



50 Minutes and 500 Dollars:
Real World Solutions for
PCI DSS Security

In the real world, the Payment Card Industry Data Security Standard (PCI DSS) is not a level four merchant's primary concern. It's probably not even in the top 10 list of all concerns. Merchants are more interested in turning a profit with their core business. The problem is, while a merchant's primary focus may not be on the security of its payment processing system, attackers are focused on identifying unsecured systems. If they can get onto a system, they can wreak havoc, and could potentially force a merchant into bankruptcy with PCI fines, fraud recovery, card replacement fees, loss of market share and loss of customer confidence.

Sounds serious doesn't it? An attacker does not care about a small business owner trying to keep his or her head above water. He does not care that a merchant's modest profits sends their children to college. He does not care that his activity could deplete a 401k and destroy any hope for retirement. He wants credit card data so he can sell it, turn a profit and take another first class vacation for the month. All on someone else's dime.

The Breach Triad

Trustwave's SpiderLabs investigates hundreds of breaches each year. And, each year, they see the same security vulnerabilities (detailed in "The Top 10 Vulnerabilities Leading to Compromise," available at www.trustwave.com/whitePapers.php).

As a result of our research, we've identified the Breach Triad. It consists of three elements that have to be in place for a data breach to occur:

1. Infiltration
2. Aggregation
3. Exfiltration

To illustrate this concept, think of the classic bank robbery – thief in a black-and-white striped shirt, black gloves, back hat and a white bag decorated with dollar signs. For the bank robber to commit his crime he needs to do three things. First, he needs to break into the bank, then find the money and put it into his bag, and finally make his getaway.

Data breaches are no different. An attacker needs a way onto the target computer system, he needs something to steal (usually track data--the data embedded on the magnetic stripe on the back of credit and debit cards), and he needs to remove that data off the system, and onto another system to which he has access.

While not a replacement for a full PCI DSS security assessment, understanding the Breach Triad can help to reduce the risk of being breached. Using the actionable intelligence gathered in this paper, merchants can better secure Point-of-Sale (POS) systems and become less of an easy target for attackers. We are, in essence, going to cut the "legs" out from under the Breach Triad. Doing so will not make a business unhackable, but it will help improve any business' ability to defend against a targeted attack.

Infiltration

Infiltration is the first element of the Breach Triad. In many SpiderLabs breach investigations, attackers usually access a system due to open remote administration ports and default passwords. What does this mean?

First, let's review remote administration ports. Take, for example, a successful hot dog restaurant serving a local community. The business has a dining room with two POS terminals and one back-of-house (BOH) server. Employees take orders and swipe customer's credit or debit cards at the POS terminals, and the data is sent to the BOH server where it then goes to a processing bank for authorization. Finally, it is sent back with an authorization code and an employee prints a receipt for the customer. This transaction happens in a matter of seconds.

Customer service and quality hot dogs are the hallmarks of this business. The owner, with limited knowledge of technology and data security, hires a POS integration vendor to handle the payment systems. The vendor installs the payment system, updates it, patches it and makes sure it runs properly in order for the business to process credit and debit cards (which currently makes up about 75 percent of all its sales). For this vendor to access the computer systems to perform his contracted duties, he needs to use a remote administration tool. A remote administration tool is used to remotely connect and manage computers; some of the more popular tools are Remote Desktop Protocol (RDP), pcAnywhere, Virtual Network Client (VNC) and LogMeIn. The problem with remote administration applications is that, if a vendor can access a business' systems, so can anybody else if the application is not secure.

Hackers perform "passive reconnaissance" to identify targets that have open remote administration ports. All remote administration tools listen for incoming connections on specific ports. For example, Remote Desktop Protocol (RDP) listens on TCP port 3389, pcAnywhere listens on TCP port 5631 and UDP port 5632, VNC listens on TCP ports 5800 and 5900, and so

on. Using basic port-scanning techniques, hackers quickly and easily identify which targets are listening on these remote administration ports. This reconnaissance helps hackers identify which IP addresses have these default ports listening for connections. Then, just like a POS integration vendor, they use the same tools to try to connect.

Businesses can take a few short actions to prevent an attacker from gaining access to a system through open remote administration ports.

Change the port – Cost \$0 – Time 10 minutes

Hackers are lazy. They don't want to physically type the same commands over and over again, so they write small automated script to do their dirty work for them. These scripts search for the default ports used by remote administration tools. By changing the port to something other than the default, the IP address will likely go unnoticed by a hacker's reconnaissance script.

Use the firewall to restrict incoming transactions – Cost \$0 – Time 10 minutes

By using a firewall anyone can restrict from which IP address remote administration tools will accept communications. By creating a firewall rule that only allows remote connections from approved IP addresses, one can control who accesses the systems and from where. (More information on purchasing a firewall appears later in this white paper.)

Disable remote administration services until needed – Cost \$0 – Time 10 minutes

According to the Payment Card Industry Data Security Standard (PCI DSS), remote administration tools should use "on demand" access. This means that whoever wants to access systems remotely must first contact the system owner and ask them to enable the service that will permit their connection. Once they have completed their work, they should call the system owner again, indicating that they are finished – at which time the service can be disabled, making remote connection for anyone else impossible.

The second piece to this first element of the Breach Triad is default passwords. In 2009 alone, 89% of breaches involved default vendor-supplied passwords. To quickly and easily address this vulnerability:

- Change the default password.
- Don't use the same password as the user name, such as user:user, admin:admin, etc.
- Don't use the any variation of the word "password."
- Don't leave the default password blank.

According to the PCI DSS a password should be at least seven (7) characters long, with at least one upper case letter, one number and one special character. For example: Pro!3ct. Additionally, passwords should be changed every 90 days, and no password should be reused before four other passwords have first been used.

Now, as everyone knows, when a password is complex, humans will resort to writing it down on a sticky note and post it on the side of their monitor or to the underside of the keyboard. Instead of leaving passwords out in the open, one can use "word permutation." It's simply substituting a number or special characters for a letter. For example, a "\$" can be substituted for "s," "@" instead of an "a," "8" instead of a "B," or "3" to replace an "E." This can make a password meet complexity requirements without making it so difficult that it can't be remembered without being written down.

Here are some examples of weak passwords, followed by their permuted, PCI DSS-compliant version:

| | |
|---------------|-----------------|
| DaBears | !!D@83ar\$!! |
| RollTide | R0!!T1d3 |
| HookemHorns | H00k3mH0rn\$! |
| HappyBirthday | H@ppy81rthD@y!! |

Change the vendor-supplied default password to one that complies with the PCI DSS by using word permutation– Cost \$0– Time 5 minutes

Aggregation

Now that we have covered the ways to keep the bad guys from getting onto systems, thus eliminating the first element of the Breach Triad, we will move to the second piece and take away the "something to steal."

It is a violation of the PCI DSS to store track data post authorization. This means that after receiving approval/denial of the charge, the track data associated with that transaction must be wiped, or removed, from the system.

Merchants have very little, if any, control over this aspect of a payment application. However, it IS the merchant's responsibility to ensure they are using a PCI DSS-compliant version of the payment application. To see if a POS system version is compliant, visit the PCI Security Standards Council Web site: https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml. This site contains the list of applications that have been certified compliant, which means that they should NOT store track data post authorization. All merchants should ask their POS integrator if they are running a Payment Application Data Security Standard (PA-DSS) compliant version of the application. If a merchant is not using a PA-DSS compliant application, most vendors will offer an upgrade for a fee. Since this can (and likely will) vary dramatically from one integrator to another, and one POS vendor to another, the price for an upgrade is not included in this white paper.

It is also important to ask the POS vendor if the track data is deleted or securely wiped from the system after authorization has been received. There is a big difference between the two. When a file or other data is deleted from a computer system, it's not really gone. What happens is that the entry in a Virtual Table of Contents (VTOC) is removed for that "chunk" of data, and a marker is set indicating that the system can reuse that "chunk" whenever needed.

For example, look at the table of contents in a book. This information indicates on what page specific information is located. Now, if the page with the table of contents is torn out, is the information contained within the book gone? No.

Secure wiping is different. When data is securely wiped from the hard drive, the application used to perform the secure wipe actually takes the section of disk and overwrites it with 1s, 0s or both.

Take the example of the book again. On any page, a black permanent marker is used to write either a 1 or a 0 over every letter on that page (the equivalent of a onetime overpass). This process is done over and over again. Can the data be read? No; this is what happens when a secure wiping tool is used to remove data. The "chunk" of data is physically overwritten with other data, making the original information unreadable.

There are several good secure wiping utilities that are open source and free to the public. They can be downloaded from the Internet and installed quickly and easily. Additionally, they can be used by automation (script) to wipe the unused sections of the hard drive (where the "deleted" files go) daily.

To avoid giving hackers the opportunity to steal data, don't store track data post authorization. This will likely require the involvement of a POS vendor to ensure that a PA-DSS certified version of the payment application is being used. Additionally, install a secure wiping utility to make sure all of cardholder data is wiped (overwritten) rather than simply deleted.

Upgrade to PA-DSS-compliant payment application – Cost varies – Time varies

Remember, this will vary based on the integrator, and which payment application is being used.

Implement secure wiping utility – Cost \$0 – Time 10 minutes

Using a free open source secure wiping utility can help avoid adding to the overall cost of PCI DSS security.

Exfiltration

The third and final piece of the Breach Triad is exfiltration, which is the process of sending the stolen data from the target system to a system controlled by the hackers. This can be blocked in a few different ways, but primarily by using a firewall.

When configured properly, a firewall is a powerful protection mechanism against various types of security related issues – namely preventing unauthorized infiltration and exfiltration. In this case, it is going to be used to prevent unauthorized outbound communications from the BOH server.

First, merchants should contact their processing bank and ask them to provide the IP address they use for payment transactions. It may be a single IP, or a block of IPs; regardless of number, a firewall is smart enough to account for this. Next, contact the POS vendor and ask them on which port does the payment application communicate to the bank. Remember to change that port as discussed in the second part of the Breach Triad. Once this information is obtained, a firewall rule can be created to allow that application to send outbound communications on that port, to that IP or block of IPs. This should be the only outbound destination to which the BOH server communicates. All other outbound access should

be denied. In a worst case scenario, even if hackers are on the network, and steal cardholder data, this firewall rule would prevent them from sending the data from the target system to one that they control.

The PCI DSS requires a firewall, however, merchants just need to have one that performs what is called, “stateful packet inspection,” which all current models perform. Stateful packet inspection looks at each communication thread and ensures that the “conversation” initiated from behind the firewall. This prevents several different types of attacks in which an intruder would try to fake, or “spoof,” the fact that his communication thread did not really start from behind the firewall.

Simply buying a firewall, taking it out of the box and installing it in a network will not adequately secure that network. Firewalls aren’t an out-of-the-box solution. Firewalls require Access Control Lists, or ACLs (pronounced ACK-LL-S), that tell it what to do. Much like a traffic cop who tells cars to either go, stop or turn, firewalls indicate which data communications are allowed to proceed and which aren’t.

By approaching PCI DSS security in terms of the Breach Triad (Infiltration, Aggregation and Exfiltration), merchants can quickly, and inexpensively improve the overall data security posture of their business. Remember, this will not necessarily make a business unhackable.

Purchase and implement a firewall—Cost \$200 - \$500—Time 30 minutes

A decent firewall that meets the PCI DSS requirements for implementing a packet filtering firewall can be purchased for as little as \$175. Configuring a firewall may take anywhere between 20 and 30 minutes depending on the complexity of the network and the technical expertise of the person configuring the appliance. The labor should not cost more than \$150. On average, implementing a firewall can cost \$325. Merchants can spend more than that, but the effects will basically be the same.

These modern day bank robbers are smart and understand return on investment (ROI); they desire a high gain from a low investment. When merchants implement these few basic security measures, hackers are faced with the decision to either put more effort into the hack (which is entirely possible), or move onto an easier target. If the return is going to be the same, then why would a hacker spend two days breaking into a secure network, when they can spend 15 minutes breaking into the business without network security? The easy hack will almost always win. But with less than \$500 and about 50 minutes of actual work, any business can mitigate its exposure and exponentially decrease the chances of suffering an expensive and damaging breach.

About Trustwave

Trustwave is the leading provider of on-demand and subscription-based information security and payment card industry compliance management solutions to businesses and government entities throughout the world. For organisations faced with today’s challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its flagship TrustKeeper® compliance management software and other proprietary security solutions. Trustwave has helped thousands of organisations—ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructure, data communications and critical information assets. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, Africa, Asia and Australia. For more information, visit <https://www.trustwave.com>.

About Trustwave’s SpiderLabs

SpiderLabs is the advanced security team within Trustwave® focused on forensics, ethical hacking and application security testing for our premier clients. The team has performed hundreds of forensic investigations, thousands of ethical hacking exercises and hundreds of application security tests globally. In addition, the SpiderLabsResearch team provides intelligence through bleeding-edge research and proof of concept tool development to enhance Trustwave’s products and services. For more information, visit <https://www.trustwave.com/spiderLabs.php>.