

## The Top 10 Vulnerabilities Leading to Compromise



## Introduction

Computer systems are attacked and compromised every day. Hollywood might position these attacks as the work of super smart hackers, holed up in a basement somewhere and shrouded in darkness, save for a wall of blinking server lights and the soft glow of flat screen monitors. But in reality, compromises are less a result of intellect, and more the result of poor system administration, lack of knowledge and even information technology budget cuts.

To help understand where an organization is exposed, this paper outlines the top 10 most frequently exploited vulnerabilities, or attack vectors, that lead to a system compromise and the subsequent loss of sensitive data as they pertain to the Payment Card Industry (PCI). Infiltration can happen at any company, regardless of size and structure. The breach of a company with a full-time information technology (IT) staff that includes an information security (IS) team may be more difficult and take more time, but the underlying vulnerabilities, left unfixed, still exist.

Before examining each of the top 10 compromises, one should first understand the key components of cyber-crimes as they pertain to data theft. An attacker needs:

1. A way into the systems (infiltration)
2. Something to steal (theft of valuable data)
3. A way to get the data off the systems (exfiltration)

Each vulnerability explored below will be categorized as either **I** for **Infiltration**, **T** for **Theft** or **E** for **Exfiltration**.

Another key principle to understand and apply as a backdrop for this whitepaper is a concept entitled "defense in depth." Defense in depth means that an organization employs multiple protection layers, techniques and mechanisms to secure critical assets. For example, using just a firewall may slow an attacker down, but may not actually stop them. Encrypting data and using strong passwords, by themselves may not be much of a deterrent either. However, if you deploy a firewall, use data encryption, require strong passwords, ensure all systems are patched and up to date, install anti-virus software and segregate the PCI network from non-PCI systems, you will have a stronger overall security posture, or defense in depth.

## The Top 10 Attack Vectors

### 1. Remote Access Applications (I)

By themselves, remote access applications, sometimes called "remote desktop" or "terminal services," are not solely responsible for a breach; they are typically used in conjunction with other attack vectors. Most small companies use remote access applications to allow their corporate partner or contracted IT shop access to their systems for maintenance. Using remote access applications for this purpose is normal in today's operating environment.

To permit remote access, the customer must have at least one Internet Protocol (IP) address that is accessible by the external Internet. This is called having a "routable" address because there is an open route from the third party to the customer's server. Having a routable IP enables the third party to establish a connection with the remote access application running on an organization's system(s).

How can the data thieves tell that a remote access application is running? Computers communicate in much the same way that ships deliver goods. When ships sail in and out of shipyards, they deliver specific goods to the appropriate, predefined ports. For computers, certain remote access applications have specific TCP/IP ports that are normally used for that application to communicate with other systems. These ports are widely known, and are seldom changed from their default configuration

settings. Hackers will use an automated scanning utility such as nmap<sup>1</sup> that tells them if those ports are open for an incoming connection. If the ports are open, then the hacker knows they have a prospective target.

Once the target has been identified, attackers can perform something called “passive reconnaissance” to obtain further details about their target. A hacker can look up a company’s IP address on the American Registry for Internet Numbers<sup>2</sup> (ARIN) to find out who owns that specific IP block, and potentially who administers that server. Additionally, Web sites such as GeoIPTool<sup>3</sup> will show hackers the specific geographical location of the server(s). In a very short period of time, an attacker can find out who you are, where the servers are on a map, who the server administrators are and which remote access application(s) you use. That is more than enough information for a hacker to begin an attack.

## 2. Passwords (I)

There is a clear difference between strong passwords and weak passwords. Strong passwords have at least eight characters and incorporate upper and lower case letters, numbers, and special characters. The best strong passwords are not based on dictionary words and have no reference to the user, the user’s hometown or their family. “Password complexity” refers to how many different characters a user is forced to use when creating their password. A password that only requires a user to have upper and lower case letters is not very complex; one that requires a user to incorporate at least one or two upper case letters, at least two numbers, and at least two special characters is very complex.

Hackers have ways of guessing passwords and use two primary types of password attacks: brute force attacks and dictionary attacks. “Brute forcing” is an attempt to use every possible variation of a password based on the complexity requirements. Brute force attacks will ALL eventually succeed. The drawback, however, is that when a high level of password complexity is in place, the time required for the attack to finally succeed would make this type of attack mathematically infeasible.

The other type of attack is called a “dictionary attack.” Simply, it uses known dictionary words and tries them as possible passwords. Surprisingly, an overwhelming majority of end-users, including IT professionals, still use dictionary words as their passwords. Attacks on these types of passwords are usually very successful in a short period of time.

Passwords need to be complex enough to prevent them from being quickly cracked but also need to be memorable. How many people can remember “Yb1\*b4T&” without writing it down? But by writing passwords down, one negates the purpose for having the password in the first place. A viable solution to this problem is word permutation. Word permutation takes every variation of actual dictionary words and provides them as passwords. If the password is Trustwave, some possible word permutations of this password could be:

- Trus1w@v3
- 4ru\$tWave
- truS4w@ve
- Tru5t#ave
- tRu5twa%e

---

<sup>1</sup> Nmap (“Network Mapper”) is a free and open source utility for security auditing, network exploration and inventory and managing service upgrade schedules. For more information, visit <http://nmap.org/>

<sup>2</sup> For US-based companies only. [www.arin.net](http://www.arin.net)

<sup>3</sup> [www.geoiptool.com](http://www.geoiptool.com)

The substitution of letters and numbers, upper and lower case letters, and special characters is an effective and relatively easy way to create complex passwords. It allows passwords to meet specific requirements, while making them relatively easy to remember.

The Payment Card Industry Data Security Standard (PCI DSS) requires seven-character passwords with at least one upper-case character, one lower-case character and one special character. However, a password with eight characters is a much more secure solution. As you can see from the table below, the amount of time it takes to crack seven character passwords as compared to eight character passwords increases dramatically, especially when the variety of characters also increases.

**Table: Password Strength**

Password length	No case requirement; letters only	No case requirement; letters and digits	Case sensitive, letters and digits	Case sensitive, letters, digits and symbols
4	N/A	N/A	1 minute	13 minutes
5	N/A	10 minutes	1 hour	22 hours
6	50 minutes	6 hours	2.2 days	3 months
7	22 hours	9 days	4 months	23 years
8	24 days	10.5 months	17 years	2287 years
9	21 months	32.6 years	881 years	219,000 years
10	45 years	1159 years	45,838 years	21 million years

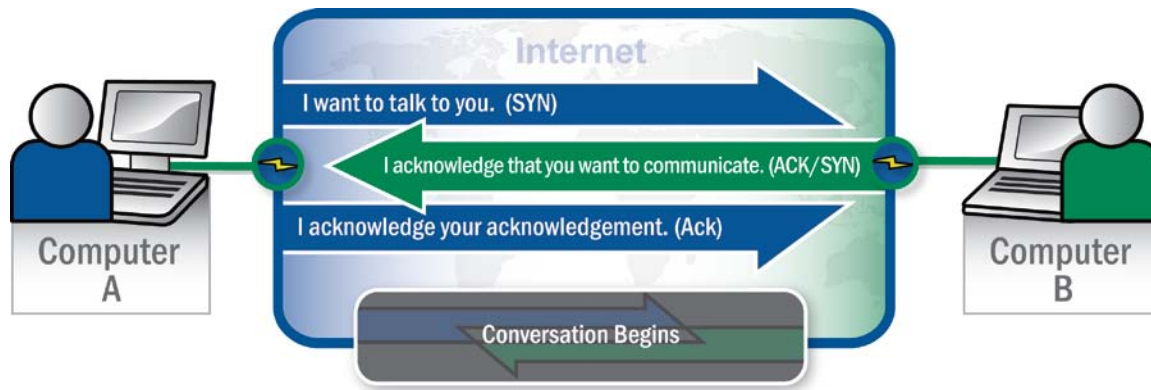
\* LastBit Corp. <https://lastbit.com/psw.asp>. Search speed is set to equal 100,000 passwords per second.

### 3. Firewalls (I, E)

The function of a firewall is to control the flow of traffic. Without a firewall in place to filter network traffic, intruders can more easily access the network. Firewalls filter communications by adhering to rules called Access Control Lists, or ACLs (pronounced "ack-ill-s"), that apply to incoming and outgoing communications, allowing certain kinds of traffic to pass and blocking others.

In general, computers communicate with one another using "packets." Rather than being sent in one large packet, data is sent in smaller, broken-down packets. If a break in the connection occurs between the two computers, or one or more of the packets are lost for some reason, the originating computer only needs to resend those packets that were lost instead of resending the entire data stream.

Computers initiate and conduct these communications through the "TCP Three-Way Handshake." The originating computer contacts the destination computer and tells it that it wants to initiate a communication; this is called a "Syn," short for Synchronize. The destination computer then responds to the originating computer, acknowledging that it understands the originating computer wishes to initiate a communication; this is called a "Syn/Ack," short for Synchronize/Acknowledge. Finally, the originating computer tells the destination computer that it acknowledges the acknowledgement; this is called just an "Ack" short for Acknowledge. Once this "handshake" takes place, the intended communication can begin.



In a common hacking technique, an attacker skips the first step of the three-way handshake and sends the destination computer a “Syn/Ack” packet. If there is no firewall (or a firewall is in place but lacks the proper configuration) in front of the destination computer, it will assume that it initiated the communication, and start communications with the originating host. Stateful Packet Inspection, a PCI requirement, prevents this kind of attack by setting up a rule that indicates a computer will only communicate when it starts the conversation and will not accept communications it did not initiate.

The other PCI requirement for firewalls is called Egress Filtering. Without Egress Filtering (the filtering of outbound packets) computer systems will simply send out whatever they are told to send regardless of the content. When Egress Filtering is enabled on the firewall, it takes a moment to inspect the contents of the data packets for information that adheres to predefined rules established by the administrator (i.e., ACLs). Commonly, Egress Filtering is configured to stop the transmission of any packets that contain credit card numbers, track data, personally identifiable information (PII), and personal health care information (PHI). Egress Filtering can also be configured to make sure that certain types of communications, like packets containing credit card data, only go to specific, designated IP addresses, like a processor or an acquiring bank.

When used together, Stateful Packet Inspection and Egress Filtering can be a formidable roadblock for would-be intruders and provides another layer to the defense-in-depth strategy.

#### 4. Encryption (T)

Even Point-of-Sale (POS) systems that claim to use full encryption may not be fully protecting clear text primary account numbers (PANs). How can this be? A company may be told that no credit card data is being stored on its POS system and that all data is stored encrypted. To demonstrate, what follows is an explanation of how credit card data ends up being stored on a system in the first place, how it is transmitted for processing, and how it is deleted.

In POS systems, credit card data is initially introduced into systems by a card reader. The card reader interprets the data that is embedded into the magnetic stripe on the back of the card, also referred to as “track” data, and loads it into that system’s temporary memory space called Random Access Memory (RAM). The computer has to put the data in RAM before it can do any sort of additional processing with it. This is not an option that can be controlled by the user; every system works with RAM in this way regardless of which POS software is being used.

Once the data is in RAM it is sent to a back of house (BOH) server for processing, the BOH server uses a mathematical algorithm to encrypt the data, sending it to an acquirer or processor for approval. Once approval is received, the BOH server sends the approval to the POS terminal, storing the data for a predefined period of time (usually 30 days in the event there needs to be a charge-back). The POS

terminal then prints out the customer receipt with a truncated PAN (typically the “\*\*\*\*” followed by the last four digits of the account number). During this process, the data is encrypted by the BOH server prior to transmission for processing, and after approval has been received and the data is stored locally. However, it is in clear text at the time the customer card was swiped, as the track data was being transmitted to the BOH server, and upon subsequent deletion of the data.

Current malware, designed to steal credit card and track data, takes advantage of the instances in which a customer’s data is unencrypted on the POS system. It grabs the targeted data at those specific points in the transaction process and sends it to a remote location. A POS system can be using encryption and a compromise can still occur.

Clear text storage can also occur in something called the “unallocated clusters” of the disk drive. Unallocated clusters are basically chunks of disk space that have either never been used by the operating system (OS), or are currently not being used by the OS. When something is deleted from a system normally (i.e., right click to delete, or drag and drop to the recycle bin) it’s not really gone. The OS simply takes those clusters of disk space and marks them for re-use later on. If the POS system deletes clusters containing credit card data, this information ends up in the unallocated clusters—and is still accessible.

Encryption issues also occur with the POS software and version upgrades. Newer versions of the POS software encrypt data while some previous versions do not. When an older version that is not already encrypting data is upgraded to a newer version that does encrypt data, data from the time of the upgrade forward will be encrypted, but the data stored prior to the upgrade will still be in clear text. This is not the case every time, nor with every POS vendor, however, it happens often enough to be a legitimate concern for businesses. When upgrading to a new version of POS software, or if an upgrade has recently taken place, contact the vendor or integrator to make them aware of this issue so they may plan accordingly. Trustwave strongly encourages companies to require proof from vendors that, when upgrading or buying new POS software, all data is being encrypted.

Though the PCI DSS requires all credit card and track data to be encrypted on POS systems, not all POS software encrypts this information. Due to the way the OS works there will be points in which data will be transmitted and stored unencrypted. Make sure you understand where these points are and why they exist (as detailed above), then implement appropriate compensating controls to help protect that data. Again, encryption alone WILL NOT adequately protect data, nor does it mean that data cannot be stolen. It is simply another mechanism of defense in depth that will make data more difficult to steal.

## 5. Network Segmentation (I, T, E)

Customer data must also be protected by using network segmentation to separate critical data from the rest of the infrastructure. When everything is on the same network segment, it’s accessible by anyone and everyone, including PCI systems where credit card data resides! An intruder can find his way onto any of the systems, and quickly and easily gain access to credit card data.

According to the PCI DSS, any and all systems within the PCI process flow should be on their own subnet. What that means is that there should be a separation between the systems that process credit card data, and those that don’t. Access into the PCI processing segment should be tightly controlled and monitored with a firewall to prevent unauthorized access.

By separating PCI systems from other systems, exposure to attack is drastically reduced. With network segmentation and proper firewall implementation an attacker cannot find a way in and/or out, and therefore cannot steal the data. For these reasons, network segmentation is one of the MOST CRITICAL components of a defense-in-depth strategy.

## 6. Patches (I)

One of the most commonly utilized attack vectors is exploiting vulnerabilities introduced by unpatched software. What is unpatched software and why is it such a security risk? A common business technique called “first to market” pushes many companies to launch products quickly, in order to gain an edge over their competitors. Software manufacturers are no different; they want to be first to market with their products. But in order to have the first, they have to make a decision regarding speed versus quality. Either they can release extremely high quality software and sacrifice speed, or they can be speedy and sacrifice quality. Many software companies opt for speed. Now, that is not to say they are releasing horrible programs, but they know that in the current operating environment, they can release somewhat incomplete code and subsequently issue patches to “fix” their subpar code. This is a practice that, in our increasingly technology-focused society, has been deemed to be wholly acceptable.

However, the desire to be first to market is not the only reason for vendor-issued patches. Hackers and security professionals are constantly on the hunt for vulnerable code to exploit and gain unauthorized access to a system. These errors are hidden in programs that, when pushed or prodded in just the right way, will provide the attacker the ability to perform some function that was never intended by the original developers. Security professionals can be contracted to help businesses identify and eliminate these coding errors. Regardless of who finds them, hackers or security professionals, once the code vulnerabilities are found, if the originating vendor does not want to have hackers use these vulnerabilities to break into systems using their own code, they will issue a patch (fix) for the bad code. This process of discovery and patching is ongoing and continuous.

The PCI DSS states that a comprehensive patch management program should be implemented. Simply, all software needs to be kept up to date. By doing so, a significant portion of exposure to intruders will be eliminated. As with any security measure, patch management by itself will not prevent an attack. It is merely another, albeit very effective, piece of a defense-in-depth strategy.

## 7. Shared Credentials (I)

The PCI DSS states that there must be a one to one ratio between users and user IDs. This is as much for accountability as it is for security. This ratio, coupled with appropriate auditing, allows for user activity to be traced back to a single user account.

But incidences of shared credentials still occur. When users share account information it takes away from the overall security posture of the environment in a couple of ways. First, if the shared account is compromised it becomes difficult--if not impossible--to differentiate between legitimate user activity and intruder activity. In smaller environments with just a few users, data reduction activities such as login times and the type of information being accessed can be used to identify intruder activity (i.e., IT employees accessing a drive share normally only accessed by the legal department). However, in larger environments with hundreds of users, the complexity of data reduction increases exponentially.

Second, when IDs are shared IDs, litigation or Human Resource action becomes impossible. If there are multiple users using the same account, how could it be proven beyond reasonable doubt that person X was the source of the illicit activity? The short answer is: it becomes extremely difficult and very costly. .

Each user should have an account. Additionally, the number of users with Administrative login credentials should be limited to business critical personnel only. While this number is going to vary from business to business based on size and complexity, the number of employees that have this level of access should be tightly regulated, maintained, and monitored. If there are currently not any administrative access policies, consider developing them.

## 8. Anti-Virus (I, T, E)

Confusion surrounds anti-virus (AV) software and its effectiveness against the threat of computer viruses. In the early days of computer viruses, when the rise of AV software came about, information about viral programs lacked detail. Media hype coupled with a basic lack of understanding of computing technology served to create a great deal of fear, uncertainty, and doubt. To dispel the common rumors and establish a baseline of understanding how these programs work, let's start with the definition of a computer virus.

A virus infects a computer unbeknownst to the owner, and can replicate itself in order to spread from one computer to the next. But in the current operating environment, a more inclusive term than virus is "malware." Malware is a name given to any program that is being used for malicious purposes. Malware coders use standard process names that look completely legitimate to most end users. In fact, well-coded malware can function on a system with current OS patches and up-to-date virus definitions. One might question the efficacy of even having AV software, but organizations may find AV software to be useful.

AV software uses what is referred to as a "one to many database comparison" to identify malware on a system. Much like a human fingerprint, malware has a fingerprint of sorts, referred to as a "hash," which is nothing more than a series of letters and numbers. For example "6d778e0f95447e6546553e66a709d03c" is the "Message Digest version 5" (MD5) hashed value for the common Windows binary "cmd.exe."

The AV program contains a database-like listing of all of these hash values, normally called a "dat" (data) or a "def" (definition) file. The AV software scans the systems searching for hash values that match those in its database. If a match is found, it reports this information to the user and takes predefined action, like quarantining or removing the file. This is very effective against **known** malware. Unfortunately, if the AV database does not have a hash signature for the malware, it will not find it.

Some vendors have developed more advanced AV software, integrating heuristics into the scanning technology. Heuristic detection software conducts behavior-based analysis instead of relying solely on signature analysis (i.e., searching for known hashes). This type of AV software looks for anomalous patterns in what the system is doing, such as processes running with an unusual amount of memory, opening of network connections to foreign systems, or accesses to abnormal files. Any anomalies are reported, and the end user decides whether or not this is acceptable or unacceptable behavior.

By itself, AV software is an insufficient layer of security. However, when combined with other mechanisms such as firewalls, network segmentation and user access controls, it does provide effective countermeasures against certain types of malware.

The PCI DSS states that AV software must be installed on all systems within the PCI processing environment. In order to be Payment Application Data Security Standard (PA-DSS) compliant, a POS vendor must be able to run AV software in conjunction with their POS software.

## 9. Auditing (I, E)

Every operating system, and most applications and network appliances such as firewalls and routers, have the ability to audit system activities. Events such as user logins, file access and system access, and system errors are recorded in something called "log files." While these logs will not prevent the systems from being attacked, they will provide critical information to any IT staff and security incident responders as they try to piece together what happened, when, and how.

Windows-based POS systems, widely used, maintain three different log files: system logs, security logs and application logs. These are commonly referred to as "event logs." By default, these logs have a 512

KB or seven-day retention period, whichever comes first. Once the threshold is exceeded the log entries will be deleted from the list, starting with the oldest. Since most PCI-related breaches are not detected for weeks, or months after the initial intrusion, the default configuration settings do not provide sufficient logging capabilities.

The PCI DSS states that all logs need to be maintained for 90 days online and one-year offline. To do this, default configurations settings need to be modified and a storage solution will need to be implemented for offline log storage.

## 10. Non-Validated Payment Applications (T)

According to the PCI-DSS, all payment applications in use should be PA-DSS certified. PA-DSS certified software receives validation from a Qualified Security Assessor (QSA) to be compliant with the Data Security Standard. This is a process where aspects of the software are reviewed for their overall security after installation. The PA-DSS and various supporting documents were updated to version 1.2 on October 1, 2008 and can be downloaded from the PCI Council's Web site<sup>4</sup>.

Referring to payment applications, the PCI Security Standards Council (PCI SSC) Web site<sup>5</sup> states:

"PA-DSS is the Council-managed program formerly under the supervision of the Visa Inc. program known as the Payment Application Best Practices (PABP). The goal of PA-DSS is to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI DSS. Payment applications that are sold, distributed or licensed to third parties are subject to the PA-DSS requirements. In-house payment applications developed by merchants or service providers that are not sold to a third party are not subject to the PA-DSS requirements, but must still be secured in accordance with the PCI DSS."

Once an application has been validated, it is placed on the PCI SSC's<sup>6</sup> list of "Validated Payment Applications." This list shows the validated software packages including specific versions that have been validated, when they were validated and when the validation expires.

Remember, simply having a PA-DSS certified payment application does not mean that there won't be (or hasn't already been) a compromise. Again, this is another mechanism in the defense-in-depth strategy that makes data more difficult to steal.

## Conclusion

No system is un-hackable. But the defense-in depth-strategy outlined above will go a long way in helping to secure a company's critical assets. Hackers, motivated by money, are unlikely to spend time wading through each of the levels of the defense strategy; this is not a good business decision for them. As Visa indicated in 2008, there are about 10 Million level 4 merchants in the US alone (A Level 4 merchant is any organization that processes less than \$500,000 annually in credit card transactions.). With so many potential targets that DON'T have a comprehensive defense posture, why would they waste their time with a Fortune 500 company?

---

<sup>4</sup> [https://www.pcisecuritystandards.org/security\\_standards/pci\\_pa\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_pa_dss.shtml)

<sup>5</sup> [https://www.pcisecuritystandards.org/security\\_standards/pa\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml)

<sup>6</sup> [https://www.pcisecuritystandards.org/security\\_standards/vpa/vpa\\_approval\\_list.html](https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html)

PCI compliance is not negotiable. If a company wants to process credit cards, it absolutely has to be compliant. Businesses are faced with a very simple decision. They can budget the time and resources necessary to attain compliance now, on their timetable and with their own staff. Or a company can wait until it gets hacked, spend thousands of dollars not in the budget, and have to adhere to the credit card brand's timetable, typically two weeks. After a breach, a company may also lose customer confidence and market share, and are fiscally liable for any fraud that takes place due to the breach as well as fines assessed by EACH of the compromised brands. It only makes good business sense to do it NOW, rather than wait for the thieves to come knocking.

If a company is PCI compliant and still suffers a breach and subsequent loss of cardholder data, it falls into a "Safe Harbor." Under Safe Harbor, credit card brands will not hold a business financially liable for the fraud nor will they issue fines for non-compliance.

Security is not an exact science. Rather, security is a way of methodically approaching the protection of critical assets and continually assessing and reassessing their overall safety. The defense-in-depth strategy should be considered a part of the operational strategy to protect not only a company's critical assets, but its reputation as well.

### **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 organizations 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 organizations—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, China and Australia. For more information, visit <https://www.trustwave.com>.



