GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Point of Sale (POS) Systems and Security

GIAC (GSEC) Gold Certification

Author: Wes Whitteker, wes_whitt@yahoo.com

Advisor: Hamed Khiabani, Ph.D.

Accepted: August 4th 2014

Abstract

With the Target Corporation breach as the main example, the last year has seen several POS systems compromised by bad actors. In many cases, these environments were PCI-DSS compliant. If the information security standard organization's use for securing POS systems isn't achieving the desired goal of stopping, or reducing, the impact of a data breach, something must be done – an "Offense must inform Defense Approach". Thus, this paper provides a comprehensive overview of the common POS environments, bad actor attack methods, and a mapping of data-driven best practices to the Council on CyberSecurity's 20 Critical Security Controls for Effective Cyber Defense.

© 2014 SANS Institute, Author retains full rights.

© 2014 The SANS Institute Author retains full rights.

1. Introduction

As Dr. Eric Cole (2014) mentioned in a recent SANS SEC401: Security Essentials Bootcamp Style course, "2014 will be the year of the retailer". Over the last several months, several retail organizations have been victims of information security breaches targeting consumer payment card data. The most notable of these was the Target corporation breach. However, several other retail organizations have also been victims of payment card data theft over the past year to include Michaels Stores, Inc., Sally Beauty Holdings, Inc., and Neiman Marcus (Harris, 2014; Tate, 2014; Zetter, 2014). This is certainly not an all-inclusive list of retailers that have experienced payment card data theft in recent months. There are several additional examples within retail as well as other markets (e.g. Food and Beverage, Hospitality, Healthcare, etc.) (Identity Theft Resource Center, 2014). However, the resources available to the breached organizations compared to the level of bad actor success paints a picture that more needs to be done to protect consumer payment card data.

The primary motivator for the payment card data breaches is profit, and the primary target (no pun intended) is payment card data (Trustwave Holdings, Inc., 2014; Team Cymru, 2013). Although, Personally Identifiable Information (PII) is also collected during many payment card data breaches, it's less desirable to an attacker because it's harder and riskier to use (Trustwave Holdings, Inc., 2013, p. 8). In general, thieves steal the card data and sell it to "dump shops" who then sell it to buyers (Krebs, 2014). Dump Shops are underground stores that advertise and sell stolen payment card data. One such example of a Dump Shop is McDumpals. McDumpals not only sells payment card data, it also allows the consumer to filter the card data by geographical

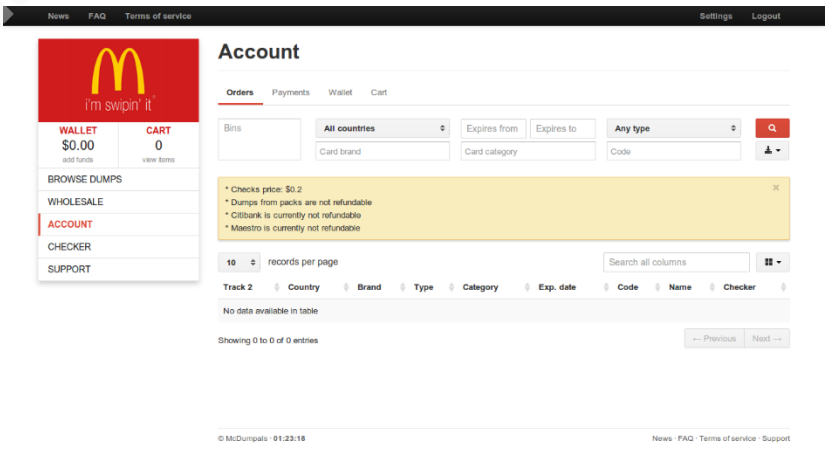


Figure 1: Screenshot of McDumpals User Account Screen (Patrick, 2014)

Wes Whitteker, wes_whitt@yahoo.com

© 2014 The SANS Institute Author retains full rights.

location, which improves the users' chances of successfully using the card data (i.e. "Cashing Out") (Krebs, 2014).

The Payment Card Industry Data Security Standard (PCI DSS) is the main payment card industry information security standard. It was created in 2006 by the PCI security standards council (SSC). The PCI SSC is led by members of the five global payment card brands to include American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. (PCI Security Standards Council, LLC., 2014). PCI DSS was a good starting point when no other security standard existed, but due to the continued increase in payment card data breaches, it's obvious there's room for an improved standard. On January 1, 2014, version 3 of PCI DSS went into effect (2.0 compliant organizations have until January 2015 to comply with the new standards). This update shows that even the PCI SSC has recognized the evolving security landscape and is continuing to evolve the DSS (Freed, 2013; Moyle, 2013; PCI Security Standards Council, LLC., 2013a; PCI Security Standards Council, LLC., 2013b). However, even with the use of the PCI DSS, there's significant weakness in the payment card security architecture. According to Gomzin (2014):

> PA-DSS and PCI DSS, even if implemented in full, provide minimal to no protection against threats in the three (out of four) payment application key vulnerabilities: data in memory, data in transit, application code and configuration. Both PA-DSS and PCI DSS facilitate significant (but not full) protection in one of these four key vulnerability areas—data at rest—if the software vendor implements strong cryptographic mechanisms.

To this end, Mandiant (2014) states in their M-Trends 2014 Beyond the Breach report with respect to POS environments that "Each of the victims which Mandiant responded to in 2013 operated a PCI-compliant environment". With an understanding that POS system security needs to be improved, this paper will offer another perspective on POS system security. This paper will provide an overview of payment card systems and attack methods, and will offer suggestions for leveraging the Council on CyberSecurity's 20 Critical Controls, a standard that uses an "offense must inform defense approach" (Whitehouse, 2009, p.3), to protect payment card information.

© 2014 The SANS Institute Author retains full rights.

2. What are Point of Sale systems?

2.1 History

The term Point of Sale (POS) is used to describe the technology used by a consumer to provide their payment information in exchange for a good or service. POS technology has actually been around for many years with the first cash register dating back to 1879 (Abell, 2009). However, it wasn't until the mid-70s that this technology was converted from a mechanical to an electrical form. In the 1980s, the technology was advanced again to leverage modern day personal computing (PC) technology. Over the next several years, support for barcode scanning and payment card reading was added. Today, the most familiar example of a POS system would be the check-out counter at a retail or grocery store. However, there are many more forms of point of sale systems used in many business types (Posmatic, n.d.).

2.2 Stakeholders

Today's POS systems consist of many of the same components that are found in traditional information systems. One of the key differences between POS systems and other information systems is its stakeholders. The primary stakeholders for today's POS systems are as follows: consumers, merchants, acquirer, issuer, card brand companies, payment processors, payment gateways, software vendors, and hardware vendors. A consumer is those people that use payment cards for the purchase of goods (most humans). Merchants are businesses who accept payment cards as a form payment for goods and services. Merchants are also the implementers of the POS systems (Gomzin, 2014, Key Players).

An acquirer, also referred to as an acquiring bank, handles authorization requests from payment processors and settles the transaction with the card issuer. Issuers provide the cards to consumers and maintain the payment card accounts. Card Brands, also referred to as card networks (e.g. VisaNet), manage the overall process of authorization and settlement (Gomzin, 2014, Key Players).

Payment gateways, though they're not always used, provide the ability to switch between

© 2014 The SANS Institute Author retains full rights.

payment processors without having to make significant changes to a store's payment application. Software vendors provide the payment application and other software used in the payment process. A payment processor receives transactions from merchants and then contacts the proper acquirer (i.e. a middle man). Hardware manufacturers develop the pinpads and magnetic stripe readers (MSR) that most of us have used at a brick and mortar store (Gomzin, 2014, More Players).

2.3 Software and Hardware

Two additional unique areas of the payment card system to discuss are the "frontline" software and hardware;specifically, payment applications, magnetic strip readers (MSRs), and personal identification number (PIN) pads. A payment application (PA) is the software that is situated between the in store hardware and the payment processors. According to Gomzin (2014), "PA implements all functions associated with acceptance, processing, storage, and transmission of sensitive card data" (Glossary).

The two primary ways card data is ingested into the POS system is through MSRs and PIN pads. MSRs are the pieces of hardware that most of us have used at a store to swipe our payment card when paying for a good or service. PIN pads are just that, a piece of hardware used to enter a PIN. PIN pads are referred to as a point of interaction (POI) device when it's combined with additional functions such as MSR capabilities, displays, and peripheral support (Gomzin, 2014, Card Entry Methods). It's worth noting that both software vendors and hardware manufacturers are rarely discussed as unique entities when describing the payment processing life-cycle even though they are both held to independent PCI standards, PCI-Payment Application (PA) and PCI-PIN Transaction Security (PTS), respectively (PCI Security Standards Council, LLC., n.d.).

2.4 Payment Cards

2.4.1 History

Payment card existence can be traced back to the 1940s, although the electronic systems in use today date back to the mid to late 1980s. As such, throughout the course of time, several

© 2014 The SANS Institute Author retains full rights.

categories of payment cards developed. Today, payment cards can come in single-use or multi-use forms (i.e. credit & debit). The main payment card types are Credit and Debit. A credit card is nothing more than a link to a line of credit provided to a customer from a financial institution. A debit card is linked to a customer's (i.e. consumer or business) actual account that contains funds for purchases (Mastercard Worldwide, n.d.).

There are several other sub categories of cards such as prepaid, fleet, etc. The sub categories are tailored for a specific use. For example, a fleet card wouldn't be authorized for use at an ATM or online (Gomzin, 2014, Payment Cards). At this point it's worth noting that there's a technology referred to as Europay Mastercard and Visa (EMV), which has been used globally, with the exception of the US, for many years. It's now being actively adopted within the US and is being touted by some as the saving grace for payment card security mainly due its ability to prevent card cloning (Hawes, 2013; Smart Card Alliance, n.d.). However, as always, the devil is in the details and this technology also has several security issues. (Bjorhus, 2014; Schwartz, 2014; Roberts, 2012).

2.4.2 Physical Card Architecture

Since the payment card contains the targeted information, it's imperative that security professionals have a firm understanding of the card architecture. Payment cards consist of both physical and logical (i.e. Magnetic Stripe Data) components. From a physical perspective, the card consists of the payment brand logo, background color, image, embossed Primary Account Number (PAN), expiration date, cardholder name, card verification value (CVV2), ultraviolet (UV) marks, customer service phone numbers, metallic tipping (optional), cardholder signature (optional), cardholder photo

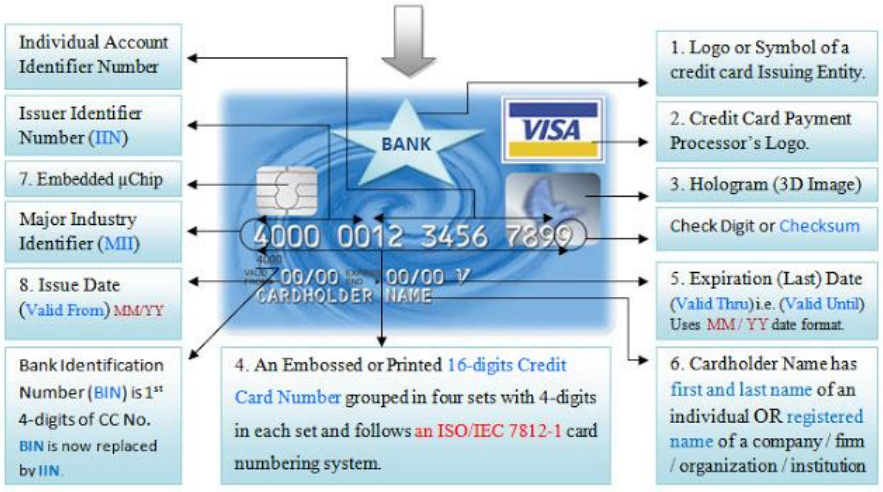


Figure 2: Front-side payment card physical structure (Akrani, 2012)

© 2014 The SANS Institute Author retains full rights.

(optional), hologram (optional), and a holographic magnetic stripe (optional). The point to remember with all these features is that they were designed with an intended security purpose in mind but can be bypassed. The ineffectiveness of these security features is due to the fact that counterfeiting is very cheap; the industry lacks a standard in card design; and much of the mechanisms rely on human validation (i.e. a cashier who doesn't have the time or training to validate every card he/she processes) (Gomzin, 2014, Physical Structure and Security Features).

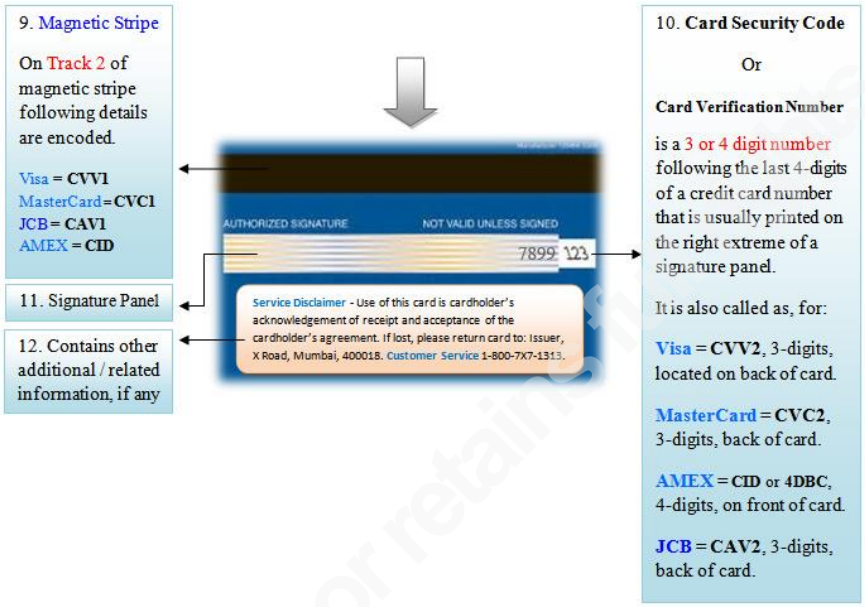


Figure 3: Backside payment card physical structure (Akrani, 2012)

The magnetic stripe of the payment card holds the majority of the critical data. The information on magnetic stripe of the card is broken up into 3 areas referred to as "tracks". Tracks 1 and 2, which are standardized under ISO/IEC 7813, are the focus for payment card usage (and bad actors). Track 3 is covered under ISO/IEC 4909 (Gundert, 2014; ISO, n.d.). Track 1 and 2 data on the magnetic stripe is not encrypted, which allows for easy duplication of a card as well as easy retrieval by thieves should the card be stolen. Track one, which has a maximum length of 79 bytes (i.e. 79 ASCII characters), has

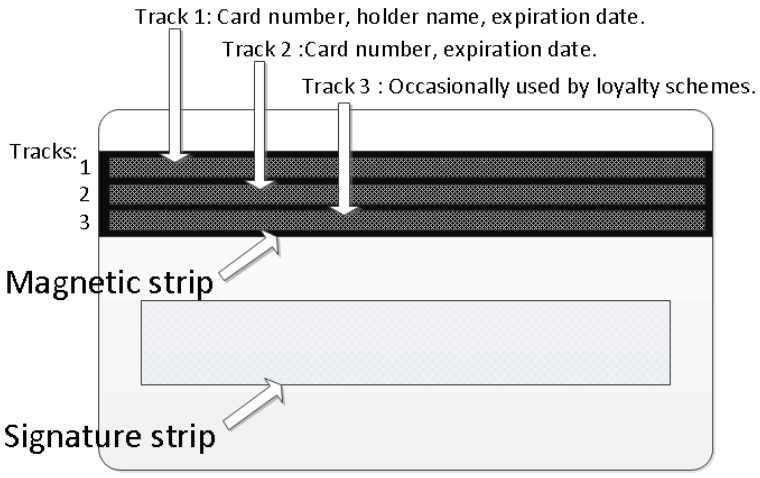


Figure 4: Track data arrangement on magnetic strip (Gundert, 2014)

© 2014 The SANS Institute Author retains full rights.

several main components to include the start sentinel character (always %), format code, PAN, field separator (always ^), name (last/first), field separator (always ^), expiration data, service code, discretionary data, end sentinel, and the longitudinal redundancy check (LRC) (Q-Card, n.d.).

Track 2, which has a maximum length of 40 bytes (i.e. 40 ASCII characters), has several main components to include the start sentinel character (always %), format code, PAN, field separator (always ^), name (last/first), field separator (always ^), expiration data, service code, discretionary data, end sentinel, and the longitudinal redundancy check (LRC) (Q-Card, n.d.).

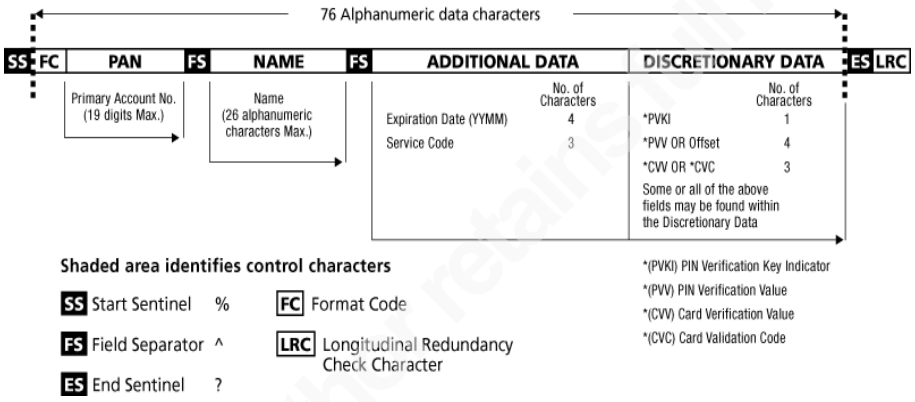


Figure 5: Track 1 Graphical Depiction (Q-Card, n.d.)

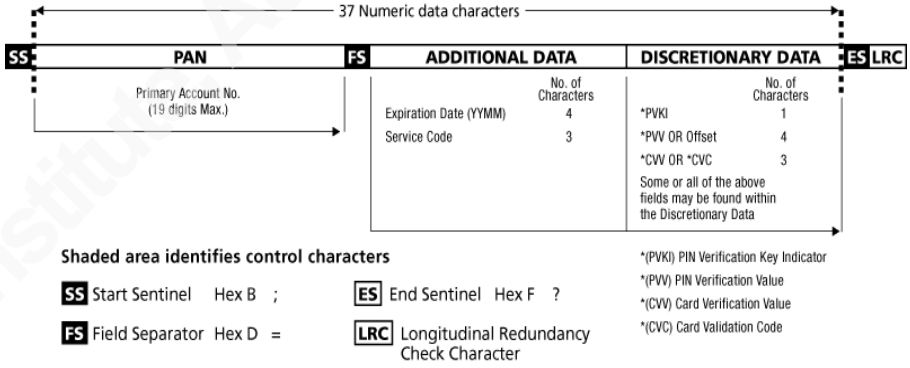


Figure 6: Track 2 Graphical Depiction (Q-Card, n.d.)

2.5 System Deployment Models

Now that the basic components of the POS system have been covered, it's time to look at POS systems with a complete payment system. There are several categories of electronic payment system (EPS) deployment models to discuss including the Store EPS Deployment Model; the POS EPS Deployment Model; the Hybrid/POS Store Deployment Model; the Gas Station Payment System; and the Mobile Payments [Near Field Communication (NFC) and Non-

© 2014 The SANS Institute Author retains full rights.

NFC]. To provide context for this discussion, it is important to understand that an EPS is a separate function from the typical POS function, although the EPS and POS system could be co-located on the same machine. In general, the EPS performs all the payment processing while the POS system is the tool used by the Cashier or Consumer (e.g. self-checkout kiosk for the consumer) (Gomzin, 2014, Deployment of Payment Applications).

When looking at the systems, it's valuable to follow the path the payment card data takes because the data is what's valuable to a bad actor. The payment data enters the system via the POI device and then makes its way through processing – as seen in the diagrams below.

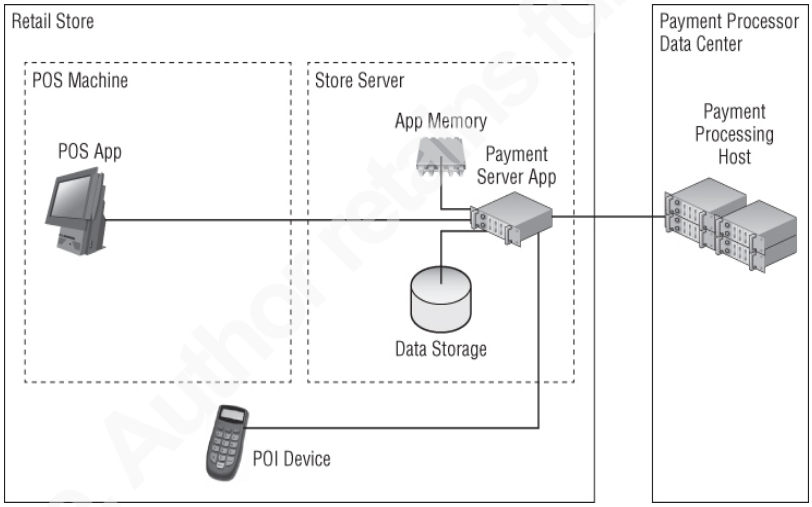


Figure 7: Store EPS Deployment Model (Gomzin, 2014, Deployment of Payment Applications)

In a store EPS deployment model, the POS and EPS functions are located on separate machines. Essentially, the EPS is serving as a "middle-man", which prevents any sensitive data from entering the actual POS system. As you can see in the image to the right, the POI device connects directly to the EPS (i.e. Store Server) instead of the POS machine. In a POS EPS deployment model, the POS function and the EPS function are both on the same system. This places payment processing function on the actual POS machine. Thus, the POS machine is exposed to sensitive data in this model. In a hybrid/POS store deployment model, the EPS functions are broken up

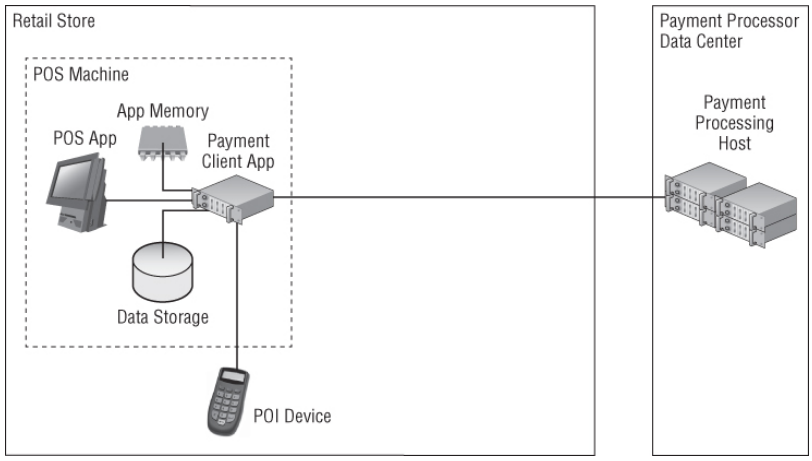


Figure 8: POS EPS Deployment Model (Gomzin, 2014, Deployment of Payment Applications)

© 2014 The SANS Institute Author retains full rights.

across multiple systems. In this model, multiple machines are exposed to sensitive data creating multiple targets of opportunity for the bad guys (Gomzin, 2014, Deployment of Payment Applications).

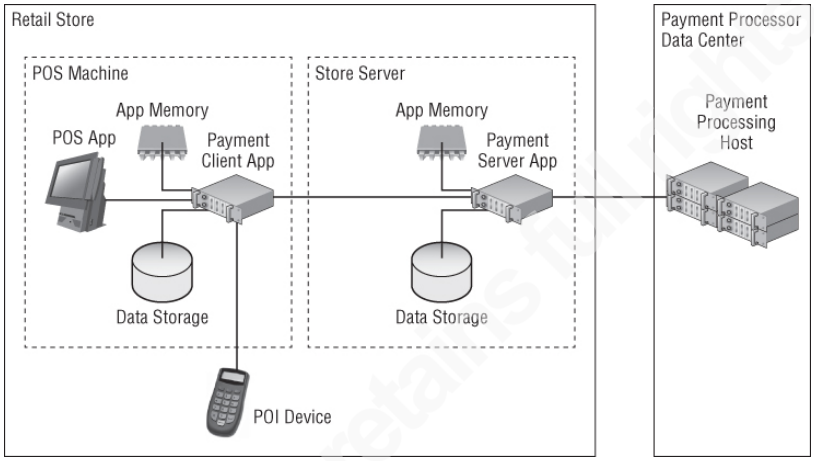


Figure 9: Hybrid/POS Store Deployment Model (Gomzin, 2014, Deployment of Payment Applications)

The deployment models discussed and depicted so far represent the POS systems seen in most retail stores. However, it's worth mentioning that there are other deployment models that don't fit into the categories above such as gas station payment systems and mobile payments (e.g. NFC). The primary differences between these models and the ones mentioned are that there are a few different pieces of software (e.g. mobile apps) and hardware (e.g. mobile phone, fueling pump) (Gomzin, 2014, Deployment of Payment Applications).

2.6 Process

With a firm understanding of the overall POS system's technologies and people (i.e. stakeholders), the final area to look at before digging into the cyber security details is the actual payment process. In general, there are two main payment processing stages: authorization and settlement. Authorization is a term used to represent the state of the payment process to the point where the purchase is

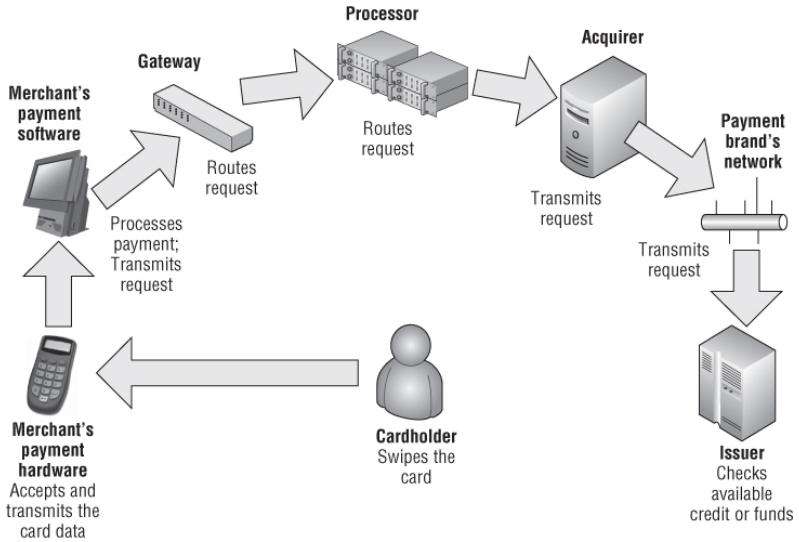


Figure 10: POS Authorization Process (Gomzin, 2014, Payment Stages)

© 2014 The SANS Institute Author retains full rights.

finalized. This stage is where most attacks occur as the payment card data (track 1, track 2, or both) is sent through the entire system (Gomzin, 2014, Payment Stages).

Settlement is a term used to represent what happens after the sale to settle the account balances between all parties (i.e. merchant, acquirer, and issuer). Though this stage is not normally thought of as a vulnerable stage, there is some weakness in the fact that most store transactions are stored at the store for a set period of time in a large group known as a batch (Gomzin, 2014, Payment Stages). Granted, this data (normally the Primary Account Number) isn't as valuable as the data used during the authorization stage, it's still sensitive in nature. If you couple this sensitivity with the fact that it can be retrieved in mass quantities relative to the authorization phase, it serves as another viable target for the bad actors.

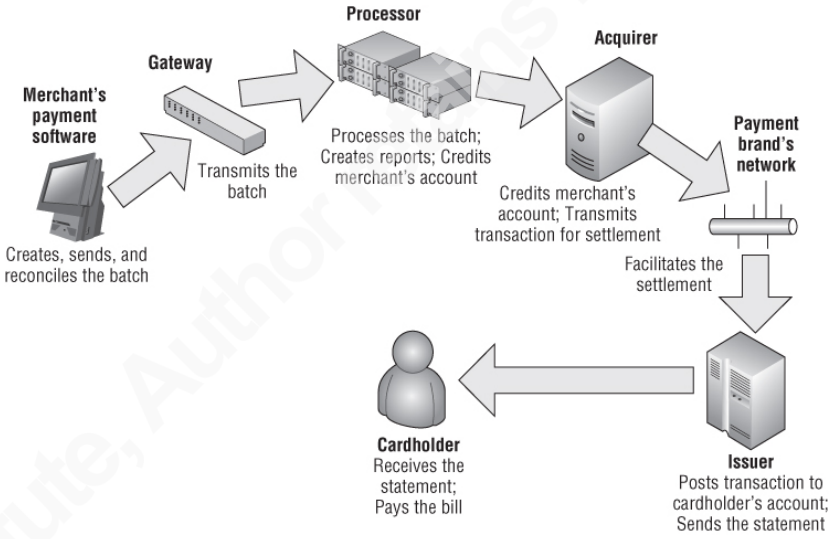


Figure 11: POS Settlement Process (Gomzin, 2014, Payment Stages)

3. Attack Methodology

Although POS breaches are declining (Verizon, 2014, p. 16), they still remain an extremely lucrative endeavor for criminals (Mandiant, 2014, p. 14). As such, with a firm understanding of the people, processes, and technologies involved in the retail payment card market, it's time to take a deeper look at POS information security breaches. This section will cover POS data vulnerabilities, attack methods (including common malware types), and the phases of POS breaches.

3.1 Data Vulnerabilities

© 2014 The SANS Institute Author retains full rights.

With respect to POS data vulnerabilities, there are three specific areas that should be given attention including data in memory; data in transit; data at rest. Data in memory in this context is when the card track data is brought into the system at the POS system via a POI (or some other input device). Data in memory is nearly impossible to defend if an attacker has access to the POS system.

Traditionally, data input into the POS system was in memory in the clear, which is what allowed attackers' memory scrapers to be very successful. The way to minimize this risk is by encrypting the card data ASAP and keeping it encrypted as much as possible through its life within the system. Point to Point Encryption (P2PE) is a technical feature that can be taken to address the issue of encrypting data in memory (Gomzin, 2014, Data in Memory).

Data in transit in this context would be the data that's passed via the network connections between the systems that process the payment card data. By not encrypting the data that is transmitted, it offers an attacker another point where they could capture easily usable payment card data. The technologies that are normally used for addressing the data in transit vulnerability include the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) and IPsec (Gomzin, 2014, Data in Transit).

Data at rest in this context would be anytime the card data is stored somewhere within the entire system other than a form of primary storage (i.e. system memory, cache, etc.). The best option for defending against data at rest attacks is to not store the data. P2PE would be the next option with direct symmetric encryption of the data as a last resort (Gomzin, 2014, Data at Rest).

3.2 Attack Methods

Understanding the areas where card data is vulnerable provides the context to look at some of the attack methods that have been used by bad actors for intercepting payment card data within the POS system (Trend Micro Inc., 2014; Trust Wave Holdings Inc., 2013). The methods covered include skimming, supply chain integrity, memory scraping (including specific malware), forcing offline authorization, attacking the application, sniffing, 3rd party usage, and crimeware kit usage.

© 2014 The SANS Institute Author retains full rights.

Skimming has been an attack method that has been around for a while. It's a scenario where the POI components of POS system are replaced by a bad actor. When the unsuspecting consumer uses these devices, their data is captured. There are some risks from the bad actor's perspective (i.e. physical presence at the POS location) but with the growth in P2PE, this may become a more viable option (Gomzin, 2014, Exploiting Other Vulnerabilities).

There have been several cases where POS systems have been purchased with vulnerable or misconfigured software. In these cases, the attackers find the software and leverage it for access to the POS system. If you consider a small business or franchise that doesn't have the resources of a large retailer, they may not consider what's "inside" the system, thus the system shows up to their store and they install it without an awareness of the potential information security concerns (MacWillson, 2012).

Memory scraping has become a popular choice among bad actors (i.e. Target and Neiman Marcus). Scrapers are very opportunistic in that they can be can be tailored to target specific patterns of data (i.e. track data) or they can simply grab all data. Further, they don't require information on the environment where they will be emplaced, they're system agnostic. The bottom line is that they are a simple yet extremely effective attack choice (Schwartz, 2014a).

Just like standard viruses, POS malware doesn't have a single, well-defined, taxonomy (Microsoft, n.d.; Kapersky Lab, n.d.). However, there are several specific POS malware families to include but not limited to Alina, Dexter, vSkimmer, FYSNA, Decebel, and BlackPOS (Team Cymru, 2013; Trend Micro Inc., 2014). It's important to be familiar with the family behaviors to understand how best to defend against them. In general, all of these families inject themselves into memory, collect the desired information (i.e. track data), exfiltrate the data to another system, and use a C&C system (Mandiant, 2014; Team Cymru, 2013; Trend Micro Inc., 2014).

The POS malware families are extremely opportunistic and in many cases aren't detectable with traditional antivirus detection. In most cases, the captured data is exfiltrated from the POS system to another system within the targeted environment for aggregation and uploaded to a remote system, thus reducing the chances of detection. These families continue to evolve as evasion techniques improve with several versions of each family in existence

© 2014 The SANS Institute Author retains full rights.

(Mandiant, 2014; Trend Micro Inc., 2014; Trust Wave Holdings, Inc., 2013).

In a forced offline authorization attack the attacker would create DOS for the local retail network to go offline, which would "force" the PA to locally authenticate payment card information. Local authentication is traditionally less robust and stores all transactions locally until the network is brought back online. By forcing the location to store all the transactions locally, this creates an opportunity for the bad actor to easily collect all the transaction information (Gomzin, 2014, Attacks on Availability and Integrity).

Abusing remote access is another method used to attack POS systems. The level of access could be complete desktop control, or a basic command and control (C&C) channel (Trust Wave Holdings, 2013, p. 12).

The payment applications themselves are also vulnerable to several attack types such as Application Programming Interface (API) abuse, tampering, disassembling, and spoofing. In API attacks, lack of access control implemented on the PA's API is exploited to retrieve sensitive card data. In tampering attacks, PA configuration files, to include updates, could be manipulated to support the attacker's malicious efforts. Disassembling is in reference to the ability to reverse engineer the POS firmware and payment application software in an effort to replace it with functionality of the attacker's choosing. Spoofing is a scenario where the authentication credentials for a communication channel are used to "spoof" the identity of the attacker, which allows the attacker to impersonate the client or the server in the POS system (Gomzin, 2014, Exploiting Other Vulnerabilities).

Sniffing is nothing new. Attackers have been doing sniffing since the dawn of time. However, sniffing is another method that can be used to capture card data. It's nothing more than collecting network traffic and analyzing it for payment card track data (Gomzin, 2014, Sniffing).

Input hooking is a category of attack where the input provided from a user is intercepted at the OS or system level (as opposed to a physical key logging device). This is possible because in most cases the POS input device input to the system appears as keyboard data. For example, Microsoft Windows uses the Human Interface Device (HID) API for input device interfacing.

© 2014 The SANS Institute Author retains full rights.

It's essentially a driver suite for connecting various input devices to a windows system. Thus, compromising this library would allow all user input to be collected (Trust Wave Holdings, 2013, p. 18).

As seen in the Target breach, 3rd parties to organizations can be a weak link in an organizations data security armor (Poulin, 2014). Many 3rd parties (i.e. small businesses) think that they will not be a target of an attacker, which creates a false sense of security. This false sense of security, many times, results in less focus on information security measures that the bad actor will leverage for their advantage (Levin, 2014).

Though not a specific "attack", crimeware kits are often seen as the main creators of the command and control setup used in credit card breaches (Prolexic, 2014). Crimeware kits allow the not-so-technical person to create a highly technical attack. In addition to their ease of use, it's important to know that an ecosystem of crimeware kits, including continued support, is being used by bad actors. These kits are sold on the digital underground for several thousands of dollars. Essentially, crimeware kits have commoditized the compromising of an environment because they have reduced the barrier to entry for those motivated to use it (Trust Wave Holdigns Inc., 2013).

3.3 Basic POS Breach Phases

With an understanding of the POS system architectures and various attack methods, the basis has been provided to look at the general POS breach phases. As with most basic pentesting methodologies, POS breach phases don't necessarily have to happen in any particular order but generally there is some consistency in the methodology. The phases include infiltration, propagation, aggregation, and exfiltration (Trustwave Holdings Inc., 2013).

The infiltration phase is where the attacker collects information on the target environment (i.e. reconnaissance) in an effort to find access. Once access is found, it's exploited and the attacker then creates a more permanent foothold in the environment (i.e. a beachhead) normally using a stealthy trojan (Mandiant, 2014; Trustwave Holdings Inc., 2013). After the infiltration phase, the bad actor moves to spread malware to the target systems (i.e. POS systems). This

© 2014 The SANS Institute Author retains full rights.

propagation of malware is often done leveraging existing resources in the target environment (e.g. domain controllers, remote administration tools, etc.) (Mandiant, 2014; Trustwave Holdings Inc., 2013).

After the malware is propagated to the targeted systems, it will often send the desired information to a single point (i.e. pivot machine) within the environment for aggregation and exfiltration. However, the data could also be sent directly from the target machine to a single point outside the environment -- exfiltrating the information before aggregating it (Mandiant, 2014; Trustwave Holdings Inc., 2013).

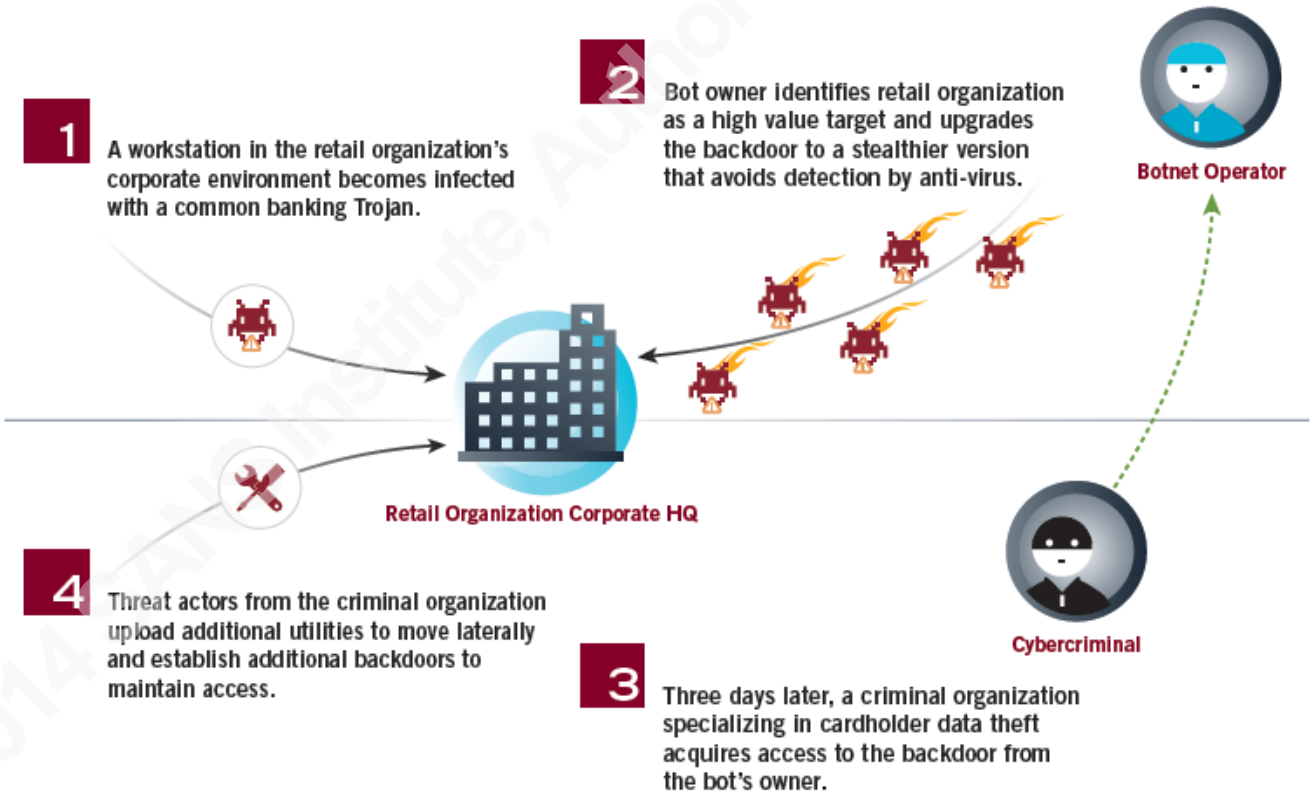


Figure 12: Depiction of gaining access to POS environment (Mandiant, 2014)

© 2014 The SANS Institute Author retains full rights.

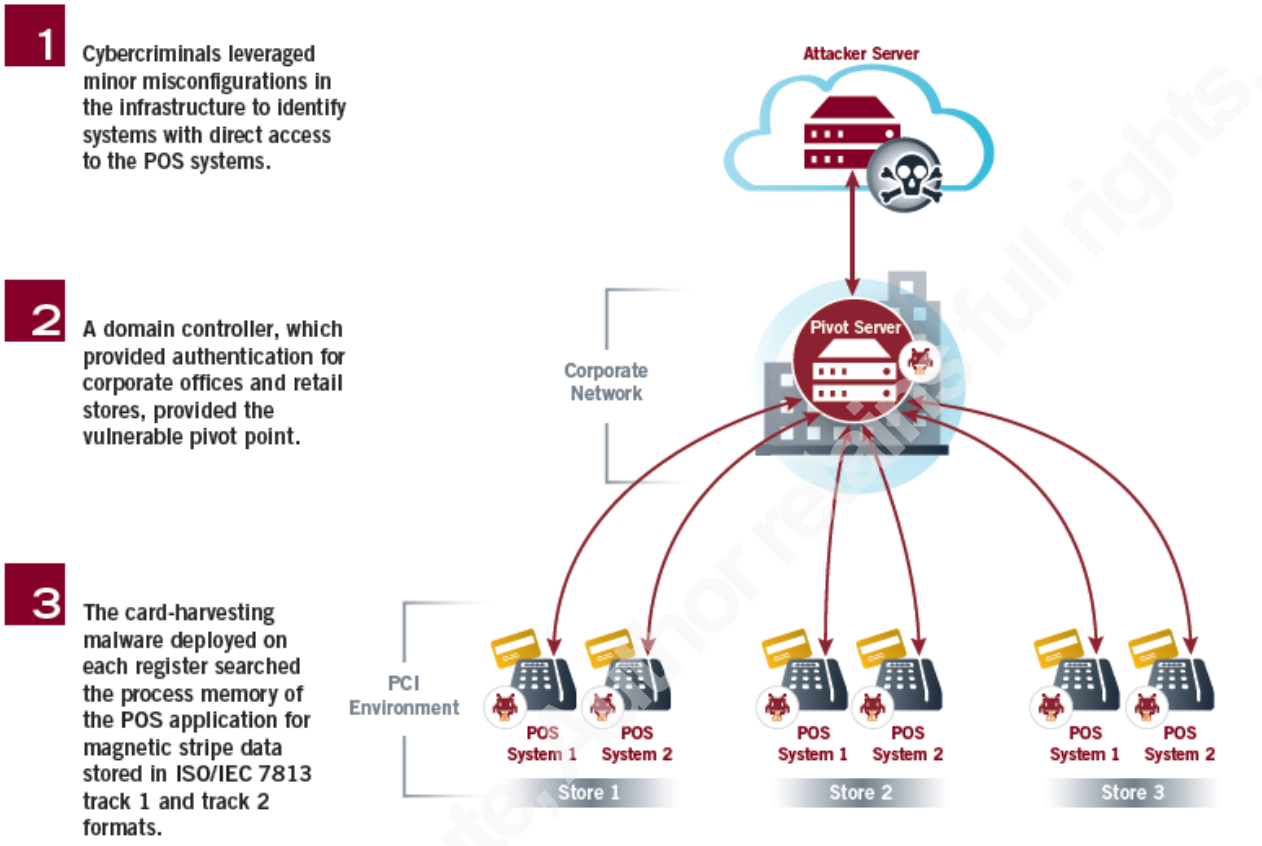


Figure 13: Depiction of Spreading Malware to POS targets (Mandiant, 2014)

4. Critical Security Controls Applicability

As noted previously, several of the compromised POS environments were PCI compliant, thus there's a gap between the PCI compliance process and what bad actors are actually doing. To this end, with an understanding of the POS architecture as well as the attack methodology, recommended best practices based on actual threat data can be derived using the Council on Cyber Security's 20 Critical Controls for Effective Cyber Defense (formerly maintained by the SANS Institute) (Council on CyberSecurity, n.d.).

As such, Appendix A contains a table that shows recommended best practices from organizations such as the US-CERT (2014), Mandiant (2014), Trustwave Holdings Inc. (2013), Verizon (2014), and Trend Micro Inc. (2014) mapped to the applicable CSCs. Note that this

© 2014 The SANS Institute Author retains full rights.

isn't an all-encompassing list of security controls that could be implemented in a POS environment but rather a set of controls that are based on POS incident data – an "offense must inform defense approach" (Whitehouse, 2009, p. 3).

5. Conclusion

It's no secret that thoroughly understanding your environment and its vulnerabilities serve as a catalyst for implementing effective security controls (whatever the control standard). As time marches into the future it's inevitable that more payment card data breaches will be exposed. These exposures will take place in those organizations that thought they understood their environment and the information security standard they were holding themselves to was sufficient, in this case PCI-DSS.

In most cases, the details of the POS breaches aren't shared with the public. Unfortunately, this results in a knowledge gap for organizations that haven't yet suffered a breach, or don't know they have suffered a breach. The PCI SSC has done a good job at putting a standard in place for organizations to follow when nothing else existed but struggles with implementation consistency and keeping pace with the latest threat landscape. Further, there's irony in leveraging a static standard for a knowledge domain (hacking) that embraces openness and innovative thought.

Organizations need more than the PCI-DSS compliance stamp. The 20 CSCs can fill this gap. They are easy to understand and have a level of proven effectiveness in organizations since they have been designed with an offense must inform defense approach. Further, they are supported by a joint international community of information security professionals from various business environments, which provides a broad perspective throughout their continued development.

© 2014 The SANS Institute Author retains full rights.

References

Abell, J.C. (2009, November 4). Nov. 4, 1879: Ka-Ching! The World's First Cash Register. *Wired*. Retrieved from http://www.wired.com/2009/11/1104ritty-cash-register/

Akrani, G. (2012, January 16). *What is a credit card? Meaning Definition Size Anatomy Glossary*. Retrieved from http://kalyan-city.blogspot.com/2012/01/what-is-credit-card-meaning-definition.html

Bjorhus, J. (2014, January 19). Next-generation credit cards aren't foolproof. *Star Tribune*. Retrieved from http://www.startribune.com/business/241031161.html

Cole, Dr. E. (2014, February 6). SEC401: Security Essentials Bootcamp Style. *SEC401.1-01: Networking Concepts Podcast*. Podcast retrieved from https://www.sans.org/self-study.php

Council on CyberSecurity. (n.d.). The Critical Security Controls for Effective Cyber Defense: Version 5.0. Retrieved from http://www.counciloncybersecurity.org/critical-controls/reports/

Freed, A.M. (2013, December 5). PCI DSS 3.0 – What's New? An Infographic…. *The state of security: News. Trends. Insights*. Retrieved from http://www.tripwire.com/state-of-security/regulatory-compliance/pci-dss-3-0-whats-new-infographic/

Gomzin, S. (2014). *Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions*. Available from https://www.safaribooksonline.com/

Gundert, L. (2014, January 13). *Detecting Payment Card Data Breaches Today to Avoid Becoming Tomorrow's Headline*. Retrieved fromhttp://blogs.cisco.com/security/detecting-payment-card-data-breaches-today-to-avoid-becoming-tomorrows-headline/

Harris, E.A. (2014, April 18). Michaels Stores' Breach Involved 3 Million Customers. *The New*

© 2014 The SANS Institute Author retains full rights.

York Times. Retrieved from http://www.nytimes.com/2014/04/19/business/michaels-stores-confirms-breach-involving-three-million-customers.html?_r=0

Hawes, J. (2013, May 8). Lack of Chip and PIN technology leaves US shoppers and diners at risk from hackers. *Naked Security*. http://nakedsecurity.sophos.com/2013/05/08/lack-of-chip-and-pin-technology-leaves-us-shoppers-and-diners-at-risk-from-hackers/

Identity Theft Resource Center. (2014). *Identity Theft Resource Center Breach Report*. Retrieved from http://www.idtheftcenter.org/images/breach/ITRC_Breach_Report_2014.pdf

International Standards Organization. (n.d.) ISO/IEC 4909:2006 Identification cards – Financial transaction cards -- Magnetic stripe data content for track 3. Retrieved from http://www.iso.org/iso/catalogue_detail.htm?csnumber=43309&ei=_kizUabZDvfi4AO9_IDAAQ&usg=AFQjCNHwqVa43v1NX_L9Tm5OlvuqRPZ2YA&sig2=X-RjSmISXB6cMP3k7wtlvA

Kapersky Lab. (n.d.) Type of Malware. Retrieved from http://usa.kaspersky.com/internet security-center/threats/malware-classifications#.U755xLEe8SR

Krebs, B. (2014, June). Peek Inside a Professional Carding Shop. *Krebs on Security: In-depth Security New and Investigation*. Retrieved from http://krebsonsecurity.com/2014/06/peek-inside-a-professional-carding-shop/

Levin, A. (2014, February 13). Small Businesses: Prepare to Be Breached! Retrieved from http://www.huffingtonpost.com/adam-levin/small-businesses-prepare_b_4777204.html

MacWillson, Dr. A. (2012, March 13). The Need to Secure the Cyber Supply Chain. SecurityWeek: Internet and Enterprise Security News, Insights and Analysis. Retrieved from http://www.securityweek.com/need-secure-cyber-supply-chain

Mandiant. (2014). M-Trends: Beyond the Breach. Retrieved from https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

© 2014 The SANS Institute Author retains full rights.

Mastercard Worldwide. (n.d.). All About Payment Cards. Retrieved from http://www.mastercard.com/us/company/en/docs/All_About_Payment_Cards.pdf

Moyle, E. (2013, November 12). PCI DSS version 3.0: The five most important changes for merchants. *SearchSecurity.com*. Retrieved from http://searchsecurity.techtarget.com/tip/PCI-DSS-version-30-The-five-most-important-changes-for-merchants

Microsoft. (n.d.). *Malware Protection Center*. Retrieved from http://www.microsoft.com/security/portal/mmpc/shared/malwarenaming.aspx

Patrick. (2014, June 5). McDumpals - I'm swipin' it. *ProtectYourNet: Researching Cybercrime and Malware*. Retrieved from http://protectyournet.blogspot.com/2014/06/mcdumpals-im-swipin-it_5.html

PCI Security Standards Council, LLC. (n.d.). PCI SSC Data Security Standards Overview. Retrieved from https://www.pcisecuritystandards.org/security_standards/

PCI Security Standards Council, LLC. (2014). About Us. Retrieved from https://www.pcisecuritystandards.org/organization_info/index.php

PCI Security Standards Council, LLC. (2013a, November). *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures Version 3.0*. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

PCI Security Standards Council, LLC. (2013b, November). Payment Card Industry (PCI) Data Security Standard: Summary of Changes from PCI DSS Version 2.0 to 3.0. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_Summary_of_Changes.pdf

Posmatic. (n.d.). What is Point of Sale (POS)?. Retrieved from http://www.posmatic.com/point-of-sale/what-is-point-of-sale.php

Poulin, C. (2014, January 31). What Retailers Need to Learn from the Target Breach to Protect

© 2014 The SANS Institute Author retains full rights.

against Similar Attacks. Security Intelligence: Analysis and Insight for Information Security Professionals. Retrieved from http://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/#.U76Cp7Ee8SR

Prolexic. (2014, June 10). Threat Advisory: Zeus Crimeware. Prolexic Threat Advisory. Retrieved from http://www.prolexic.com/kcresources/prolexic-threat-advisories/prolexic-threat-advisory-zeus-060614/Threat-Advisory-Zeus-Crimeware-Framework-US-061014.pdf

Q-Card. (n.d.). *ISO Magnetic Stripe Card Standards*. Retrieved from http://www.q-card.com/support/magnetic-stripe-card-standards.asp

Roberts, P. (2012, September 12). A picked pocket in Mallorca reveals chink in chip-and-PIN security. Naked Security. Retrieved from http://nakedsecurity.sophos.com/2012/09/12/a-picked-pocket-in-mallorca-reveals-chink-in-chip-and-pin-security/

Schwartz, M.J. (2014a, January 14). Target Breach: 8 Facts On Memory-Scraping Malware. *Dark Reading*. Retrieved from http://www.darkreading.com/attacks-and-breaches/target-breach-8-facts-on-memory-scraping-malware/d/d-id/1113440?page_number=1

Schwartz, M.J. (2014b, January 24). Target Breach: Why Smartcards Won't Stop Hackers. *Dark Reading*. Retrieved from http://www.darkreading.com/attacks-and-breaches/target-breach-why-smartcards-wont-stop-hackers-/d/d-id/1113565

Smart Card Alliance. (n.d.). EMV: FAQ Retrieved from http://www.smartcardalliance.org/pages/publications-emv-faq#q1

Tate, K. (2014, March 20). Texas-Based Sally Beauty Supply Hacked, Credit Cards Compromised. *Breitbart.com*. Retrieved from http://www.breitbart.com/Breitbart-Texas/2014/03/20/Texas-Based-Sally-Beauty-Supply-Hacked-Credit-Cards-Compromised

Team Cymru. (2013, May). *Alina & other POS Malware*. Retrieved from https://www.team

© 2014 The SANS Institute Author retains full rights.

cymru.com/ReadingRoom/Whitepapers/

Trend Micro Inc. (2014). *Point-of-Sale System Breaches: Threats to the Retail and Hospitality Industries*. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-pos-system-breaches.pdf

Trustwave Holdings, Inc. (2013). *2013 Trustwave Global Security Report*. Retrieved from http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

Trustwave Holdings, Inc. (2014). *2014 Trustwave Global Security Report*. Retrieved from http://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf

US CERT. (2014, February 5). Alert (TA14-002A) Malware Targeting Point of Sale Systems. *Alerts*. Retrieved from https://www.us-cert.gov/ncas/alerts/TA14-002A

Verizon. (2014). *2014 Data Breach Investigations Report*. Retrieved from http://www.verizonenterprise.com/DBIR/2014/

Whitehouse. (2009, May 8). The United States Cyber Challenge. Retrieved from http://www.whitehouse.gov/files/documents/cyber/The%20United%20States%20Cyber%20Challenge%201.1%20%28updated%205-8-09%29.pdf

Zetter, K. (2014, January 24). Neiman Marcus: 1.1 Million Credit Cards Exposed in Three Month Hack. *Wired.com*. Retrieved from http://www.wired.com/2014/01/neiman-marcus-hack/

© 2014 The SANS Institute Author retains full rights.

Appendix A

Recommended Best Practices	Applicable Critical Security Controls	Control Details
Strong Password Use (no vendor default passwords)	12.3, 12.4, & 12.5	CSC 12-3: Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length. CSC 12-4: Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts. CSC 12-5: Ensure that all service accounts have long and difficult-to-guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.
Patched and Up-To-Date Software	4.1	CSC 4-1: Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).
Firewall (Ingress & Egress)	11.2, 11.5, 11.6	CSC 11-2: Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. CSC 11-5: Verify any server that is visible from the

© 2014 The SANS Institute Author retains full rights.

		Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address. CSC 11-6: Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.
Updated AntiVirus Solution	5.1 & 5.2	CSC 5-1: Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers. CSC 5-2: Employ anti-malware software that offers a remote, cloud-based centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.
Restrict POS System Access to the Internet	11.2, 11.5, 11.6	CSC 11-2: Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. CSC 11-5: Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address. CSC 11-6: Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.
Disallow Remote Access to the POS systems	11.2, 11.5, 11.6	CSC 11-2: Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. CSC 11-5: Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal

© 2014 The SANS Institute Author retains full rights.

		VLAN and give it a private address. CSC 11-6: Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.
Strict Network Segmentation (Card data from non-card data segments)	13.10	13.10: To limit access by an insider, untrusted subcontractor/vendor, or malware spreading on an internal network, devise internal network segmentation schemes to limit traffic to only those services needed for business use across the organization's internal network.
Two-Factor Authentication for Access POS system environment	13.7	13.7: Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.
Manage Privileged Access (Unique Admin Accounts & Principle of Least Privilege)	3.3	CSC 3-3: Limit administrative privileges to very few users who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system. This will help prevent installation of unauthorized software and other abuses of administrator privileges.
True Hardware P2P Encryption for all sensitive data	17.6	SC 17-6: Conduct periodic scans of server machines using automated tools to determine whether sensitive data (i.e., personally identifiable information, health, credit card, and classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information.
Application Whitelisting	2.1	CSC 2-1: Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose

© 2014 The SANS Institute Author retains full rights.

		systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow. When protecting systems with customized software that may be seen as difficult to whitelist, use item 8 below (isolating the custom software in a virtual operating system that does not retain infections.).
Endpoint Threat Detection/Response	5.1 & 5.2 & 14.5	CSC 5-1: Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers. CSC 5-2: Employ anti-malware software that offers a remote, cloud-based centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update. CSC 14-5: Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings.
File Integrity Monitoring	3.8, 5.1 & 5.2	CSC 3-8: Utilize file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. All alterations to such files should be automatically reported to security personnel. The reporting system should have the ability to account for routine and expected changes, highlighting unusual or unexpected alterations. For investigative support, the reporting system should be able to show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should also identify suspicious system alterations such as owner and permissions changes to files or

© 2014 The SANS Institute Author retains full rights.

		directories; the use of alternate data streams which could be used to hide malicious activities; as well as detecting the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes). CSC 5-1: Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers. CSC 5-2: Employ anti-malware software that offers a remote, cloud-based centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.
Actively monitor the Environment (i.e. NIDS)	5.1 & 5.2 & 13.14	CSC 5-1: Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers. CSC 5-2: Employ anti-malware software that offers a remote, cloud-based centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update. CSC 13-14: Deploy NetFlow collection and analysis to DMZ flows to detect anomalous activity.
Ensure Cardholder Data is Deleted (encrypted or	17.6	SC 17-6: Conduct periodic scans of server machines using automated tools to determine whether sensitive data (i.e., personally identifiable information, health, credit card, and classified information) is present on the

© 2014 The SANS Institute Author retains full rights.

not)		system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information.
Physical Access Policies (system upgrades/repairs)	?	Not specifically addressed by the CSCs.
3rd party Agreements (no universal customer passwords)	18.5	CSC 18-5: Assemble and maintain information on third-party contact information to be used to report a security incident (i.e., maintain an e-mail address of security@organization.com or have a web page http://organization.com/security).
Secure Coding if Custom Developed	6.3, 6.4, & 6.7	CSC 6-3: For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. CSC 6-4: Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis. Include tests for application behavior under denial-of-service or resource exhaustion attacks. CSC 6-7: Test in-house-developed web and other application software for coding errors and potential vulnerabilities prior to deployment using automated static code analysis software, as well as manual testing and inspection. In particular, input validation and output encoding routines of application software should be reviewed and tested.

© 2014 The SANS Institute Author retains full rights.