

LOGICAL ATTACKS SERIES :

1. Attacks and their mitigations
2. Offline Malware
3. Online Malware
4. Network Attacks
5. Blackbox Attacks

Security Attacks and Vulnerabilities in the news...

ATM Jackpotting Attacks Hit the US

- US Secret Service Alert and press release warning to North America ATM Deployers and Financial Institutions to protect against :-
 - Black Box attacks AND
 - Hard Disk removed from Diebold ATM, Malware (Ploutus-D) Installed, Disk returned to ATM



Spectre/Meltdown Vulnerabilities

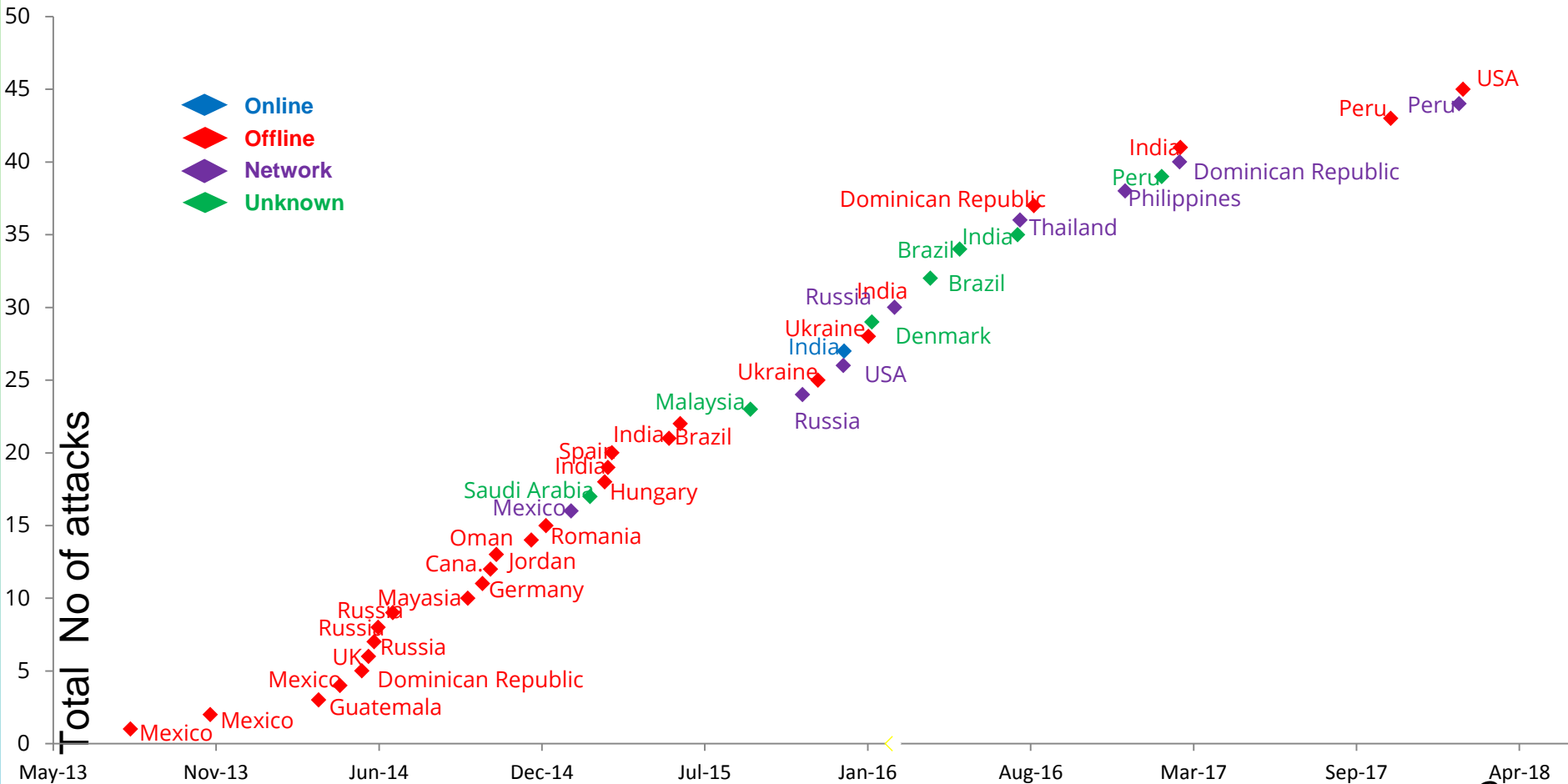
- Vulnerability found in Processor Chips from Intel, ARM, & AMD.
- Speculative Execution Flaw impacts ALL modern processors



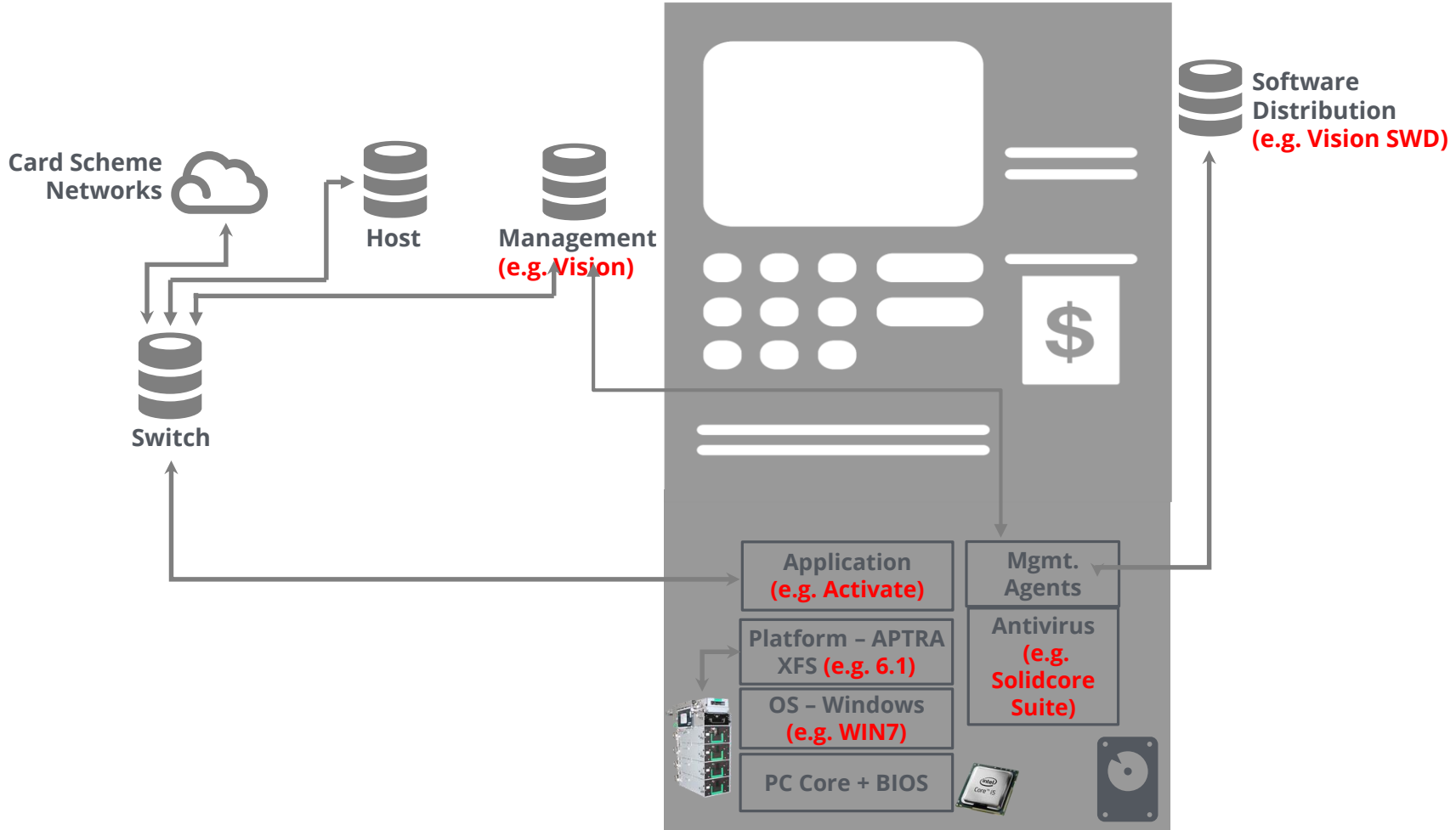
Logical Attacks (other than Black Box) since 2013

- Online
- Offline
- Network
- Unknown

Total No of attacks



High Level Architecture



Malware Installed on the ATM

‘Ploutus/PADPIN/TYUPKIN’ Malware

- Security SW is disabled
- Malware files transferred to ATM
- ATM put back in service
- Dispense commands may be executed via external keyboard or through PINPAD

‘Skimer’ Malware

Reported by Kaspersky – but first seen in 2009 (Russia only)

Backdoor.Win32.Skimer and **Trojan.Win32.Patched.rb**

Uses standard XFS commands to communicate with card reader,
EPP & Dispenser to obtain card and pin data and also to dispense cash

Has been not been reported on NCR ATMs as yet

‘Suceful’ & ‘GreenDispense’ Malware

- Malware discovered on Virus upload sites
- Uses standard XFS commands to communicate with card reader, EPP, and SIU & Dispenser

Compatible with NCR and Diebold ATMs

‘Suceful’ Malware does not appear to be a ‘working’ version. Could be indicative of development in this area

‘Ripper’ Malware

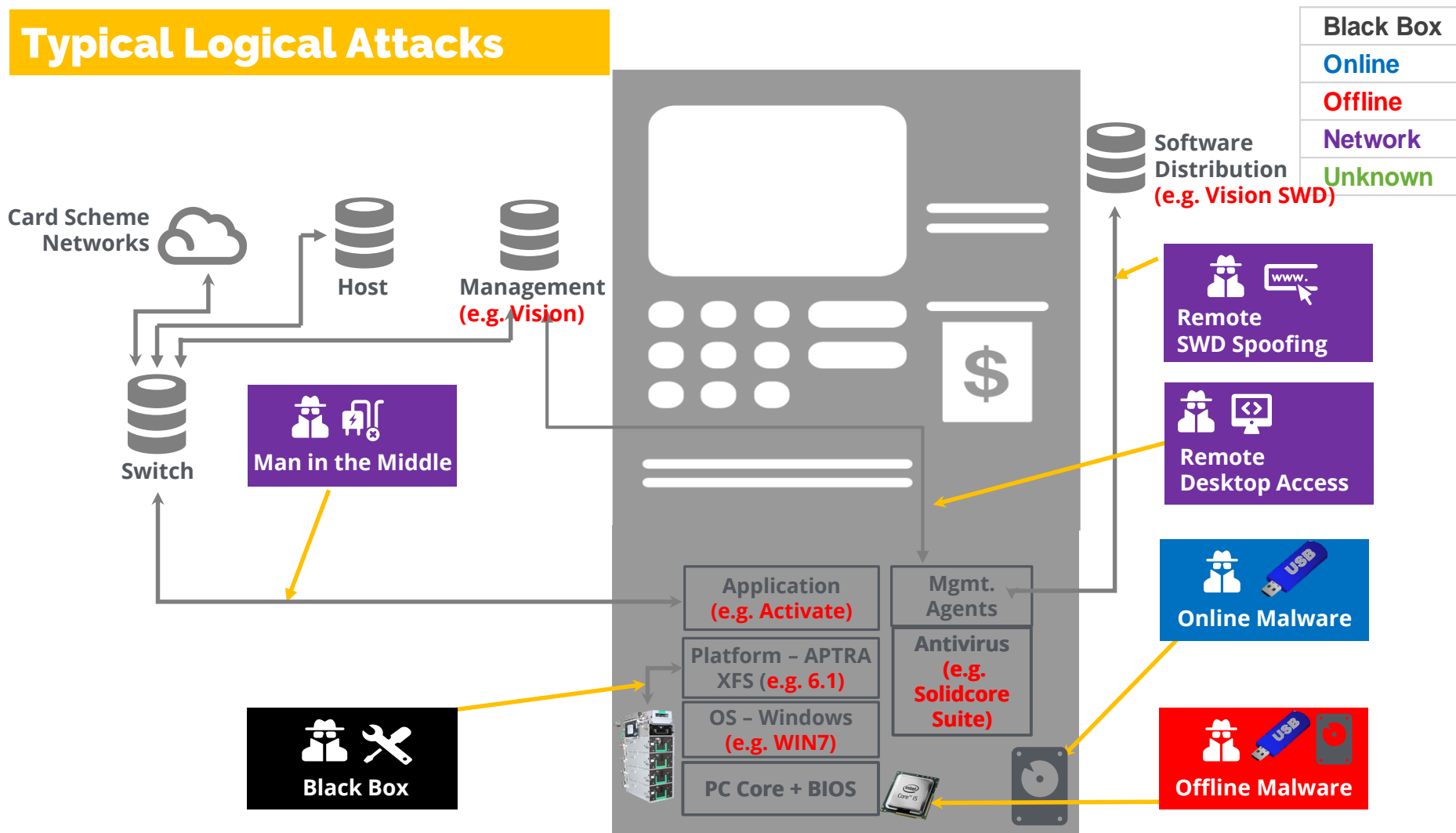
Thailand Malware – Jackpotting.
It reads data from inserted cards, identifying when an accomplice is physically located at the ATM.

Includes a self-destruct feature

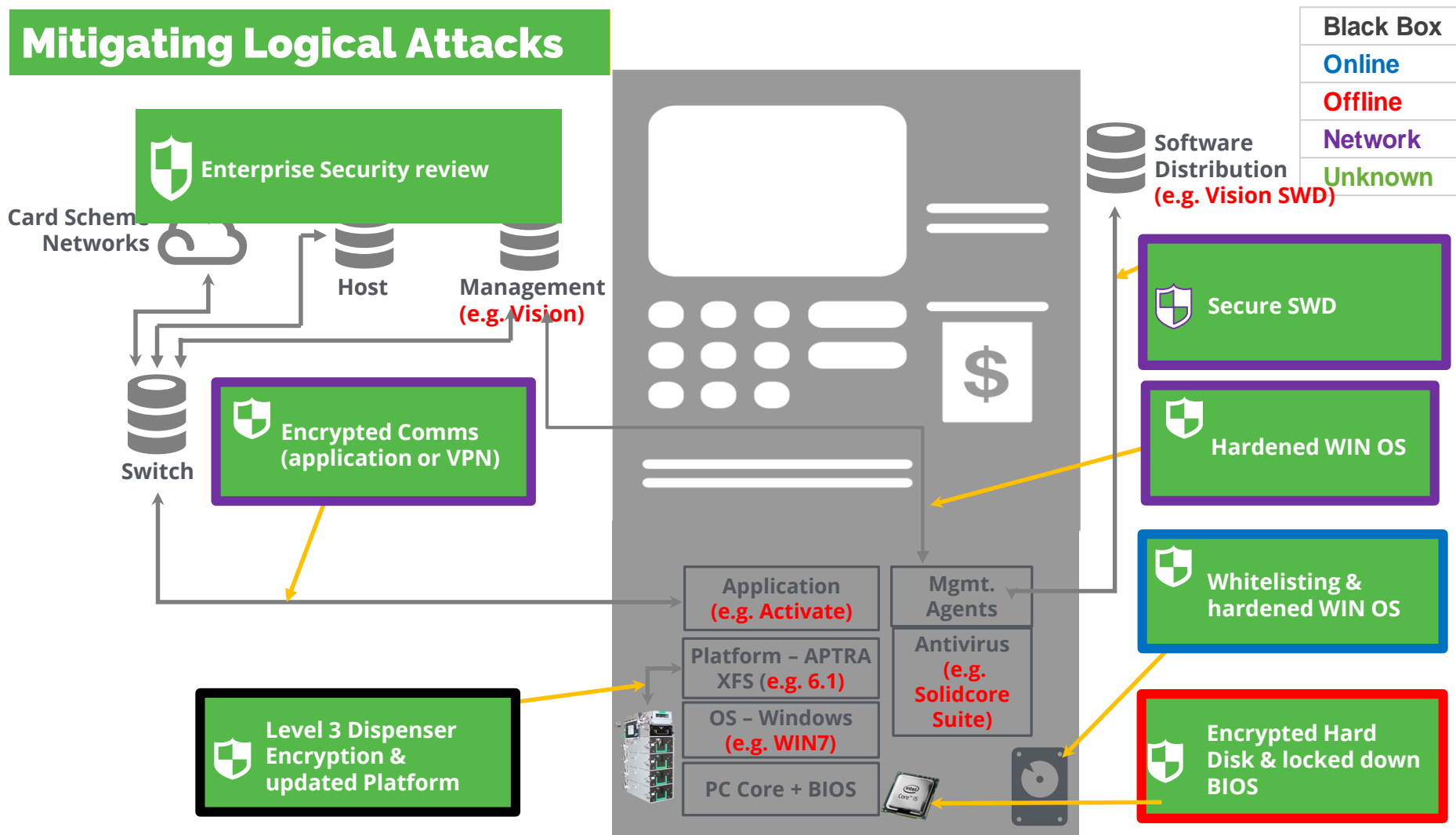
Can disable/enable Network; clean logs;

Capable of recognizing and installing on three of the main ATM Vendors worldwide

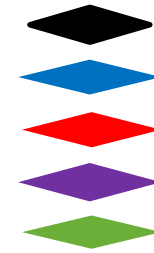
Typical Logical Attacks



Mitigating Logical Attacks



Logical Attacks



Black Box

Online

Offline

Network

Unknown

ATTACK CATEGORIES

When Malware added when ATM Hard Disk is Offline

ATM Hard Disk Offline

When the ATM's hard disk's Operating System (typically Windows) is not running

This is done either by :-

- Removing the ATM Hard Disk and mounting it as a secondary drive attached to a laptop or other device

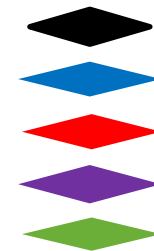
OR

- Inserting bootable removable media (USB/DVD) into the ATM and re-booting the ATM to this media

When the hard disk is Offline attackers can :-

- View and modify the contents/files of the hard disk
- Disable Solidcore or other anti-malware solutions
- Copy malware onto the hard disk
- Copy sensitive information from the hard disk

Logical Attacks



Black Box

Online

Offline

Network

Unknown

MITIGATIONS

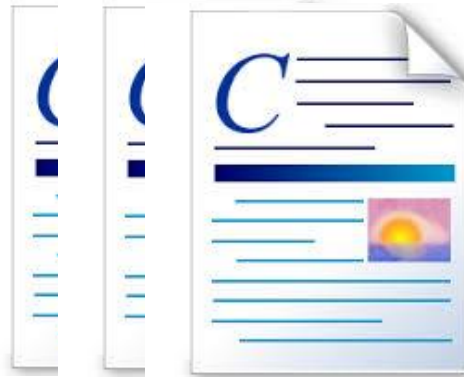
When Malware added when ATM Hard Disk is Offline

Encrypt the hard disk

Protects against
Offline malware
attacks by
preventing
malware being
copied onto the
hard disk when the
hard disk
offline/mounted as
a secondary drive

To read an **encrypted** file, you must have access to a secret (encryption) key or password that enables you to decrypt it. Unencrypted data is called plain text ; **encrypted** data is referred to as cipher text.

Plain text



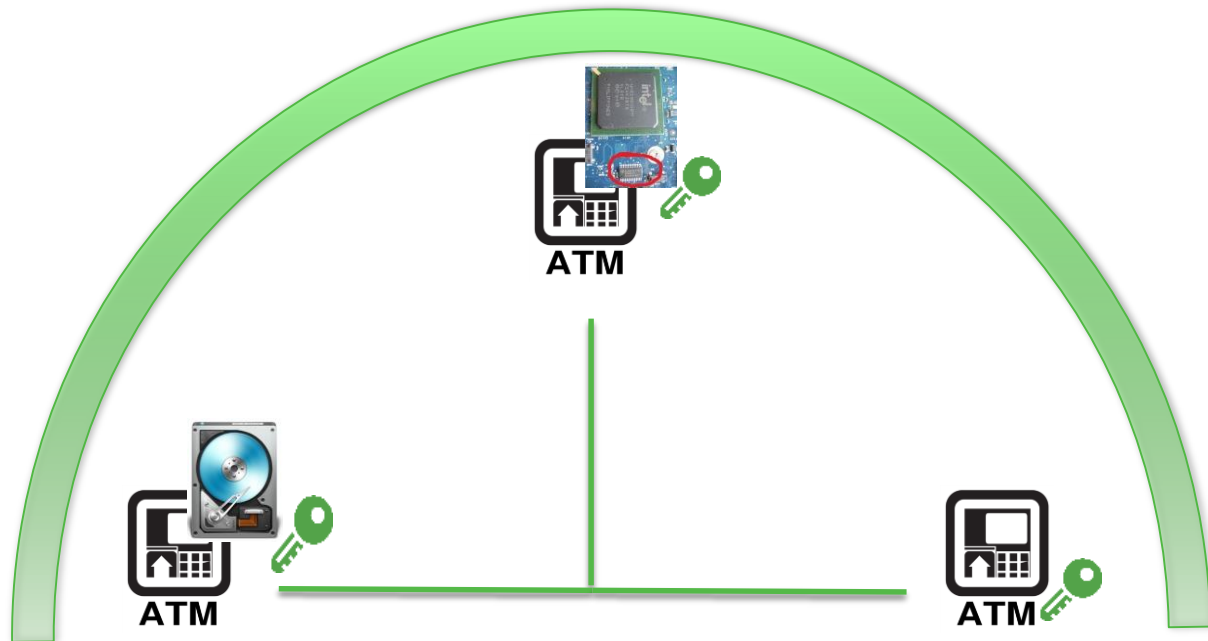
Cipher text



But where can the encryption key be stored securely?

The encryption keys can be locally stored or derived

- The secret key is stored on an unencrypted part of the ATM hard disk
 - Less secure
 - Not PCI compliant



- The secret key is stored in a TPM chip in the core
 - Quite secure but will not protect data if the whole core is stolen
- The algorithm to derive the secret key from the devices attached is stored on an unencrypted part of the ATM hard disk
 - Less secure

NCR Secure Hard Disk Encryption

Protects against offline malware and protects data on stolen hard disks

- ATM software being disabled, modified or tampered with when data is at rest (offline attack)
- Dispenser Encryption Keys being compromised when data is at rest
- Mounting HD as secondary drive
- Reverse engineering stolen HD
- Data on HD being compromised
- Poor disposal of HD

Network Based Authentication

- Keys are held at the server which is much more secure than
 - Keys held locally on hard disk
 - Keys derived from an algorithm which uses attached ATM devices
 - Keys held in the TPM chip

Centralised Control

- Authorised central management of decryption and encryption
 - Allows authorised decryption for support & troubleshooting
 - Encryption status known centrally – encrypting, encrypted, not encrypted
- Centralised policy updates can be pushed to ATM

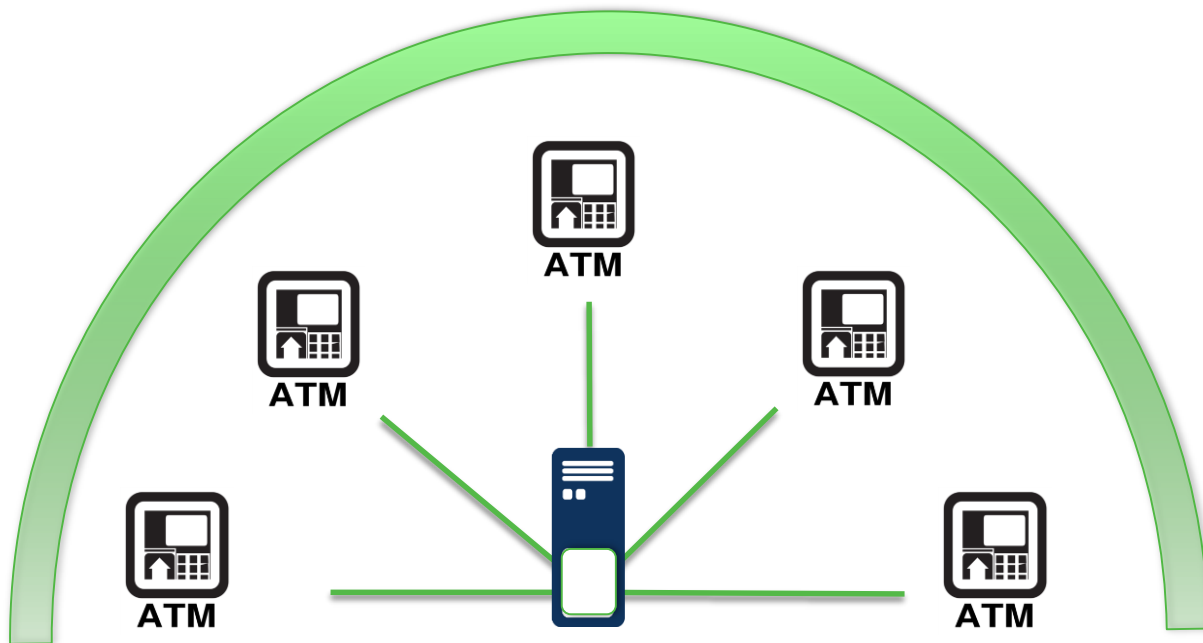
Works on XP, W7 and Windows 10

Is Vendor Independent (ie Multi-vendor)

PCI Compliant

FIPS 140-2 certified

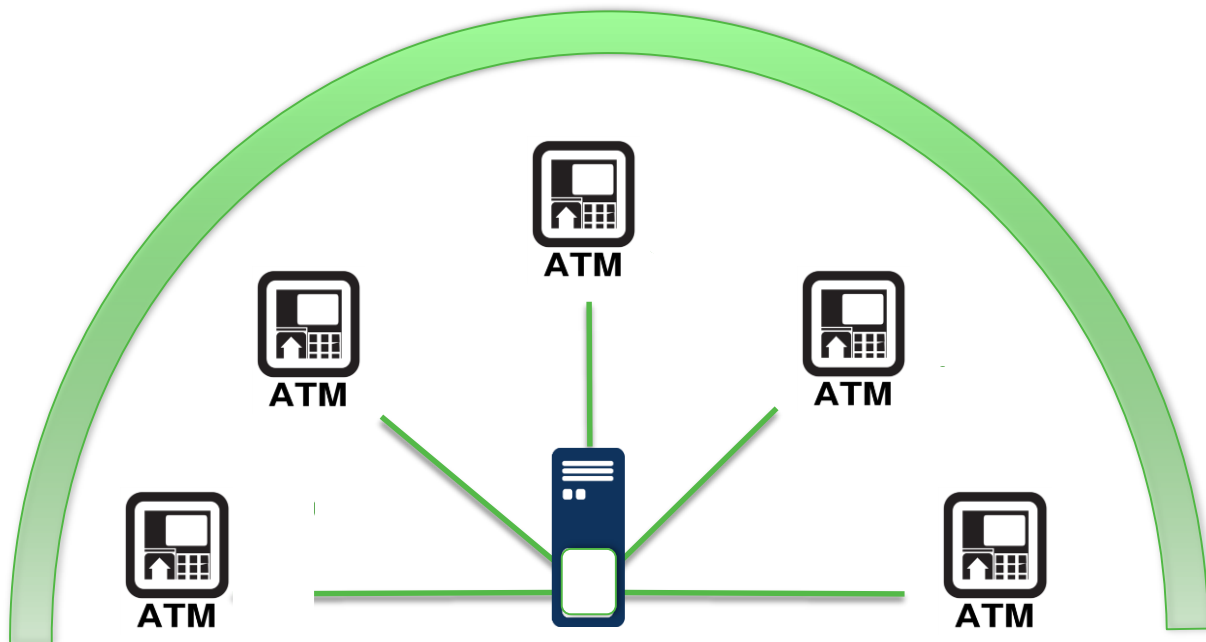
Network based authentication for Encryption keys



- Is PCI compliant
- Has centralised key management, configuration and deployment
- Provides compliance reporting
- Has Audit logs
- Uses Pre boot networking for external authentication and key management

Network based authentication for Encryption keys

The encryption package is sent down to ATMs and encryption process starts

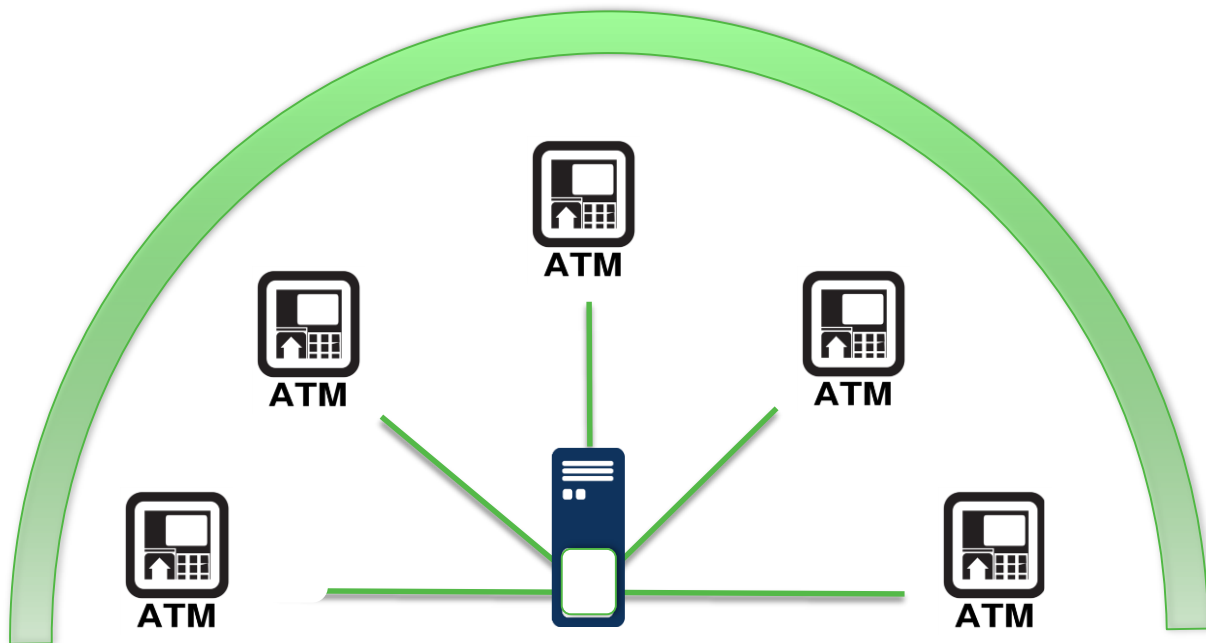


After the initial encryption the keys are then transmitted over the network in an encrypted, secure fashion to the central manager. Where they are then stored

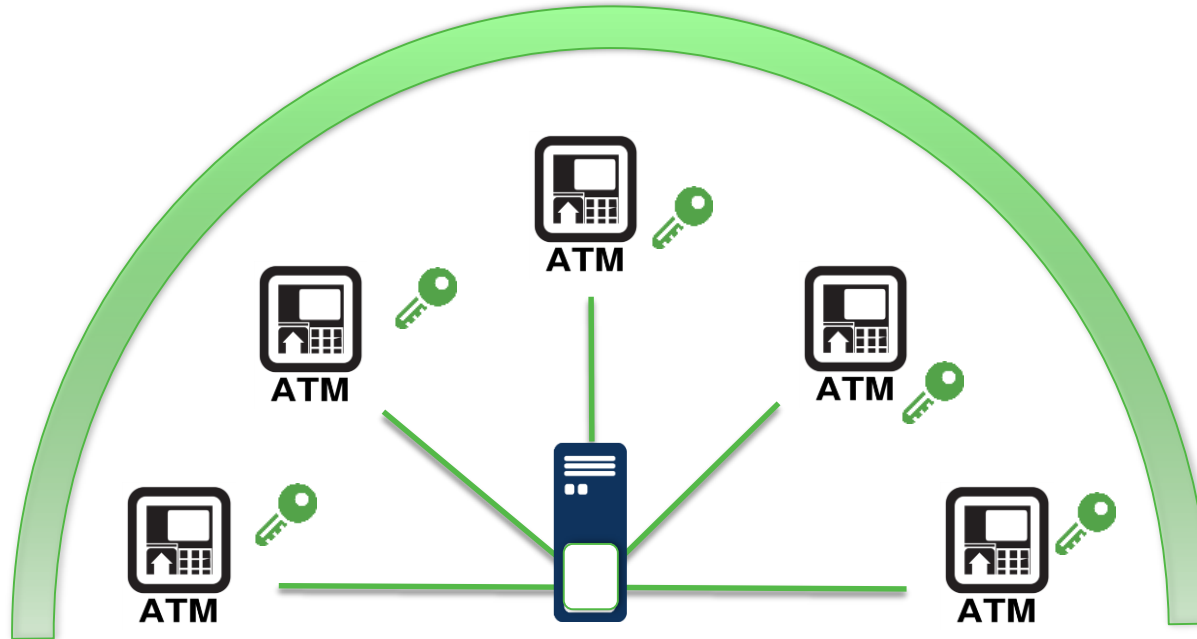
Network based authentication for Encryption keys

When the ATMs start up, they use pre-boot networking to contact the central key manager.

If, and only if, they can contact the central manager AND the ATM is configured to be able to boot then the keys are provided over the network BEFORE the OS boots.



Network based authentication for Encryption keys



If an ATM/Core/Hard Disk is brought offline by an attacker and they attempt to reverse engineer it, the data, OS files and software are all protected for confidentiality and against injection of malware.

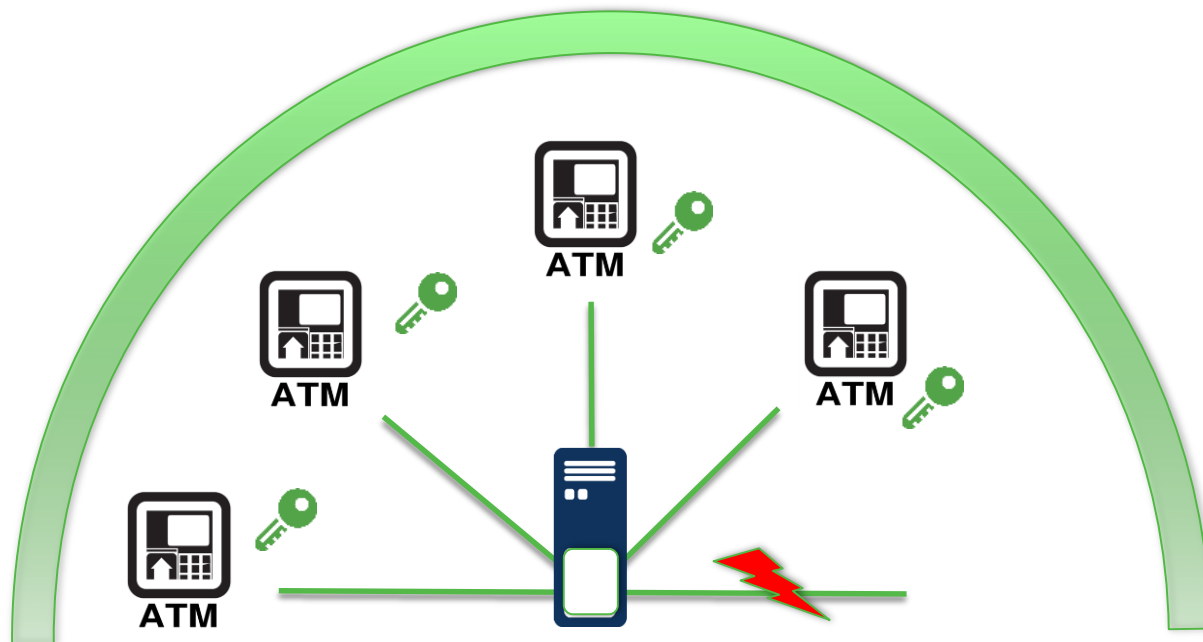
Network based authentication for Encryption keys

If ATM is reported stolen the central key manager administrator :-

- Removes it from the autoboot group
- Can que up a crypto-erase

So if the attacker attempts to put the machine back online :-

- it will be crypto-erased via pre-boot networking and the event will be logged

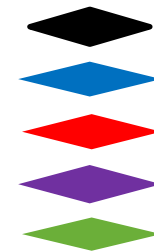


Perceived Barrier – Performance Impact

- **During** encryption (up to 24 hours after installation):
 - SST performance **IS** affected, particularly on start-up and shutdown
 - Transactions may take 8% longer than normal
 - Start-up may take 60% longer than normal
- **After** encryption:
 - Transactions are unaffected
 - There is some **minimal** impact during start-up and shutdown
- Start-up displays a pre-boot screen until keys are obtained via the network
 - A valid network connection to the server is required only for start-up



Logical Attacks



Black Box

Online

Offline

Network

Unknown

MITIGATIONS

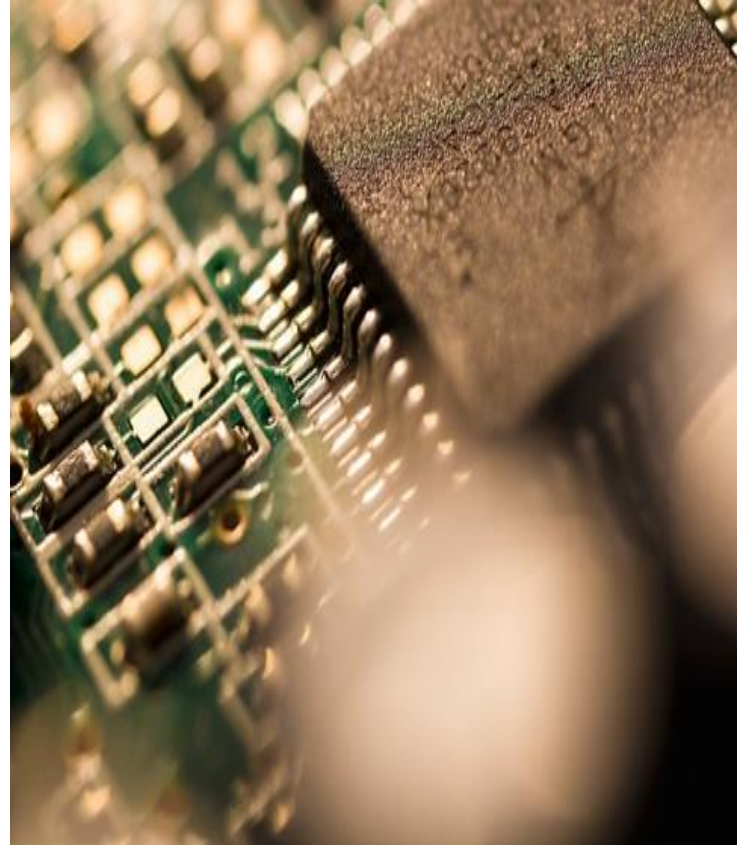
When Malware added when ATM Hard Disk is Offline

Lockdown the BIOS

It is still important to ensure the BIOS is locked down to only allow boot from the primary hard drive and have bios editing password protected.

If the BIOS had been password protected and locked down to prevent boot from removable media then the majority of offline attacks would not have been successful

This lockdown can be done manually
This will help protect against future new attack techniques



NCR Secure Remote BIOS Update

RBU Flash Utility

Flashes the BIOS to :-

- Only allow boot from primary hard drive (Disallow boot from CD/USB)
- Add a default BIOS password to all the ATMs in a Financial Institution's network
- Set up unique UUIDs per ATM
- Update the BIOS when vulnerabilities are found
- Enable no-touch password implementation and maintenance
- Works on NCR only

Must be sent down via Software Distribution

Needs an ATM reboot to take effect.

RBU Update Utilities

RBU Change Password Utility

- Used to change the default password to a new secure password of your choice. No flash. No ATM reboot needed
- Can also be used to update password anytime (daily/weekly/monthly etc)

RBU Change Boot order utility

- Used to update the boot order to USB/CD/DVD to allow for example FEs to use bootable sysapp
- Can then be used to set the boot order back to Hard drive only to lock the BIOS back down/ No flash. No ATM reboot needed.

RBU Check Boot order utility:

- check which device is currently set to boot from

RBU Check Password Set Utility:

- check there is a password set

Security Vulnerabilities in the news...

Spectre/Meltdown Vulnerabilities

- Vulnerability found in Processor Chips from Intel, ARM, & AMD.
- Speculative Execution Flaw impacts ALL modern processors

Intel expands bug bounty program to include Spectre-like side ...

<https://www.geekwire.com> > Cloud Tech ▼

Feb 14, 2018 - In response, **Intel** is changing its **bug bounty** program from invitation-only to a public program, and offering up to \$250,000 for researchers who report new side-channel vulnerabilities to the chip giant, it said in a blog post Wednesday. The company will also increase the amount it awards for the discovery ...

Google's bug bounty programs paid out almost \$3M in 2017 ...

<https://techcrunch.com/.../googles-bug-bounty-programs-paid-out-almost-3m-in-2017...> ▼

Feb 7, 2018 - **Bug bounty** programs are designed to sic security researchers on software and pay them to find vulnerabilities and report back to the sponsor. In return, the researchers are richly rewarded for their findings. In fact, **Google's bug bounty** paid out a hefty \$2.9 million in **bug bounties** in 2017. Rewards can range ...



Security Requirements to Protect against Logical Attacks Summary

1. Secure your BIOS
 - Only allow boot from the primary hard disk
 - Editing of BIOS settings must be password protected
2. Establish an adequate operational password policy for all passwords
3. Implement communications encryption
 - e.g. NCR Secure TLS Encrypted Communications
4. Establish a secure firewall
 - The ATM firewall must be configured to only allow known authorized incoming and outgoing connections necessary for an ATM environment, the connections must be configured per program rather than per port
5. Remove unused services and applications
 - Removing these from the system help reduce the attack surface area
6. Deploy an effective anti-malware mechanism
 - NCR Recommends active whitelisting applications: e.g. Solidcore Suite for APTRA
7. Establish a regular patching process for ALL software installed
8. Harden the Operating System e.g.
 - Ensure the application runs in a locked down account with minimum privileges required
 - Disable Auto play
9. Implement Rule based access control e.g.
 - Define different accounts for different user privileges
 - Restrict functionality allowed via remote desktop access to ATMs
10. Deploy a network authentication based Hard Disk Encryption Solution
 - NCR Secure Hard Disk Encryption
11. Ensure there is protected communications to the dispenser of the ATM
12. Perform a Penetration Test of your ATM production environment annually
13. Use a secure Remote Software Distribution that will assist in maintaining the Confidentiality; Integrity and Availability of your ATMs
 - Required to meet rule 7 and allows for timely distribution of updated malware signature files if malware is found
14. Consider the physical environment of ATM deployment
 - e.g. Through the Wall ATMs may be more suitable for unattended environments
15. Consult a security enterprise specialist to deploy industry best-practice security controls within your enterprise

COMMITTED TO SECURING YOUR BUSINESS

Let us keep you informed



NCR Security Alerts

As part of our commitment to security, we regularly provide alerts and updates to the market on global ATM security issues and situations.

We issue alerts when:

- We receive reports of new attacks
- We receive reports of modifications to attack methods
- Industry compliance issues require actions by ATM deployers

Keep yourself fully informed by signing up today.

response.ncr.com/security-alerts

Sign up today for important alerts

First Name*

Last Name*

Email Address*

Company*

Title*

Job Role*

Country*

Questions?

