, then they are occupied to the reject receptacle.

Also Read **A Fileless Malware Called "ATMitch" Attack The ATM machines Remotely and Delete The Attack Evidence**

ATM BPT style penetration testing

Security professionals perform **advanced penetration tests** on automated teller machine (ATM) solutions in the financial sector. In most cases, serious security flaws are identified in the ATM configurations and associated processes.

ATMs test with our '**Business Penetration Test' (BPT) methodology**, which simulates real attacks on ATM solutions. This includes carefully designed targeted attacks, which combines physical, logical and optionally social engineering attack vectors.

ATM security is often considered a complex area by IT security managers, who tend to focus more on the physical risks and less on the logical weaknesses in the operating system and application layer.

Meanwhile, ATM security is a business area that often lacks holistic security assessments. Our ATM tests are based on this belief, and seek to paint a holistic) picture of your ATM environment.

Physical controls

Many banks rely heavily on the assumption that physical access to their ATM solutions is effectively restricted. In the meantime repeated, illustrates how little effort is often required to gain unauthorized access to the ATM CPU, which controls the user interface and transaction device.

Logical controls

With physical access to the ATM CPU, authentication mechanisms can be bypassed to gain unauthorized access to the ATM platform.

With this access, an attacker may be able to steal credit card data that is stored in file systems or memory, without ever alerting the bank. Furthermore, experts able to demonstrate, this unauthorized access can be expanded from the ATM to the bank’s network and back-end servers by using the compromised ATM as an attack platform.

ATM solution management processes associated with third party service providers and application development vendors are often the golden key for an attacker, and can be included in the scope of our test to identify logical weaknesses in trust relationships that an attacker can exploit to compromise an ATM.

ATM ecosystem

An ATM solution and network form a complex ecosystem that consists of different vendors and responsible agents, both internal and external to the banking organization.

Due to the complexity of this ecosystem with its distributed roles and responsibilities that cross organizational

boundaries, the areas associated with security risk are often overlooked. The ATM application itself, with its software updates, operating system patches, platform hardening, and networks, is often vulnerable to attacks.

These attacks are not necessarily sophisticated and often not included in standard penetration tests.

PCI DSS

The ATM environment is also part of the PCI DSS scope. However, only a part of the real life hacking attacks is entirely covered by PCI DSS and PA-DSS. The PCI SSC released the “ATM Security guideline” information supplement document in January 2013.

ATM Penetration testing

In ATM Penetration testing , As the number of ATM units increase, the machine is prone to hack attacks, robberies, fraud, etc. Most of ATMs are still using Windows XP which make this ATM an easy target for the hackers.

Electronic fund transfer has three components which are communication link, computer, and terminal (ATM). All

three of the components must be secured to avoid the attack. We will look into the type of assessment we can perform to analyze the overall security of an ATM.

1. Vulnerability Assessment and Network Penetration Testing

VAPT are two types of vulnerability testing. The tests have different strengths and are often combined to achieve a complete vulnerability analysis. In short, Penetration Testing and Vulnerability Assessments perform two different tasks, usually with different results, within the same area of focus.

Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to cause damage and those that cannot. Vulnerability scanners alert companies to the pre-existing flaws in their code and where they are located.

These two activities are very common when dealing with ATM security. In network penetration testing we check for network level vulnerability in an ATM. Since ATM communicates with the back-end server, it has to be part of

some network. By obtaining the IP address of the ATM, we can perform a network level penetration test.

As a security best practice, ATM network is segregated with another network of the bank. So the tester has to be part of the ATM network to reach the ATM IP and perform testing. Once in the ATM network, we can perform a Nessus scan to identify the open port, services running on them and vulnerabilities associated with the running services.

We can run full port NMAP scan to identify the TCP and UDP ports and services running on the ATM. Additionally, Nessus authenticated scan can be used to identify vulnerability associated with the installed components in the ATM OS like Adobe, Internet Explorer, etc.

The configuration audit deals with the hardening of the operating system. Most of the ATM runs the Windows OS. This OS must be hardened as per security best practices to reduce the attack surface for the attacker. Some of the areas we can look into while doing configuration audit are:

- **System access and authentication:** Checks related to password and account lockout policy, User right policy, etc.
- **Auditing and logging:** Checks related to the event, application and security logs, audit policy, permission on

event logs.

- **Account configuration:** Checks related to users under administrator group, the presence of default users, guest account, password requirement, and expiration.

2. Application Security Audit:

An application security audit is an intensive, technical, unprivileged and privileged security test of an application and its associated components with a high percentage of manual testing and verification. Since unprivileged and privileged tests will be carried out, both the perspective of an outsider (e.g. hacker) and an insider are covered.

We can divide this activity into two categories:

a. Thick client application penetration testing:
Majority of the ATM application are a thick client. We can perform an application penetration testing of this thick client application. Some of the test cases we can perform is:

- Sensitive information in application configuration files, credentials in the registry, sensitive information, hardcoded in code.

- Intercept the traffic going to the server and try to manipulate/ tamper with the parameters or look for any sensitive information passing between application and server.
- Check if application and database are communication in cleartext protocol.
- Protection from Reverse Engineering.

b. Application Design Review: In this activity, we can check for security practices being followed in the application. Some of the test cases can be:

- Types of event logged to the log file.
- The privilege with which ATM application is running.
- Does the software have provision to restrict different menu options to different user-IDs based on user level?
- Access the application related folders.
- Does the application allow the transaction without a pin or with an old pin?
- Does the application allow the access to OS while running?
- Communication with back-end components.
- Check for effective network isolation.
- Logging out of a customer in case of even a single invalid pin?
- PIN entry for each and every transaction is Mandatory?

Assessment of ATM Security Solution installed in the ATM:

What is ATM security solution?

Most of the ATMs run on Windows XP and 7. Patching individual ATM is a quite complex process. Since Windows XP is no longer supported by Microsoft, many ATM vendor uses security solution to mitigate the threats related to ATM attacks such as Malware-based attacks, OS-level vulnerabilities. These security solutions allow the ATM application to run in very restrictive environment with limited services and processes in the back end. Two of such security solutions are Mcafee Solidcore and Phoenix Vista ATM.

Mcafee Solidcore:

McAfee Application Control blocks unauthorized executables on servers, corporate desktops, and fixed-function devices. Using a dynamic trust model and innovative security features such as local and global reputation intelligence, real-time behavioral analytics, and auto-immunization of endpoints, it immediately thwarts advanced persistent

threats—without requiring labor-intensive list management or signature updates.

- Complete protection from unwanted applications with coverage of executable files, libraries, drivers, Java apps, ActiveX controls, scripts, and specialty code.
- Flexibility for desktop users and server admins with self-approval and auto-approval based on application rating.
- Viable security for fixed-function, legacy, and modern systems.
- Patch cycle reduction and advanced memory protection.
- Centralized, integrated management via McAfee ePolicy Orchestrator.

Phoenix Vista ATM:

Phoenix Vista ATM is a product of Phoenix Interactive Design Inc .This solution integrates with the ATM application itself. This application works on file integrity check where any modification/tampering with the application related critical file will result in a system shutdown. This disallows any unauthorized program to modify the application specific file.

XFS (eXtensions for Financial Services) provides a client-server architecture for financial applications on the

Microsoft Windows platform, especially peripheral devices such as ATMs which are unique to the financial industry. It is an international standard promoted by the European Committee for Standardization (known by the acronym CEN, hence CEN/XFS). XFS provides a common API for accessing and manipulating various financial services devices regardless of the manufacturer.

Vista ATM communicates with the XFS layer which gives commands to the hardware like cash dispenser of the ATM to dispense the cash. Any unauthorized modification in XFS files will trigger the Vista ATM application to restart the machine forcefully. The machine restarts 4-5 times, and after that, it goes into maintenance mode which does not allow the user to perform any transaction.

Pentesting Security Solutions: PCI Standards

The approach for testing security solution in ATM remains the same. The end objective is to gain access to OS or to fiddle with the application related file to see how does the application behave. An attacker after gaining access to OS

can create a malware which can issue the command to system hardware using XFS components.

Some of the test cases that can be considered are:

Test cases related to access the OS and related file:

1. Check if USB is enabled, make your USB bootable.
2. Plug-in the USB and boot the system through USB.
3. Since most of the security solution take over the OS as soon as it boots, keep on pressing the “Shift” button at boot time. This will break any sequence configured to run at boot in OS. This will result in Windows login screen.
4. If you are aware of valid username, then enter that and press the “Enter” button. This will result in direct access to the OS without a password.
5. If you are not aware of valid username, try login with “Administrator” as many ATM does not disable the default administrator account.
6. Another way is to make your USB bootable. Boot from USB, this will give access to file system directly without any Windows login.

1. **Test related to runtime code authorization:** Check if USB is enabled, try to run unauthorized code (exe or batch

file) directly from the USB or using autorun feature of the USB.

2. **Test related to code protection:** Check if application related files can be moved to another location, modified or deleted.
3. **Checks related to process modification:** Rename unauthorized file to a valid security solution process. This will result in the execution of unauthorized file when the application starts.
4. **Threats related to unauthorized execution through registry**: Check if any critical registry key can be modified or unauthorized software can be executed by keeping them in the Windows startup folder. Executables under Windows startup folder will execute first when the system restarts.

   Security Best Practices to be followed for ATM

   The banks can implement security best practices to reduce the attack surface for the attacker. This section can be categories into three categories:

5. **Protection against physical attacks:**

- Detection and protection against Card skimming.
- Detection and protection against card/ cash trapping.
- Detection against keypad tampering.

- Mirror and pin shield to identify and prevent shoulder surfing attack.
- Implementing a DVSS camera inbuilt in the ATM to capture facial features of the user along with transaction details and timestamp.
- Vault protection against fire, explosion, etc.
- Lock protection again unauthorized access to banknotes or bills.
- Electric power point and network point protection.
- Disabling unused network and electric port.
- The ATM must be grouted on the floor to secure against threats related to the robbery. ATM can be implemented with shock sensor to identify the impact and movement of ATM machine.
- Implementation of CCTV camera. The presence of security guard.

6 . Protection against logical attacks:

- Protection against unauthorized booting by setting non-guessable boot and BIOS password. Most of ATM have default boot password configured.
- Protection against USB and unauthorized hard disk access.
- OS hardening and latest patch.
- Whitelisting the application, services, and process on ATM.

- Running ATM with least privilege user. Need to know and need to have approach.
- File integrity checks.
- Securing the transaction logs.
- Use of secure channel for the communication and transaction.
- Configure security best practices in ATM application.
- Antivirus protection.
- ATM network segregation with other networks.
- Protection against Malware like tyupkin, ploutus, etc.

7 . Protection against fraud attacks:

- Implementation of geo-blocking. In this implementation, the card can only be used in originating country or region. The user has to take permission to use the card outside the originating country.
- Implementation of chip and pin based card to mitigate copied and skimming card based attack.
- Implementing a behavior mentoring which detects the unusual transaction in term of the amount, place of transaction, frequency of transaction, etc.

For More about ATM skimming attack protection **Click here**

Sources & Credits

https://www.pcisecuritystandards/pdfs/PCI_ATM_Security_Guidelines_Info_Supplement.pdf

http://money.howstuffworks.com/personal-finance/debt-management/credit-card.htm

http://money.howstuffworks.com/personal-finance/banking/atm3.htm

BALAJI N

http://www.gbhackers.com

BALAJI is a Security Researcher (Threat Research Labs) at Comodo Cybersecurity. He is a Certified Ethical Hacker, Editor-in-Chief, Author & Co-Creator of GBHackers On Security

RELATED ARTICLES MORE FROM AUTHOR

Best Way to Accelerate and Secure Your Website From Top Common Web Threats

Secure Cloud Migration Guide – Technical and Business Considerations

Key Elements and Important Steps to General Data Protection Regulation (GDPR)

Most Important Considerations with Malware Analysis Cheats And Tools list

Top 500 Most Important XSS Script Cheat Sheet for Web Application Penetration Testing

Secure File Storage with Virtual Private Server (VPS)- A Detailed Guide

which including Cyber Security Research,Web Application and Network Penetration Testing, Hacking Tutorials,Live Security Updates, Technology updates, Security investigations With dedicated Cyber security Expert Team and help to community more secure.

Contact us: admin@gbhackers.com