DEFENDING AGAINST POS RAM SCRAPERS

Current and Next-Generation Technologies

Numaan Huq
Forward-Looking Threat Research Team

CONTENTS

INTRODUCTION

In light of ongoing data breaches involving the compromise of point-of-sale (PoS) systems, everyone is asking two questions—"How do we better protect PoS systems from attacks?" and "What new technologies are being introduced to better protect them?"

Stealing payment card data has become an everyday crime that yields quick monetary gains. Attackers aim to steal data stored in the magnetic stripe of payment cards, optionally clone the cards, and run charges on the accounts associated with them. In the past, attackers physically skimmed payment cards. [1] Today, they have resorted to using malicious software to steal payment card data, primarily from credit cards. They found low-hanging fruits for grabs within the layered payment card security framework—unencrypted credit card data. They prey on vulnerable systems and networks to get inside their targets' networks. They even compromise the networks of third-party vendors who have access to better secured partner networks.

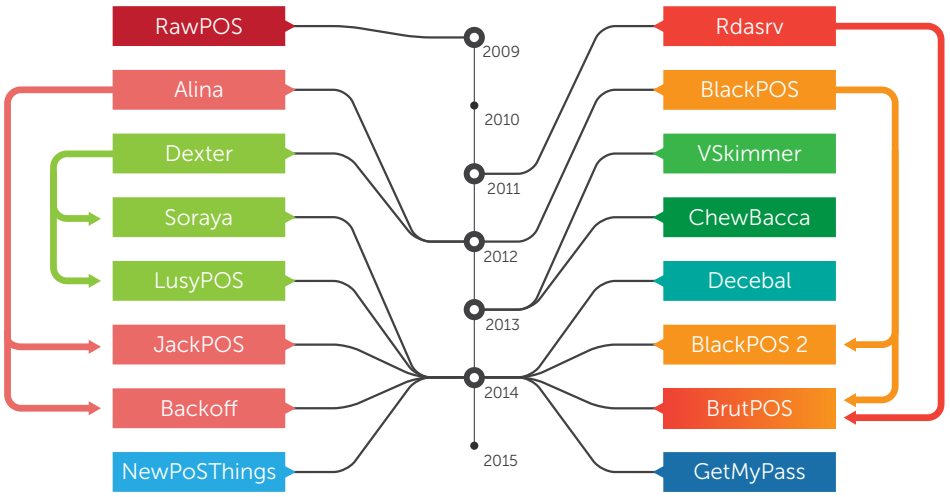
This research paper discusses how PoS RAM scrapers infect systems and exfiltrate stolen data; provides a list of defense technologies and strategies against the threat, along with recommendations for small businesses and medium and large enterprises; and new technologies that PoS system vendors and credit card brands are introducing to protect businesses and consumers.

WHAT WE KNOW ABOUT POS RAM SCRAPERS SO FAR

PoS RAM scrapers retrieve a list of running processes on infected systems, loads-inspects each process's memory space in the RAM, and searches for credit card data. Information on the credit card data format is publicly available in ISO/IEC 7813. [2] They scrape credit card data from infected systems' RAM, which is then exfiltrated. Stolen Tracks 1 and 2 data can be used to physically clone credit cards or commit fraudulent "card-not-present" transactions such as online purchases.

The earliest evidence of PoS RAM scraping was reported in a Visa Data Security Alert issued on 2 October 2008. [3] Back then, cybercriminals attempted to install debugging tools on PoS systems to dump Tracks 1 and 2 credit card data from the RAM. PoS RAM scrapers have quickly evolved since then. They now use multiple components and exfiltration techniques; single binaries; network, bot, and kill-switch functionality; encryption; and development kits.

To get a better perspective of the PoS RAM scraper evolution, we organized all known PoS malware families by year of discovery in a timeline. Note that a variant may have existed long before it was discovered because tracking exact dates is extremely difficult.



PoS RAM scraper families from 2009 to 2014

As shown, seven unique PoS RAM scraper families were discovered between 2009 and 2013 while nine were discovered in 2014 alone. Connecting arrows indicate either direct evolution or technology reuse. The majority of new PoS RAM scrapers discovered from 2013 to 2014 were part of the three "foundation families"—BlackPOS, Alina, and Dexter.

More information on Rdasrv, BlackPOS, Alina, Dexter, VSkimmer, JackPOS, Decebal, Soraya, BrutPOS, and Backoff is available in "PoS RAM Scrapers: Past, Present, and Future." [4] Those that were not discussed in the said paper are briefly described below:

- **RawPOS:** This was probably the first PoS RAM scraper found in the wild dating back to 2008 or 2009. RawPOS targets processes of known PoS software. [5] It was reported to have been used in the Goodwill breach in July 2014. [6]
- **BlackPOS ver. 2:** This was reported to be the variant responsible for the Home Depot compromise. [7] It is a clone of the original BlackPOS variant that compromised Target. [8] BlackPOS ver. 2 pretends to be a component of a commercial antimalware program.

- **NewPoSThings:** In addition to scraping RAM for credit card data, this malware also attempts to steal Virtual Network Computing (VNC) passwords from infected systems. Recent attacks saw the use of VNC to access compromised payment kiosks in parking facilities and train stations even though NewPoSThings was not implicated. [9]
- **GetMyPass:** This was discovered during the 2014 holiday shopping season. [10] It reads instructions from a configuration file, which allows cybercriminals to specify processes to target for scanning.
- **LusyPOS:** This is an evolution of Dexter that exfiltrates stolen data via the Tor network. [11] LusyPOS was reportedly being sold in underground markets for US$2,000. [12]

HOW POS RAM SCRAPERS WORK

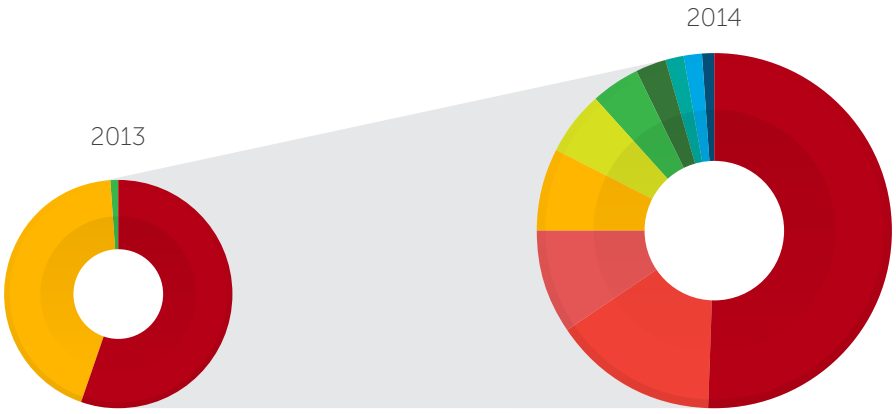
The key to setting up a strong defense against PoS RAM scrapers is to understand their nature. This means understanding the PoS malware attack chain.

Points of Entry

Any company that processes credit cards, irrespective of size, is a potential data theft target. The most convenient place to steal credit card data is from the RAM of PoS systems where information temporarily resides in plain-text format during transaction processing. The only challenge that remains for cybercriminals is to find a reliable method to infect PoS systems.

Some of the common infection methods include:

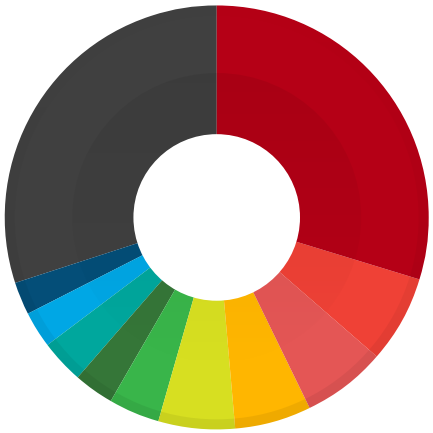
- **Inside jobs:** These are the most difficult to protect against, as they involve people that businesses trust or who can abuse certain privileges to commit crime. [13] Inside jobs can be performed by disgruntled or disillusioned employees out to take revenge on their employers or unscrupulous individuals out to make a quick buck at their employers' expense.
- **Phishing and social engineering:** PoS RAM scrapers are never spammed out to millions of potential victims. They are instead sent out to a chosen few via phishing emails with effective social engineering lures. Small businesses often use their PoS servers to browse the Internet and check email, which makes them easy phishing targets.
- **Vulnerability exploitation:** New software vulnerabilities are disclosed and patched each month by their respective vendors.



Alina	55.39%
Rdasrv	43.63%
VSkimmer	0.98%

The number of PoS RAM scraper families we are detecting has increased from three in 2013 to 10 in 2014. [14]

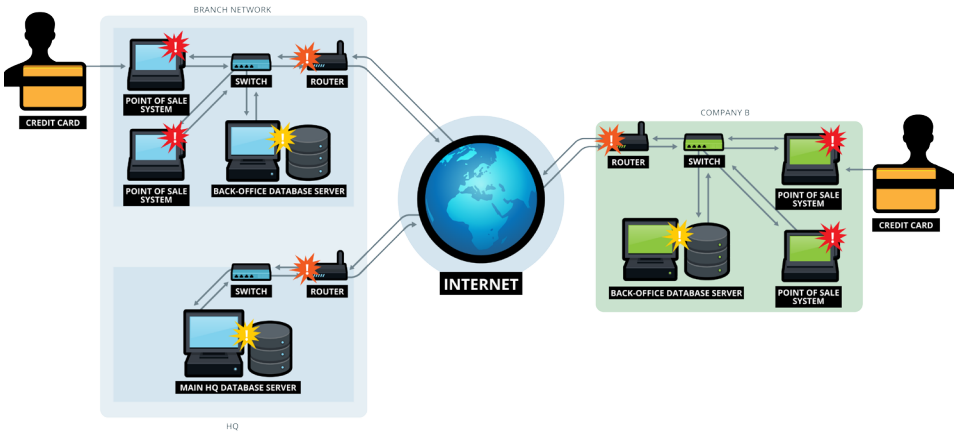
BlackPOS	50.73%
Soraya	14.88%
Alina	9.64%
Rdasrv	7.34%
JackPOS	5.87%
VSkimmer	4.40%
Backoff	2.94%
BrutPOS	1.68%
ChewBacca	1.47%
Decebal	1.05%



United States	29.77%
Canada	6.71%
United Kingdom	6.50%
Australia	5.87%
Philippines	5.66%
Taiwan	3.98%
France	3.14%
Italy	3.14%
Brazil	2.94%
Japan	2.31%
Others	29.98%

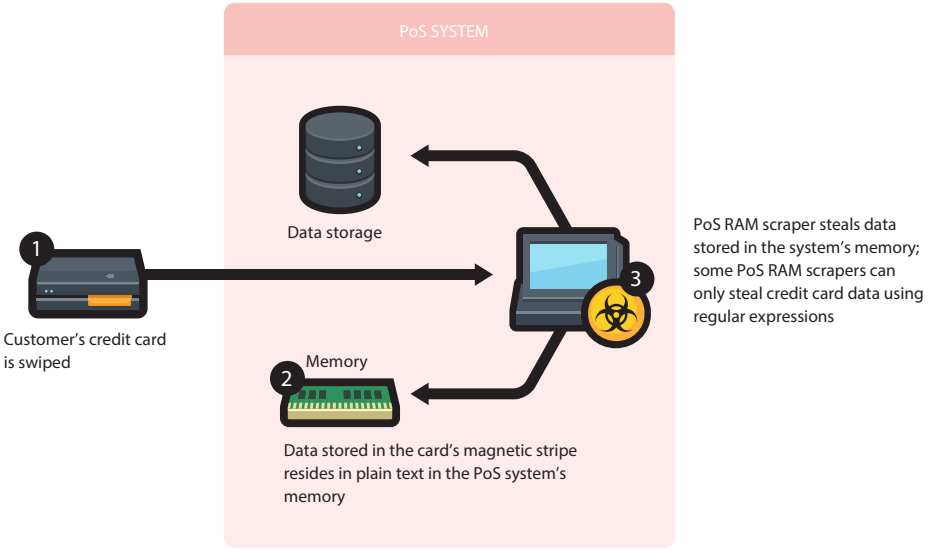
PoS RAM scraper infections by country

Only a handful of them are successfully "weaponized" for use in cyber attacks that are used over and over for years. Examples of these are CVE-2008-4841, CVE-2010-3333, and CVE-2012-0158. Exploits successfully compromise systems because patches for vulnerabilities have not been routinely applied. And many PoS servers still run OSs that are no longer supported by their respective vendors.



How PoS RAM scrapers obtain data from infected devices

- **Security standard noncompliance:** Payment Card Industry Data Security Standard (PCI DSS) refers to a set of requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. [15] It does not offer new secure technologies to protect electronic payment systems but provides requirements to build up additional layers of security controls around existing ones. Hardening systems and networks is not a trivial task. Companies that lack expertise or resources often incorrectly configure their PoS environments, which makes them susceptible to different malware attacks and compromise.



PoS system RAM—the best place to steal payment data from

- **Cyber attacks:** PoS RAM scraper attacks against large enterprises that yield millions of users' credit card credentials are considered targeted. A targeted attack can be broken down into five stages—victim reconnaissance, phishing and social engineering attacks, lateral movement, data collection, and data exfiltration. Targeted attacks are meticulously planned and well-executed, which make them difficult to detect.

Lateral Movement

Lateral movement involves activities related to reconnaissance, credential theft, and infiltrating other systems. [16] Attackers compromise systems inside organizational networks. Compromised systems are then used as beachheads in attempts to gain access to and spread across other networked systems. Lateral movement also uses the victims' own resources against them—the attackers use legitimate Windows® features and tools used by IT administrators to move around networks. It occurs at human speed and takes time to succeed. Stealth is an important factor in lateral movement. The goal is to remain undetected and deeply penetrate target networks.

The lateral movement techniques include:

- Identify the host-naming conventions that aid in network discovery
- Perform host discovery to figure out the network hierarchy
- Scan for vulnerable services, applications, and servers to compromise
- Scan for open ports used for tunneling to command-and-control (C&C) servers and bypass firewalls
- Dump password hashes from the Windows registry using different tools

The attackers' goals include:

- To perform "pass-the-hash" attacks and gain access to remote systems
- To spoof Address Resolution Protocol (ARP) addresses in order to perform denial-of-service (DoS), man-in-the-middle (MitM), and session-hijacking attacks
- To exploit vulnerable services and applications in order to gain access to remote systems
- To exploit and gain access to unpatched network-connected servers
- To spread the malware to network-connected systems and devices
- To compromise and use System Center Configuration Manager (SCCM) servers in order to install malware across websites
- To set up both internal and external watering-hole attacks
- To compromise domain controllers by abusing the trust that exists between domains for lateral movement

PoS RAM scrapers are typically final attack payloads. Depending on the complexity of target networks, attackers either directly infect or laterally move across networks to search for PoS servers. Once found, PoS RAM scrapers infect the servers.

Data-Exfiltration Techniques

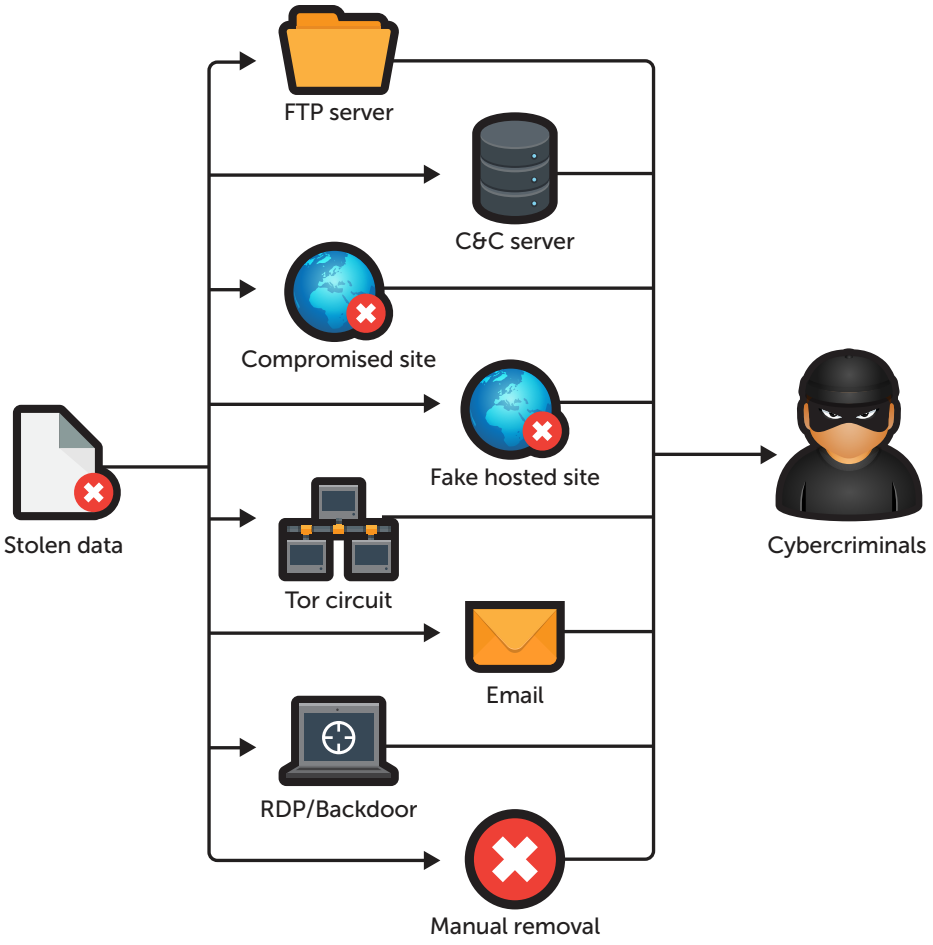
Tracks 1 and 2 card data harvested from infected PoS systems is only valuable if successfully exfiltrated. Older PoS RAM scrapers did not have data-exfiltration functionality. Instead, they dropped the data gathered into text files that were then manually removed or

remotely collected. With the growing popularity of PoS RAM scrapers as a tool for stealing large volumes of credit card data, their functionality has quickly evolved to include data exfiltration.

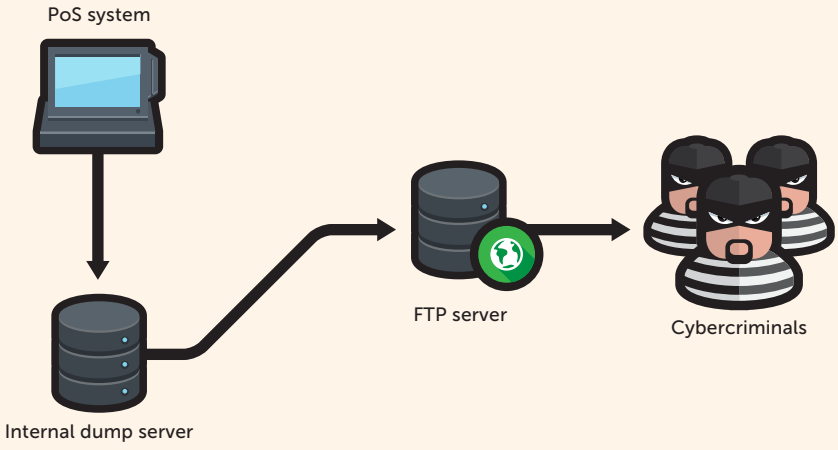
Our analysis of various PoS RAM scraper families allowed us to classify data-exfiltration techniques into eight categories.

Attackers who use PoS RAM scrapers usually register fake websites with hosting providers in countries that have lax Internet law enforcement such as Russia, Romania, and the Ukraine. These fake domains act like MitM data collectors. Attackers also compromise legitimate websites to use them as MitM data collectors. They use compromised email accounts to exfiltrate stolen data as attachments. They create accounts on File Transfer Protocol (FTP) servers hosted in countries with lax Internet law enforcement that PoS RAM scrapers can log in to using hard-coded credentials when sending over stolen data. The majority of PoS RAM scrapers though directly exfiltrate stolen data to C&C servers by embedding it in HTTP POST/GET/Header requests. Attackers also remotely access compromised PoS servers via Remote Desktop Protocol (RDP) or VNC to collect stolen card data dumped onto text files. Manual removal, in the case of insider jobs, works the same way.

In some attacks, the Tor network conceals C&C servers' IP addresses and by default encrypts all traffic. The C&C domains in these attacks end with a .onion pseudo-top-level domain (TLD), which cannot be



PoS RAM scraper data-exfiltration techniques



Multistage data-exfiltration steps

resolved outside the Tor network and can only be accessed using a Tor proxy application.

In cases that involve the exfiltration of millions of credit card numbers—Target and Home Depot—attackers use multistage data exfiltration.

Attackers do not create an outbound HTTP POST/GET/Header request for every harvested credit card number because massive volumes of such requests would quickly alert IT staff. Instead, they use an already-compromised system on the LAN/WAN as an internal dump server for large batches of stolen credit card data. Internal dump servers have external Internet access. Attackers upload stolen credit card data from dump servers to remote FTP servers then delete all traces from the dump servers.

HOW DATA SECURITY STANDARD COMPLIANCE HELPS PROTECT AGAINST POS RAM SCRAPERS

The PCI Security Standards Council is an open global forum responsible for PCI security standards development, management, education, and awareness. The PCI security standards include the PCI DSS, the Payment Application DSS (PA DSS), and PIN Transaction Security (PTS) requirements. [17–18] These standards aim to protect businesses and cardholders from the threats that PoS RAM scrapers pose. This paper will only discuss PCI and PA DSS.

PCI DSS

PCI DSS refers to a set of requirements designed to ensure that all companies that process, store, or transmit credit card data maintains a secure environment. [19] It does not offer new secure technologies to protect electronic payment systems but does provide requirements to build additional layers of security around existing ones. PCI DSS ver. 1.0 was published in December 2004, long after electronic payment systems were developed and already deployed worldwide. At that point, defining, developing, and deploying a brand new secure technology standard for payment cards would have been extremely expensive. PCI DSS has 12 major requirements. [20]

The PCI Security Standards Council introduced new requirements in PCI DSS ver. 3.0, which were made effective on 1 January 2015 in hopes of mitigating problems identified in recent PoS-system-related breaches. The following are some of the requirements:

- **5.1.2:** Evaluate evolving malware threats for any system not considered commonly affected.
- **8.2.3:** Combine minimum password complexity and strength requirements into one and increase the flexibility for alternatives.
- **8.5.1:** For service providers with remote access to customer premises, use unique authentication credentials for each customer.*
- **8.6:** Where other authentication mechanisms—physical or logical security tokens, smart cards, and certificates—are used, these must be linked to an individual account. Ensure that only the intended user can gain access to these mechanisms.
- **9.3:** Control on-site personnel's physical access to sensitive areas. Implement a process to authorize access and immediately revoke access upon staff termination.
- **9.9:** Protect devices that capture payment card data via direct physical interaction from tampering and substitution. *
- **11.3 and 11.4:** Implement a penetration-testing methodology. If segmentation is used to isolate the cardholder data environment from other networks, perform penetration tests to verify that the segmentation methods are operational and effective. *
- **11.5.1:** Implement a process to respond to any alert generated by a change-detection mechanism.
- **12.8.5:** Maintain information on which PCI DSS requirements are managed by each service provider and which are managed by an entity.

Items marked with an * are future-dated requirements that are considered best practices until 1 July 2015.

PA DSS

PA DSS refers to a set of requirements that intend to help software vendors develop secure payment applications that support PCI DSS compliance. PA DSS applies to all third-party applications that store, process, or transmit payment cardholder data during transaction processing. Software developed by retailers and merchants for in-house use are exempted from PA DSS but not from PCI DSS compliance. [21] PA DSS has 14 major requirements:

- Do not retain full magnetic stripe, card verification code or value (i.e., CAV2, CID, CVC2, and CVV2), or PIN block data. [22]
- Protect stored cardholder data.
- Provide secure authentication features.
- Log payment application activity.
- Develop secure payment applications.
- Protect wireless transmissions.
- Test payment applications to address vulnerabilities.
- Facilitate secure network implementation.

- Cardholder data must never be stored on an Internet-connected server.
- Facilitate secure remote software updates.
- Facilitate secure remote access to payment application.
- Encrypt sensitive traffic over public networks.
- Encrypt all nonconsole administrative access.
- Maintain instructional documentation and training programs for customers, resellers, and integrators.

To date, no known PoS credit card data breaches have been attributed to PoS software vulnerability exploitation but that does not guarantee it will not happen in the future. PA DSS ver. 3.0 strengthened requirements to help protect against possible exploitation attacks in the future, as evidenced by the following:

- **5.1.5:** Payment application developers need to verify the integrity of source codes during development.
- **5.1.6:** Payment applications should be developed according to industry best practices with regard to secure coding techniques.
- **5.4:** Vendors should incorporate versioning methodology into each payment application.
- **5.5:** Payment application vendors should incorporate risk assessment techniques into their software development processes.
- **7.3:** Vendors should provide release notes for all application updates.
- **10.2.2:** Vendors with remote access to customer premises so they can provide support or maintenance services, for instance, should use unique authentication credentials for each customer.

Third-Party Vendor Access Issues

The merchants and vendors in the PoS transaction chain are ultimately responsible for implementing PCI DSS. Many large companies allow third-party vendors that provide them with goods and services access to their corporate networks for business purposes. The two biggest credit card theft incidents in recent times—the Target and Home Depot breaches—both involved third parties that had access to the vendors' networks. [23] After gaining initial entry into the vendors' corporate networks, the attackers laterally moved to find and compromise PoS servers.

A recent breach of a parking facilities provider's network also involved a third-party vendor that maintained the company's payment card systems in multiple locations across the United States. [24] The third-party vendor's

network was compromised and its own remote access tool (RAT) was used to gain access to its customer's—the parking facilities provider's—payment-processing systems. Investigations revealed that the third-party vendor did not use two-factor authentication for remote access, which made it easy for attackers to gain entry into its network.

The cases described above are just a few examples wherein major gaps in operations security could have been addressed by PCI and PA DSS compliance.

DEFENDING AGAINST POS RAM SCRAPERS

Traditional defenses against malware are signature-based solutions such as those found in antivirus software that scan for known threats. Against zero days, new malware, new exploits, targeted attacks, and the like, signature-based solutions cannot provide sufficient protection. By the time new signatures are added to block the threat, the damage may have already been done. [25] The solution is to put multilayer defenses in place to make up for the shortcomings of individual security products and provide holistic protection.

PoS Defense Model

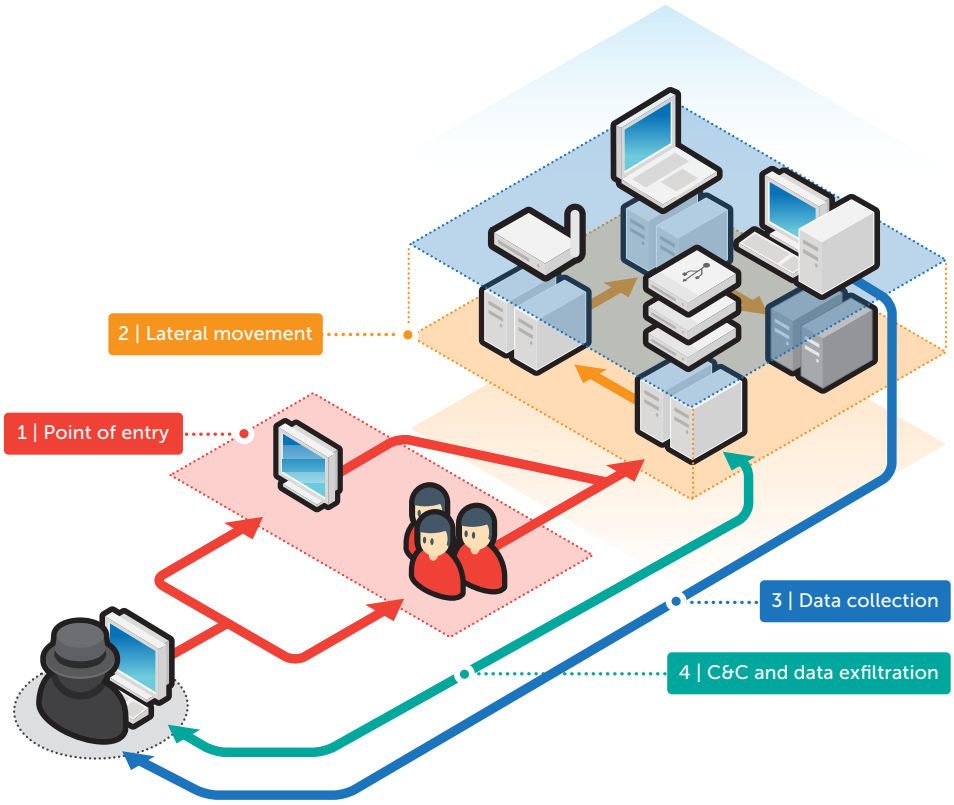
Our analysis of the PoS RAM scraper attack chain and PCI and PA DSS requirements allowed us to create a multilayer defense model that businesses can implement to defend against attacks. The four layers of the PoS defense model are:

- **Point of entry:** This is the first and most important line of defense against PoS RAM scrapers, as it aims to prevent initial infection or block malware execution before it can cause damage.
- **Lateral movement:** If the infection layer fails to thwart malware execution, the next layer should be able to stop the malware from spreading by identifying suspicious or malicious behaviors.
- **Data collection:** PoS RAM scrapers can have other data-stealing components that sniff network traffic, log keystrokes, and steal sensitive files. This protection layer aims to prevent data theft.
- **C&C and data exfiltration:** Stolen credit card data is only valuable after exfiltration. This final layer of protection aims to prevent the malware from communicating with C&C servers and exfiltrating stolen data.

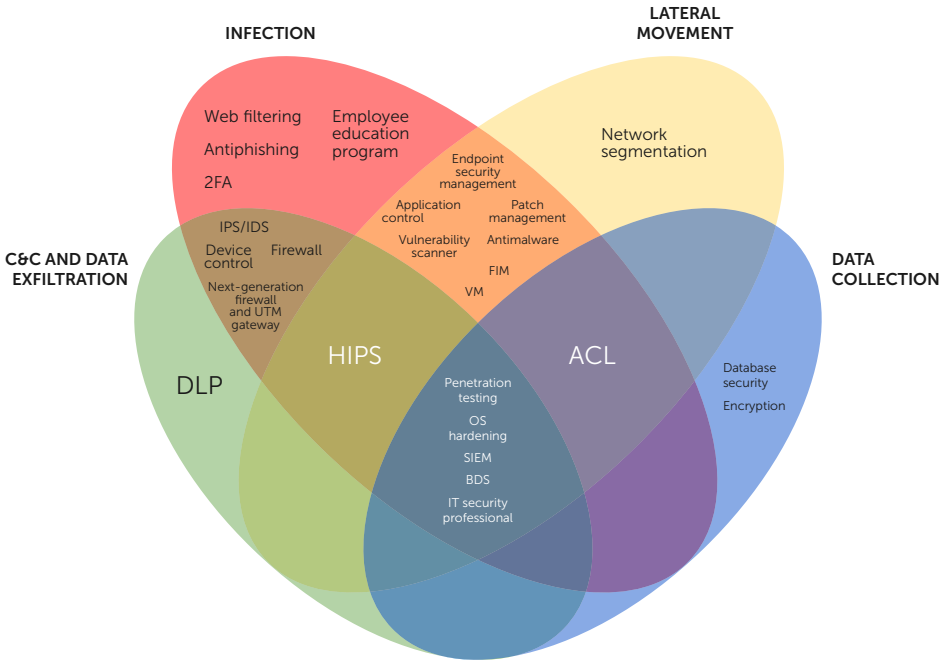
Defensive Technologies and Strategies

We listed down 26 defensive technologies and strategies that companies can implement in their environments to defend against PoS RAM scraper attacks. Some of them overlap in terms of coverage in the PoS defense model.

The majority of commercially available solutions focus on preventing infections. Many of them are multifunctional and block both lateral movement and data exfiltration. However, only a handful covers all aspects of the PoS defense model.



PoS defense model



Defensive technologies and strategies against PoS RAM scrapers

More detailed descriptions of the defensive technologies and strategies are provided in the following table.

Defensive Technology/Strategy	PoS Defense Model Coverage	Description	PoS RAM Scraper Defense
Access control lists (ACLs)	Infection, lateral movement, and data collection	File system objects such as directories, folders, and files have a security attribute that specifies which user groups can access them and what kinds of access privilege—read, write, and/or execute—each user group has over them. ACL provides a rundown of objects with their corresponding user-access privileges. [26]	ACLs can be used to restrict read, write, and/or execute permissions on PoS system directories and folders. This blocks normal PoS RAM scraper behaviors, thus preventing execution, lateral movement, and data theft.
Antiphishing solutions	Infection	Antiphishing solutions are email-filtering products that scan for and block incoming spam.	Spear-phishing emails remain the top PoS RAM scraper means of infection. Antiphishing solutions block phishing emails and prevent infections. Some antiphishing solutions also use message sandboxes to screen for potential threats.
Antimalware solutions	Infection and lateral movement	Antimalware solutions scan files to detect, block, and remove malicious software such as viruses, Trojans, worms, keyloggers, and rootkits from systems.	Antimalware solutions detect known and zero-day PoS RAM scrapers using heuristic and generic signatures. They also detect other dropped or downloaded malicious components that may be used for lateral movement and data exfiltration.
Application control or white-listing solutions	Infection and lateral movement	Application control solutions are designed to prevent unwanted and unknown applications from executing on endpoints. They only allow white-listed applications to execute.	Application control solutions prevent unknown binaries from executing, thus blocking PoS RAM scrapers and/or their other malicious components from executing.

Defensive Technology/Strategy	PoS Defense Model Coverage	Description	PoS RAM Scraper Defense
Breach detection systems (BDSs)	Infection, lateral movement, data collection, C&C, and data exfiltration	BDSs are security solutions that detect intrusions caused by targeted attacks and other sophisticated threats designed to harvest data from compromised systems. [27] BDSs analyze complex attacks out of band, detecting rather than preventing network breaches.	BDSs can analyze network traffic patterns across multiple protocols; identify malicious domains; and using emulation-sandboxing, model the behavior and impact of dropped or downloaded malicious files. [28] As such, they can identify and alert IT administrators to the presence of zero-day PoS RAM scrapers.
Data loss prevention (DLP) systems	C&C and data exfiltration	DLP systems detect and thwart potential data breach or exfiltration transmissions by monitoring, detecting, and blocking the transmission of sensitive data while in use (by endpoints), in motion (part of network traffic), and at rest (stored data). [29]	Some PoS RAM scrapers exfiltrate stolen credit card Tracks 1 and 2 data in plain text format. DLP solutions can identify and block Tracks 1 and 2 data transmissions.
Database security controls	Data collection	Database security refers to controls and measures such as access control, authentication, encryption, and backup designed to protect databases against confidentiality, integrity, and availability compromise. [30]	Attackers reportedly stole full databases containing sensitive credit card data in several PoS system breaches. [31] Database security controls help protect against these types of theft.
Device control systems	Infection, C&C, and data exfiltration	Device control systems regulate access to external storage devices and network resources connected to endpoints. These help prevent data loss and leakage. [32]	PoS RAM scrapers such as VSkimmer attempt to exfiltrate stolen credit card data via removable storage devices. Device control systems installed on PoS systems prevent data exfiltration.

Defensive Technology/Strategy	PoS Defense Model Coverage	Description	PoS RAM Scraper Defense
Employee education programs	Infection	These structured learning programs should teach employees information security best practices at work.	Educating employees on social engineering, phishing, and malware and how these can damage their organization, along with security best practices, can increase their awareness of potential threats. They will be armed with the knowledge to safeguard themselves against becoming victims.
Encryption technologies	Data collection	These encrypt and decrypt data in the form of files, emails, or packets sent over networks. [33]	PCI DSS does not mandate that credit card data sent over LANs/WANs be encrypted. Only data sent over public networks requires encryption. This can potentially lead to network-sniffing attacks. Encrypting all sensitive data transmitted over networks prevents this type of attack.
Endpoint security management	Infection and lateral movement	Endpoint security management is a policy-based approach to network security that requires endpoint devices to comply with specified security criteria before they are granted access to network resources. [34]	This mandates that all PoS systems, endpoints and servers alike, in the operating environment be uniformly security compliant before getting access to network resources. Enforced security policies help prevent infection and lateral movement.
File integrity monitoring (FIM)	Infection and lateral movement	FIM validates the integrity of OS and application software files by monitoring and comparing current file states against known good baselines. [35]	FIM will alert IT administrators to any unexpected PoS system security setting, configuration, file, and credential alteration.

Defensive Technology/Strategy	PoS Defense Model Coverage	Description	PoS RAM Scraper Defense
Firewalls	Infection, C&C, and data exfiltration	Firewalls are network security systems that control incoming and outgoing traffic based on applied rule sets. [36]	Firewalls monitor for ingress and egress traffic to unknown and bad domains and identifies applications or endpoints that generate or request bad traffic. They block data exfiltration and C&C traffic.
Host-based intrusion prevention systems (HIPSs)	Infection, lateral movement, C&C, and data exfiltration	HIPSs monitor and analyze events that occur on hosts to identify suspicious or malicious activities.	PoS RAM scrapers generate events when they read the process memory, modify registry keys, write to network shares, and copy themselves to system folders. HIPSs monitor these events and generate alerts when suspicious activities are detected.
Intrusion prevention systems (IPSs)/Intrusion detection systems (IDSs)	Infection, C&C, and data exfiltration	IDSs/IPSs are network security systems that examine traffic flow to detect and prevent network-based attacks. [37] IDSs are passive systems that generate reports when known bad events are identified. IPSs, meanwhile, reject packets when known bad events are identified.	IDSs/IPSs monitor entire networks for suspicious traffic by analyzing protocols and performing deep packet inspections. Outgoing HTTP POST/ GET/Header requests to suspicious domains, FTP sites, and the Tor network generated by some PoS RAM scrapers will trigger IDS/IPS alerts.
IT security professionals	Infection, lateral movement, data collection, C&C, and data exfiltration	IT security professionals specialize in detecting, preventing, and resolving computer security threats in a business environment. They also maintain the integrity and confidentiality of the company's data and information systems. [38]	IT staff specializing in computer security routinely investigate all areas of the PoS environment to determine if there are ongoing data breaches so they can take preventive measures. They also perform forensic analysis and incident response for attribution purposes.

Defensive Technology/Strategy	PoS Defense Model Coverage	Description	PoS RAM Scraper Defense
Network segmentation	Lateral movement	Network segmentation refers to splitting a network into multiple subnetworks to reduce congestion, limit failures, and improve security.	Putting all PoS systems on a dedicated network that is separate from the corporate network reduces risks of lateral movement and improves overall security.
Next-generation firewalls/ Unified threat management (UTM) gateways	Infection, C&C, and data exfiltration	Next-generation firewalls and UTM gateways are network security products that unify multiple systems and services into a single engine or appliance. [39–40] UTM gateways generally have lower traffic throughput compared with next-generation firewalls. [41–42] UTM gateways are traditionally geared for small and medium-sized businesses (SMBs) while next-generation firewalls are used by enterprises. [43]	Next-generation firewalls and UTM gateways analyze network traffic at line speeds using multiple scanning technologies. They can detect HTTP POST/GET/Header requests to suspicious or malicious domains, FTP sites, and the Tor network generated by PoS RAM scrapers. They can incorporate firewalls; IPSs/ IDSs; and antimalware, Web-filtering, application control, and other solutions in the same appliance.
OS hardening	Infection, lateral movement, data collection, C&C, and data exfiltration	Hardening means making an OS more secure by reducing its surface of vulnerability exposure. This can be done by installing security software; applying patches; enforcing password complexity requirements; and eliminating unnecessary software, user accounts, services, network ports, drivers, subsystems, features, and others. [44]	OS hardening decreases risks of malware infection via vulnerability exploitation. It also locks down services, ports, and network resources, restricting both lateral movement and data exfiltration.

Defensive Technology/Strategy	PoS Defense Model Coverage	Description	PoS RAM Scraper Defense
Physical/Virtual patch management or vulnerability shielding	Infection and lateral movement	Patch management software keep endpoints, servers, and remote systems updated by applying the latest security patches and updates. Virtual patch management uses a security enforcement layer to prevent malicious traffic from reaching vulnerable applications. Virtual patches prevent exploitation without modifying applications' code. [45]	Applying patches reduces risks of vulnerability exploitation. In an environment where patches need to be thoroughly tested first before they are applied, virtual patching acts as a stopgap measure by blocking malicious traffic from reaching vulnerable systems. Malware frequently move laterally by exploiting vulnerabilities on target systems. Patch management prevents infection and lateral movement.
Penetration testing	Infection, lateral movement, data collection, C&C, and data exfiltration	Penetration testing on systems, networks, and Web applications allows IT administrators to find vulnerabilities that attackers can exploit. [46]	The best way to test if PoS environments are susceptible to attacks is to perform penetration testing in order to find out how easily and how far attackers can penetrate them.
Security information and event management (SIEM)	Infection, lateral movement, data collection, C&C, and data exfiltration	SIEM software and services provide real-time analysis of security alerts generated by network hardware, servers, endpoints, and applications. SIEM is used for data aggregation, rule-based or statistical data correlation, alerts, dashboards, compliance, log retention, forensics, and so on. [47]	In large networks comprising thousands of connected devices that generate alerts, it becomes increasingly difficult to isolate important ones. SIEM provides IT staff the tools to create rules that filter and highlight important and relevant alerts. Log analysis helps determine if there is a breach in progress.

Defensive Technology/Strategy	PoS Defense Model Coverage	Description	PoS RAM Scraper Defense
Two-factor authentication (2FA)	Infection	2FA refers to a security process where users utilize a two-step verification process to access company resources. Step 1 typically requires a physical token such as a smart card. Step 2 requires inputting a security code or a password. [48]	In recent PoS data breach cases, initial entry into corporate networks was gained by compromising the networks of third-party vendors with business access to the real targets' corporate networks. These vendors were not required to use 2FA. Using the stolen credentials, attackers infiltrated the real targets' networks. Using 2FA protects against the use of compromised credentials.
Virtual machines (VMs)	Infection and lateral movement	VMs are self-contained operating and application environments that emulate real systems in software. [49]	PoS systems that run in virtual environments should be reimaged on a daily or weekly basis to a known good state. This will remove existing infections and make reinfection difficult and tedious to do for attackers. Generating and storing logs for possible forensic investigations is very important when using VMs.
Vulnerability scanners	Infection and lateral movement	Vulnerability scanners are automated tools that scan endpoints, servers, networks, and applications for security vulnerabilities that attackers can exploit.	One of the tried-and-tested methods that malware use to laterally move throughout networks is to exploit vulnerabilities on target systems. Vulnerability scanners look for and identify unpatched vulnerable endpoints, servers, and applications that IT administrators can patch.
Web-filtering solutions	Infection	Web-filtering solutions restrict what URLs and websites users or endpoints can visit. They use white or black listing or both to filter content.	Web-filtering applications block malicious links embedded in phishing emails from being accessed, thus preventing infection.

Defense Recommendations for Companies

PoS RAM scraper attacks have evolved to target any company that processes credit card payments, regardless of size. Stricter PCI and PA DSS compliance requirements and security strategies should now be viewed as integral components of business operations.

SECURITY STRATEGY DECISIONS

To effectively protect against PoS RAM scraper attacks, companies need to secure all aspects of their operating environments, not just their PoS systems. Attackers can gain initial entry into their corporate networks by using compromised credentials or via spear-phishing emails. They can then laterally move throughout networks to locate and infect PoS systems.

Many factors need to be considered when making security strategy decisions, some of which are:

- **Company size:** Enterprises have complex network topologies, thousands of connected devices, multiple locations, different use cases, and so on. Their security solutions need to be scalable, be able to defend complex networks, and be centrally managed.
- **Costs:** Security solutions can be expensive especially if organizations require multilayer defense. Companies also need to factor in in-house and contracted IT service costs required to manage deployed security solutions.
- **Multiplatform support:** Many companies support all major OS platforms in their operating environments. Security solutions should be able to protect multiple OS platforms and provide centralized management of protected devices.
- **Bring your own device (BYOD) trend:** Companies are increasingly moving toward implementing BYOD policies as a means to cut costs and provide better employee flexibility. BYOD policies introduce new challenges in securing employee-owned devices that access corporate resources.

To help companies identify their security requirements, we classified the previously mentioned defensive technologies and strategies by function.

Function	Defensive Technologies/ Strategies
Base protection	Antimalware, antiphishing, and Web-filtering solutions

Function	Defensive Technologies/ Strategies
Data access control	Device control and DLP systems
Network defense	IPSs/IDSs, next-generation firewalls and UTM gateways, BDSs, and firewalls
Vulnerability management	Patch management and vulnerability scanners
Policy implementation and monitoring	SIEM, FIM, HIPSs, application control solutions, and endpoint security management
IT strategy	Encryption solutions, network segmentation, OS hardening, database security controls, VMs, ACLs, 2FA, and penetration testing
Other resources	Employee education programs and IT security professionals

By taking into consideration factors such as budget, technical expertise, operating environment complexity, company size, and others, we came up with recommendations on how organizations of varying sizes can protect themselves against PoS RAM scraper attacks. These outline the various defense options available that companies can choose from based on their specific requirements.

RECOMMENDATIONS FOR SMALL BUSINESSES

Security software vendors offer bundled packages to small businesses that include antimalware, antiphishing, and Web-filtering solutions. These are easy to set up, require minimal administration, and provide excellent security out of the box. Some vendors also include device control, DLP, patch management, and application control solutions in their small business bundles. Windows also comes with a built-in, easy-to-configure firewall. Finally, most wireless routers come with hardware firewalls. Small businesses can take advantage of all of the solutions above to protect against PoS RAM scrapers.

Function	Defensive Technologies/ Strategies	PoS Defense Model Coverage
Base protection	Antimalware, antiphishing, and Web-filtering solutions	Infection and lateral movement
Data access control	Device control and DLP systems	Infection, C&C, and data exfiltration
Network defense	Firewalls	Infection, C&C, and data exfiltration
Vulnerability management	Patch management	Infection and lateral movement
Policy implementation and monitoring	Application control solutions	Infection and lateral movement

RECOMMENDATIONS FOR MEDIUM-SIZED BUSINESSES

UTM gateways provide antimalware, antiphishing, firewall, and other protections. They also give users an option to purchase additional service modules to increase the overall functionality of their appliances. Medium-sized businesses have in-house IT staff who can safeguard against PoS RAM scrapers. Some also hire contractors who externally manage their IT service requirements.

Function	Defensive Technologies/ Strategies	PoS Defense Model Coverage
Base protection	Antimalware, antiphishing, and Web-filtering solutions	Infection and lateral movement
Data access control	Device control and DLP solutions	Infection, C&C, and data exfiltration
Network defense	Firewalls and UTM gateways	Infection, C&C, and data exfiltration

Function	Defensive Technologies/ Strategies	PoS Defense Model Coverage
Vulnerability management	Patch management	Infection and lateral movement
Policy implementation and monitoring	Application control solutions, HIPSs, and SIEM	Infection, lateral movement, data collection, C&C, and data exfiltration
IT strategy	ACLs, encryption technologies, database security controls, and OS hardening	Infection, lateral movement, data collection, C&C, and data exfiltration
Other resources	Employee education programs and IT security professionals	Infection, lateral movement, data collection, C&C, and data exfiltration

RECOMMENDATIONS FOR ENTERPRISES

Given the increasing number of PoS data breaches, using BDS solutions to analyze potential targeted attacks is becoming crucial. Enterprises should regularly hire penetration testers to assess their network security. They should have mandatory employee education programs because they are lucrative targets. They should exert every effort to secure their operating environment.

Function	Defensive Technologies/ Strategies	PoS Defense Model Coverage
Base protection	Antimalware, antiphishing, and Web-filtering solutions	Infection and lateral movement
Data access control	Device control and DLP solutions	Infection, C&C, and data exfiltration
Network defense	IPSs/IDSs, nest-generation firewalls and UTM gateways, BDSs, and firewalls	Infection, lateral movement, data collection, C&C, and data exfiltration

Function	Defensive Technologies/ Strategies	PoS Defense Model Coverage
Vulnerability management	Patch management and vulnerability scanners	Infection and lateral movement
Policy implementation and monitoring	SIEM, FIM, HIPSs, application control solutions, and endpoint security management	Infection, lateral movement, data collection, C&C, and data exfiltration
IT strategy	Encryption solutions, network segmentation, OS hardening, database security controls, VMs, ACLs, 2FA, and penetration testing	Infection, lateral movement, data collection, C&C, and data exfiltration
Other resources	Employee education programs and IT security professionals	Infection, lateral movement, data collection, C&C, and data exfiltration

WILL NEXT-GENERATION PAYMENT TECHNOLOGIES HELP?

The new reality is that any Internet-connected device that processes payment card data should be viewed as a data theft target. Buyer security rests on the shoulders of several key players—device manufacturers, service providers, businesses, banks, and even credit card brands. Strong IT defense goes a long way in preventing PoS system breaches but it is not a magic bullet. New secure payment technologies must also be deployed alongside strong IT defenses to protect against PoS RAM scrapers. This section discusses some of the new and next-generation payment technologies that are being deployed to better secure payment transactions.

EMV

Europay, MasterCard, and Visa (EMV) created the EMV Consortium in 1994 to develop new technologies to counteract payment card fraud. EMV is the global standard for Integrated Circuit Cards (ICC). EMV cards store encrypted Tracks 1 and 2 data on a chip. This chip stores a cryptogram that allows banks to determine if cards or transactions have been modified. It also stores a counter that gets incremented with each transaction. Duplicate or skipped counter values indicate potential fraudulent

activities. EMV cards interact with PoS terminals that have ICC readers and use the EMV-defined protocol for transactions. As with debit cards, cardholders need to input a PIN for authentication before transactions are processed.

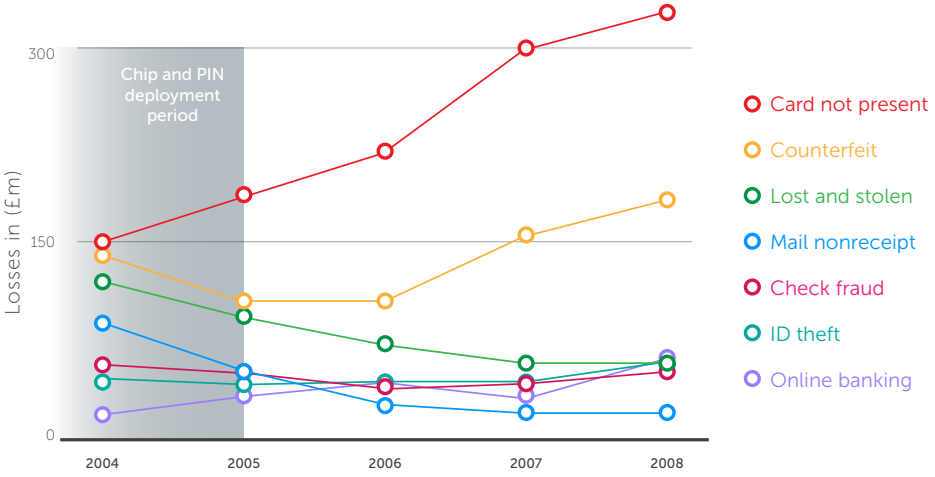
EMV and radio-frequency-identification (RFID)-enabled credit card

EMV or chip-and-PIN credit cards are widely used in Canada, Mexico, South America, Europe, and Asia. The United States is scheduled to switch to EMV credit cards by October 2015. [50] Unlike the rest of the world who use chip-and-PIN cards, the United States opted for chip-and-signature cards, which fall short on fraud control. U.S. banks chose not to go the chip-and-PIN route because they did not want customers to be burdened with remembering a new four-digit code each time a transaction is made during checkout. [51] After the switch to EMV cards by October this year, merchants who do not upgrade their payment systems will be held responsible for fraudulent charges made on EMV credit cards. Consumers typically do not bear the financial costs of fraudulent transactions as long as they can prove they did not make the purchases.

> In reality, EMV cards cannot prevent PoS RAM scraper attacks. EMV was developed to prevent credit card counterfeiting, not PoS RAM scraping.

After the Target breach in December 2013, EMV credit cards became the focus of much discussion, as many saw them as a solution to credit card data breaches. However, the more recent Home Depot breach, which involved EMV credit cards used at Canadian Home Depot locations, proved otherwise. [52] In reality, EMV credit cards cannot prevent PoS RAM scraper attacks. [53–54] EMV was developed to prevent credit card counterfeiting, not PoS RAM scraping. The EMV chip-on-card makes it extremely difficult for attackers to manufacture counterfeit credit cards using stolen data, which helps reduce counterfeiting or lost or stolen card fraud. EMV credit card Tracks 1 and 2 data sent to the PoS system for processing is still susceptible to RAM scraper attacks because decrypted data resides in the systems' RAM.

U.K. credit card fraud statistics show that even after EMV card introduction, losses related to card-not-present fraud continued to dramatically increase in volume. [55] This shows that criminals used stolen credit card data for online purchases, as opposed to making and using counterfeit cards.



U.K.-issued credit card fraud statistics (source: http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf)

Researchers from the University of Cambridge showed that attackers can cheaply construct special devices that intercept and modify

communications between EMV credit cards and PoS terminals, fooling the latter into accepting fake successful PIN verifications. Even though this is a proof-of concept (PoC) attack, it showed that flaws exist in the EMV protocol. Another EMV attack recently observed was the EMV "replay" attack whose first publicly known victim was a Canadian bank that incorrectly implemented its EMV transaction handling code and did not check either the cryptogram or counter values. Attackers spoofed EMV transaction requests made to the bank, which allowed fraudulent charges to be approved. In a similarly styled attack, cybercriminals in Brazil encoded non-EMV card transactions as EMV transactions that successfully passed through the Visa and MasterCard networks. In both cases, the attackers did not break the EMV protocol but took advantage of poor implementation and the trust model associated with EMV transactions. As EMV card use becomes more widespread, attackers will inevitably discover new exploitable flaws.

Contactless RFID Credit Cards

Contactless payment technology in credit cards such as MasterCard's PayPass and Visa's payWave uses passive RFID. This allows cardholders to wave their cards in front of contactless payment terminals to complete transactions. The RFID chip on credit cards is not powered and relies on radio frequency (RF) energy transferred from the powered contactless payment terminal to the card to power the chip-on-card. Because signature or PIN entry is not required for contactless purchases, banks set a maximum purchase limit per transaction, typically US$50. Contactless payment cards do not use a universal protocol for payment transactions. Each card brand instead defines its own proprietary protocol based on EMV principles. This means that a dedicated MasterCard PayPass reader cannot process transactions for Visa payWave cards. [56] Due to the growing popularity of contactless payment cards, hybrid card readers have been developed.

Contactless payment cards all use the same protocol—EMV Contactless Communication Protocol Specifications (EMV CCPS) to communicate with near-field-communication (NFC)-enabled devices. Note that EMV CCPS is used for physical-card-to-terminal communication and is different from the proprietary payment transaction protocol. Most smartphones today are NFC enabled and have apps that can read the data stored in contactless cards. Open source software libraries that can read and extract data from contactless cards can be used to build custom NFC apps. Armed with either an NFC-enabled smartphone and an app that reads contactless card data or a dedicated RFID reader, attackers can brush against potential victims in crowded public spaces and wirelessly steal their credentials via a tactic known as electronic pickpocketing.

Armed with either an NFC-enabled smartphone and an app that reads contactless card data or a dedicated RFID reader, attackers can brush against potential victims in crowded public spaces and wirelessly steal their credentials via a tactic known as electronic pickpocketing.

via a tactic known as electronic pickpocketing. [57–58] The simple solution to prevent electronic pickpocketing is to put contactless cards in shielded sleeves that block the RF energy required to power the chip-on-card.

Mobile Wallets

Osaifu-Keitai or mobile wallets were first launched in Japan in July 2004 by NTT DoCoMo. [59] Today, mobile wallets are a part of Japanese consumers' everyday lives. They have been integrated into all kinds of daily transactions made on credit cards, keycards, transit passes, and identity cards, among others. This decade-old mobile payment ecosystem is now being introduced to the rest of the world by companies such as Google through Google Wallet™ and Apple through Apple Pay™. Google and Apple aim to include credit, loyalty, gift, prepaid, and other cards in their mobile wallet services so everyone can start using digitally stored cards instead of physical ones.

Mobile wallet apps run on NFC-enabled smartphones. NFC allows devices that are centimeters apart to exchange data as long as both are NFC enabled. Mobile wallet apps are built from the ground up with strong security features in mind, including:

- Payment authorization requires user authentication
- Credit card data tokenization
- Sensitive data encryption and storage inside a secure element

The secure element—secure memory and execution environment—is a dynamic environment where application code and data can be securely stored and administered and where the secure execution of apps occur. [60] The secure element stores sensitive data on a dedicated chip in the phone or SIM card or in a secure cloud storage facility designed to be tamper resistant. [61]

Tokenization is the process that replaces a high-value credential such as credit card data with a surrogate value that is used in transactions in place of the high-value credential. [62] It can map the high-value credential to a new value that is either in the same or different format as the original. It removes credit card data from the PoS environment and replaces it with something that is useless outside the environment in which the token was created. There are different kinds of tokens and different ways to create them. A token can be merchant specific; single or multi use; or stored and managed in the cloud, in a token vault, or in a merchant location. It is created using a process defined by the token provider. Once created, it may be tied to a card on file, an individual transaction, or a device. Two types of tokens are used in the payment industry—those that function in place of actual payment account numbers for transactions and those that

replace payment account numbers stored by merchants for purposes such as accounting, inventory management, statistics gathering, and others.

A decade of heavy use in Japan demonstrated that the mobile wallet ecosystem is secure and reliable. In fact, so far, only insider attacks have been observed against it. [63]

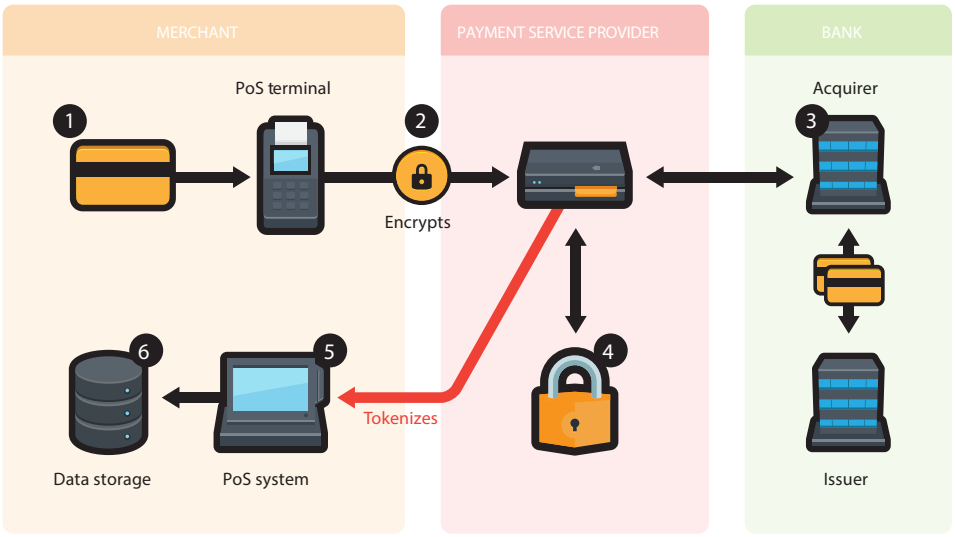
A decade of heavy use in Japan demonstrated that the mobile wallet ecosystem is secure and reliable. In fact, so far, only insider attacks have been observed against it.

New Payment-Processing Architectures

PoS RAM scrapers will have nothing to steal if credit card Tracks 1 and 2 data are not present in PoS systems' RAM. This is the underlying principle behind the new payment-processing architectures being developed and deployed today. The two leading architectural solutions to this problem are encryption plus tokenization and secure element. It is important to note that both of these solutions work with EMV credit cards.

ENCRYPTION PLUS TOKENIZATION

The encryption plus tokenization payment architecture encrypts and tokenizes credit card data, making credit card data theft virtually impossible.



How encryption plus tokenization works

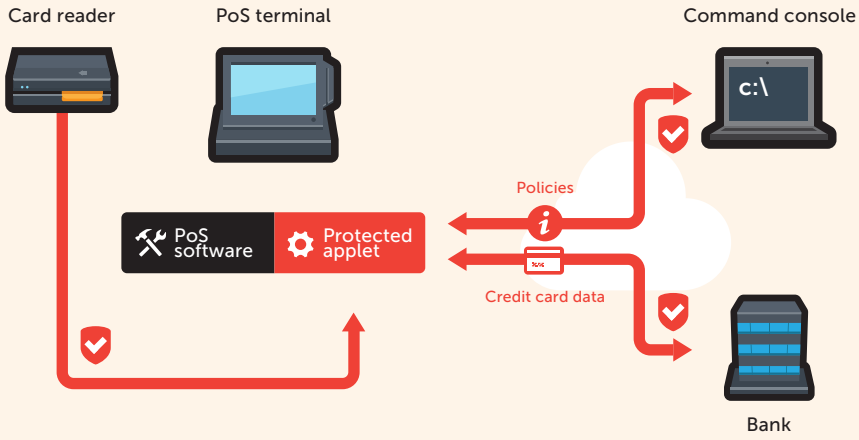
In this architecture, customers swipe their credit cards at merchants' PoS terminals to complete purchases (step 1 in the diagram). The PoS terminals read, encrypt, and transmit credit card data to the payment service providers (PSPs) for processing (step 2 in the diagram). The PSPs then forward the credit card data to banks—acquirers and issuers—for authorization (step 3 in the diagram). PSPs use a tokenization algorithm to replace actual credit card data with tokens (step 4 in the diagram). The tokens and their bank authorization statuses are then sent back to merchants' PoS systems (step 5 in the diagram), which store tokens instead of actual credit card data in all places (step 6 in the diagram).

The encryption plus tokenization payment architecture ensures that actual credit card data is never present in PoS systems' RAM or on any other merchant system. Stolen tokens cannot be used to create counterfeit credit cards and cannot be used in card-not-present transactions.

SECURE ELEMENT

Another architectural solution created by Intel uses a secure element to process credit card transactions. [64]

Credit card data is read by PoS terminals and directly sent to a secure element, which Intel calls "Protected Applet," bypassing the PoS software. Protected Applet manages all transaction-processing requests with banks and can be configured to share certain data with PoS software. [65] Moving all credit-card-processing actions to the secure element and completely bypassing PoS systems' RAM ensures that sensitive data cannot be stolen by malware. Secure element is designed to be tamper resistant and cannot be infected by PoS RAM scrapers.



How Intel's dedicated payment chip works (source: http://www.intel.com/content/www/us/en/embedded/technology/security/secure-payment-transactions/overview.html)

CONCLUSION

So what does the future hold for PoS RAM scraper attacks?

As PoS RAM scrapers become more prominent threats, big businesses will heavily invest in cybersecurity to prevent attacks against their PoS environments. Attackers will thus refocus on SMBs, as these may not necessarily have the cybersecurity budgets that enterprises have to prevent PoS system breaches. We expect to see more SMBs get compromised, which will collectively be a bigger breach than compromising a few enterprises.

The rollout of new measures such as EMV and PCI DSS ver. 3.0 compliance standards will significantly change the PoS playing field for attackers. In the United States, these measures are scheduled to come into full effect by October this year. If there is a successful nationwide rollout of the new measures, there will be a decline in the number of PoS-related data breaches. As businesses upgrade to new secure payment systems, attackers will attempt to come up with new strategies against improved systems and environments. It will take attackers several months, possibly well into 2016, before they can figure out how to breach upgraded PoS environments.

In the meantime, attackers will find new ways to breach the security of target companies via third-party vendors who have access to their corporate networks. Third-party vendors will be the weakest link in the chain because they may not necessarily have the same level of security as their corporate customers. PCI DSS ver. 3.0 compliance standards aim to strengthen third-party vendors' security requirements to minimize the risks they pose to their corporate customers.

New payment technologies and compliance standards aim to stop PoS system breaches. Their complete deployment will successfully prevent a majority of the PoS system attacks. But because easy money making is involved, it is safe to assume that attackers will figure out new breach strategies to compromise the security of systems, businesses, and consumers. To date, Bob Russo's Statement for the Record, "Our work is broad for a simple reason: there is no single answer to securing payment card data. No one technology is a panacea; security requires a multilayer approach across the payment chain," remains true. [66]

REFERENCES

[1] Brian Krebs. (10 October 2013). *Krebs on Security.* "Nordstrom Finds Cash Register Skimmers." Last accessed on 22 August 2014, http://krebsonsecurity.com/2013/10/nordstrom-finds-cash-register-skimmers/.

[2] ISO. (2014). *ISO.* "ISO/IEC 7813:2006: Information Technology—Identification Cards—Financial Transaction Cards." Last accessed on 19 August 2014, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43317.

[3] Visa Inc. (2008). "Visa Data Security Alert: Debugging Software – Memory Parsing Vulnerability." Last accessed August 18, 2014, http://usa.visa.com/download/merchants/debugging_software_memory.pdf.

[4] Numaan Huq. (September 2014). *Trend Micro Security Intelligence.* "PoS RAM Scraper Malware: Past, Present, and Future." Last accessed on 11 December 2014, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-ram-scraper-malware.pdf.

[5] Sara Peters. (4 September 2014). *Dark Reading.* "Backoff Not to Blame for Goodwill Breach." Last accessed on 17 February 2015, http://www.darkreading.com/backoff-not-to-blame-for-goodwill-breach/d/d-id/1306963.

[6] Sara Peters. (4 September 2014). *Dark Reading.* "Backoff Not to Blame for Goodwill Breach." Last accessed on 26 February 2015, http://www.darkreading.com/backoff-not-to-blame-for-goodwill-breach/d/d-id/1306963.

[7] Brian Krebs. (7 September 2014). *Krebs on Security.* "Home Depot Hit by Same Malware as Target." Last accessed on 11 December 2014, http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/.

[8] Jonathan Leopando. (9 September 2014). *TrendLabs Security Intelligence Blog.* "Home Depot Breach Linked to BlackPOS Malware." Last accessed on 17 February 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/home-depot-breach-linked-to-blackpos-malware/.

[9] Numaan Huq. (4 December 2014). *TrendLabs Security Intelligence Blog.* "Planes, Trains, and Automobiles—Are You Safe from PoS Malware Anywhere?" Last accessed on 11 December 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/planes-trains-automobiles-are-you-safe-from-pos-malware-anywhere/.

[10] Anthony Joe Melgarejo. (27 November 2014). *TrendLabs Security Intelligence Blog.* "New PoS Malware Kicks Off Holiday Shopping Weekend." Last accessed on 17 February 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/new-pos-malware-kicks-off-holiday-shopping-weekend/.

[11] Eduard Kovacs. (3 December 2014). *Security Week.* "New 'LusyPOS' Malware Uses Tor for C&C Communications." Last accessed on 17 February 2015, http://www.securityweek.com/new-lusypos-malware-uses-tor-cc-communications.

[12] PC World. "New Point-of-Sale Malware on Underground Markets for $2,000." Last accessed on 11 December 2014, http://www.pcworld.com/article/2854092/new-pointofsale-malware-on-underground-markets-for-2000.html.

[13] Jim Gogolinski. (9 December 2014). *TrendLabs Security Intelligence Blog.* "Insider Threats 101: The Threat Within." Last accessed on 17 December 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/insider-threats-101-the-threat-within/.

[14] Trend Micro Incorporated. (2015). *Trend Micro Security Intelligence.* "Magnified Losses, Amplified Need for Cyber-Attack Preparedness: TrendLabs 2014 Annual Security Roundup." Last accessed on 25 February 2015, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-magnified-losses-amplified-need-for-cyber-attack-preparedness.pdf.

[15] PCI Security Standards Council. "About Us." *PCI Security Standards Council.* Last accessed on 18 December 2014, https://www.pcisecuritystandards.org/organization_info/index.php.

[16] Trend Micro Incorporated. (2013). *Trend Micro Security Intelligence.* "Lateral Movement: How Do Threat Actors Move Deeper into Your Network?" Last accessed on 16 December 2014, http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/tlp_lateral_movement.pdf.

[17] PCI Security Standards Council. (October 2010). "Payment Card Industry (PCI): Payment Application Data Security Standard." Last accessed on 18 December 2014, https://www.pcisecuritystandards.org/documents/pa-dss_v2.pdf.

[18] Margaret Rouse. (2015). *TechTarget.* "PA-DSS (Payment Application Data Security Standard)." Last accessed on 18 December 2014, http://searchsecurity.techtarget.com/definition/PA-DSS-Payment-Application-Data-Security-Standard.

[19] PCI Security Standards Council. (7 November 2013). "PCI Council Publishes PCI DSS and PA DSS Ver. 3.0." Last accessed on 18 December 2014, https://www.pcisecuritystandards.org/pdfs/13_11_06_DSS_PCI_DSS_Ver._3_0_Press_Release.pdf.

[20] IBM. (2015). *IBM Knowledge Center.* "Addressing the PCI Data Security Standard Within WebSphere Commerce." Last accessed on 20 February 2015, http://www-01.ibm.com/support/knowledgecenter/SSZLC2_7.0.0/com.ibm.commerce.pci.doc/concepts/csepcireqs.htm.

[21] PCI ComplianceGuide.org. (2014). *PCI ComplianceGuide.org.* "PCI FAQs." Last accessed on 17 December 2014, https://www.pcicomplianceguide.org/pci-faqs-2/.

[22] DalPay. (2015). *DalPay.* Last accessed on 18 February 2015, https://www.dalpay.com/en/support/card_security_code.html.

[23] John Leyden. (17 December 2014). *The Register.* "Can't Stop Home-Depot-Style Card Pwning, but Suppliers Will Feel PCI Regulation Pain." Last accessed on 18 December 2014, http://www.theregister.co.uk/2014/12/17/pci_revamp_after_target_home_depot_breach/.

[24] Brian Prince. (14 January 2015). *Security Week.* "Park 'N Fly Confirms Data Breach Impacting E-Commerce Customers." Last accessed on 18

February 2015, http://www.securityweek.com/park-n-fly-confirms-data-breach-impacting-e-commerce-customers.

[25] Troy Leach and Christopher Strand. (23 December 2014). *Dark Reading.* "How PCI DSS 3.0 Can Help Stop Data Breaches." Last accessed on 6 January 2015, http://www.darkreading.com/risk/compliance/how-pci-dss-30-can-help-stop-data-breaches/a/d-id/1318306.

[26] QuinStreet Inc. (2105). *Webopedia.* "ACL—Access Control List." Last accessed on 31 December 2014, http://www.webopedia.com/TERM/A/ACL.html.

[27] NSS Labs Inc. (8 November 2012). "NSS Labs Announces Analyst Coverage and New Group Test for Breach Detection Systems." Last accessed on 31 December 2014, https://www.nsslabs.com/news/press-releases/nss-labs-announces-analyst-coverage-and-new-group-test-breach-detection-systems.

[28] Michael Kassner. (12 August 2013). *TechRepublic.* "Breach Detection Systems Take Aim at Targeted Persistent Attacks." Last accessed on 19 February 19, 2015, http://www.techrepublic.com/blog/it-security/breach-detection-systems-take-aim-at-targeted-persistent-attacks/.

[29] TechTarget. (2015). *WhatIs.com.* "Data Loss Prevention (DLP)." Last accessed on 19 February 2015, http://whatis.techtarget.com/definition/data-loss-prevention-DLP.

[30] Meg Coffin Murray. (2010). *Journal of Information Technology Education.* "Database Security: What Students Need to Know." Last accessed on 19 February 2015, http://jite.org/documents/Vol9/JITEv9IIPp061-077Murray804.pdf.

[31] Privacy Rights Clearinghouse. (2015). *PRC.* "Chronology of Data Breaches." Last accessed on 5 January 2015, https://www.privacyrights.org/data-breach/new.

[32] Trend Micro Incorporated. (2015). *Trend Micro.* "Device Control." Last accessed on 31 December 2014, http://docs.trendmicro.com/all/ent/officescan/v10.0/en-us/osce_10.0_olhsrv/osceag/osceag-scan/device_control.htm.

[33] Margaret Rouse. (November 2014). *TechTarget.* "Encryption." Last accessed on 19 February 2015, http://searchsecurity.techtarget.com/definition/encryption.

[34] Margaret Rouse. (January 2012). *TechTarget.* "Endpoint Security Management." Last accessed on 31 December 2014, http://searchconsumerization.techtarget.com/definition/endpoint-security-management.

[35] Infosec Institute. (18 July 2014). *Infosec Institute.* "File Integrity Monitoring (FIM) and PCI DSS." Last accessed on 19 February 2015, http://resources.infosecinstitute.com/file-integrity-monitoring-fim-pci-dss/.

[36] Vangie Beal. (2015). *Webopedia.* "Firewall." Last accessed on 19 February 2015, http://www.webopedia.com/TERM/F/firewall.html.

[37] SANS Institute. (2004). *SANS Institute InfoSec Reading Room.* "Understanding IPS and IDS: Using IPS and IDS Together for Defense in Depth." Last accessed on 19 February 2015, https://www.sans.org/reading-room/whitepapers/detection/understanding-ips-ids-ips-ids-defense-in-depth-1381.

[38] Education Portal. (2015). *Education Portal.* "Network Security Specialist: Job Description and Requirements." Last accessed on 3 January 2015, http://education-portal.com/articles/Network_Security_Specialist_Job_

Description_and_Requirements.html.

[39] Frank Ohlhorst. (1 March 2013). *Information Week.* "Next-Generation Firewalls 101." Last accessed on 19 February 2015, http://www.networkcomputing.com/careers-and-certifications/next-generation-firewalls-101/a/d-id/1234097?.

[40] Margaret Rouse. (June 2014). *TechTarget.* "Unified Threat Management (UTM)." Last accessed on 19 February 2015, http://searchmidmarketsecurity.techtarget.com/definition/unified-threat-management.

[41] Andrew Plato. (25 September 2012). *Anitian Blog.* "UTM V NGFW—A Single Shade of Grey." Last accessed on 31 December 2014, https://blog.anitian.com/utm-v-ngfw-a-single-shade-of-gray/.

[42] Sam Erdheim. (19 February 2013). *Algosec.* "State of the Firewall—UTM Vs. NGFW." Last accessed on 31 December 2014, http://blog.algosec.com/2013/02/state-of-the-firewall-utm-vs-ngfw.html.

[43] Brian Reed. (30 January 2012). *Firewalls.com.* "UTM Firewalls Versus Next-Generation Firewalls." Last accessed on 31 December 2014, http://www.firewalls.com/blog/utm_firewall_vs_ng_firewall/.

[44] Jason M. Ragland. (8 January 2015). *The University of Texas at Austin.* "Windows 2008R2 Server Hardening Checklist." Last accessed on 31 December 2014, https://wikis.utexas.edu/display/ISO/Windows+2008R2+Server+Hardening+Checklist.

[45] TechTarget. (April 2013). *WhatIs.com.* "Virtual Patching." Last accessed on 31 December 2014, http://whatis.techtarget.com/definition/virtual-patching.

[46] Margaret Rouse. (May 2011). *TechTarget.* "Pen Test (Penetration Testing)" Last accessed on 2 January 2015, http://searchsoftwarequality.techtarget.com/definition/penetration-testing.

[47] Margaret Rouse. (December 2014). *TechTarget.* "Security Information and Event Management (SIEM)." Last accessed on 19 February 2015, http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM.

[48] Margaret Rouse. (September 2005). *TechTarget.* "Two-Factor Authentication (2FA)." Last accessed on 3 January 2015, http://searchsecurity.techtarget.com/definition/two-factor-authentication.

[49] Margaret Rouse. (October 2014). *TechTarget.* "Virtual Machine." Last accessed on 19 February 2015, http://searchservervirtualization.techtarget.com/definition/virtual-machine.

[50] Tom Gara. (6 February 2014). *The Wall Street Journal.* "October 2015: The End of the Swipe-and-Sign Credit Card." Last accessed on 13 January 2015, http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/.

[51] Robin Sidel. (4 January 2015). *The Wall Street Journal.* "Why New Credit Cards May Fall Short on Fraud Control." Last accessed on 13 January 2015, http://www.wsj.com/articles/why-new-credit-cards-may-fall-short-on-fraud-control-1420423917.

[52] Home Depot. (6 November 2014). *FAQs.* "November 6th Email Announcement." Last accessed on 14 January 2015, https://corporate.homedepot.com/MediaCenter/Documents/FAQs.pdf.

[53] Lysa Myers. (3 April 2014). *WeLiveSecurity.* "What Is EMV, and Why Is It Such a Hot Topic?" Last accessed on 14 January 2015, http://www.welivesecurity.com/2014/04/03/what-is-emv-and-why-is-it-such-a-hot-

topic/.

[54] Brian Krebs. (14 October 2014). *Krebs on Security.* "'Replay' Attacks Spoof Chip Card Charges." Last accessed on 14 January 2015, http://krebsonsecurity.com/2014/10/replay-attacks-spoof-chip-card-charges/.

[55] Steven Murdoch, Saar Drimer, Ross Anderson, and Mike Bond. (25 July 2014). "Chip and PIN Is Broken." Last accessed on 14 January 2015, http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf.

[56] Level_admin. (31 January 2011). *Level2Kernel Blog.* "Contactless Card Payment Specifications." Last accessed on 14 January 2015, http://blog.level2kernel.com/contactless-card-payment-specifications/.

[57] Andy Greenberg. (30 January 2012). *Forbes.* "Hacker's Demo Shows How Easily Credit Cards Can Be Read Through Clothes and Wallets." Last accessed on 15 January 2015, http://www.forbes.com/sites/andygreenberg/2012/01/30/hackers-demo-shows-how-easily-credit-cards-can-be-read-through-clothes-and-wallets/.

[58] NFC Admin. (2 April 2012). *Near Field Communication and Mobile Technology Provided by Professionals.* "How to Read a Contactless Credit Card Such as Visa payWave or MasterCard PayPass." Last accessed on 15 January 2015, http://www.nfc.cc/2012/04/02/android-app-reads-paypass-and-paywave-creditcards/.

[59] Forthwrite Media SARL and NFC Times. (2013). *NFC Times.* "Japan: DoCoMo Drives Nationwide Rollout of Contactless Wallet Phones." Last accessed on 15 January 2015, http://nfctimes.com/project/japan-docomo-drives-nationwide-rollout-contactless-wallet-phones.

[60] Smart Card Alliance. (2015). *Smart Card Alliance.* "NFC Frequently Asked Questions." Last accessed on 15 January 2015, http://www.smartcardalliance.org/publications-nfc-frequently-asked-questions/.

[61] Sharon Profis. (5 September 2014). *CNET.* "Everything You Need to Know About NFC and Mobile Payments." Last accessed on 15 January 2015, http://www.cnet.com/how-to/how-nfc-works-and-mobile-payments/.

[62] Smart Card Alliance. (October 2014). "Technologies for Payment Fraud Prevention: EMV, Encryption, and Tokenization." Last accessed on 15 January 2015, http://www.smartcardalliance.org/wp-content/uploads/EMV-Tokenization-Encryption-WP-v51-102414-FINAL-clean.pdf.

[63] Eurotechnology Japan. (18 September 2014). *Eurotechnology Japan.* "ApplePay Vs. Osaifu-Keitai." Last accessed on 15 January 2015, http://www.eurotechnology.com/2014/09/18/applepay-vs-osaifu-keitai-cnbc/.

[64] Intel Corporation. (October 2014). *Intel.* "Intel Data Protection Technology for Transactions." Last accessed on 17 January 2015, http://www.intel.com/content/www/us/en/embedded/technology/security/secure-payment-transactions/overview.html.

[65] Intel Corporation. (October 2014). *Intel.* "Video: Intel Data Protection Technology for Transactions." Last accessed on 17 January 2015, http://www.intel.com/content/www/us/en/embedded/technology/security/secure-payment-transactions/overview-video.html.

[66] Bob Russo. (4 March 2014). "Statement for the Record: Can Technology Protect Americans from International Cybercriminals?" Last accessed on 14 January 2015, https://www.pcisecuritystandards.org/pdfs/PCI_-_House_Science_Committee_Testimony_%28Bob_Russo%29_3-4-14_-_Final.pdf.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud

225 E. John Carpenter Freeway
Suite 1500
Irving, Texas
75062 U.S.A.

Phone: +1.817.569,8900