Realtime
publishers

The Shortcut Guide™ To

PCI Compliance and How SSL Certificates Fit

sponsored by
thawte™

Dan Sullivan

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Chapter 1: Overview of Payment Card Industry Data Security Standards

Data breaches and cybercrime are routinely reported in the popular press. Popular, well-known companies such as Sony and Citibank have joined the ranks of security and payment card industry firms such as RSA and Heartland Payment Systems as victims of cyber attacks. These types of attacks are not new, and over time, businesses have responded by developing and enforcing minimal standards for protecting payment card data. The Payment Card Industry Data Security Standards (PCI DSS) define protections for credit and debit card data and holds merchants and payment processors responsible for meeting these standards.

The Shortcut Guide to PCI Compliance and How SSL Certificates Fit provides an overview of PCI DSS and SSL certificates, outlines what is required by PCI DSS, and provides a PCI compliance checklist. We start in this chapter by discussing three fundamental questions:

- Why do we need PCI standards?
- What is required by PCI standards?
- What is the role of SSL certificates in PCI compliance?

We begin by examining the business drivers that lead to the development of PCI DSS.

The Need for Payment Card Industry Data Security Standards

The PCI DSS are needed to protect consumers, merchants, and banks from credit card fraud and other forms of cybercrime. To understand what drove businesses to self-regulate the payment card industry, it can help to look at several factors that have impacted the industry:

- Well-publicized attacks on payment card businesses
- Impact of identity theft
- Emergence of professional markets for stolen credit card data
- Cost of credit card fraud on the industry

To understand how these factors help to shape the need for data protection standards, it is important to understand the basic relationship between the different actors in the payment card business.

The payment card industry is a highly distributed network of merchants, banks, and service providers that support a nearly ubiquitous payment processing system. Whether you are shopping online, traveling to another country, or dining out at your favorite restaurant, chances are you can pay for your goods and services using a credit or debit card. The payment card industry has set up procedures that allow us to use a credit card or debit card we receive from any one of a large number of issuing banks at a large number of merchants around the globe. The system is designed so that merchants do not have to have separate relationships with all banks that issue cards. Can you imagine a small business having to track hundreds, perhaps thousands of card-issuing banks? The payment card industry would collapse under the weight of so much needless administrative overhead. Instead of having one-to-one relationships between merchants and banks, the payment card industry makes use of payment processors (see Figure 1.1).

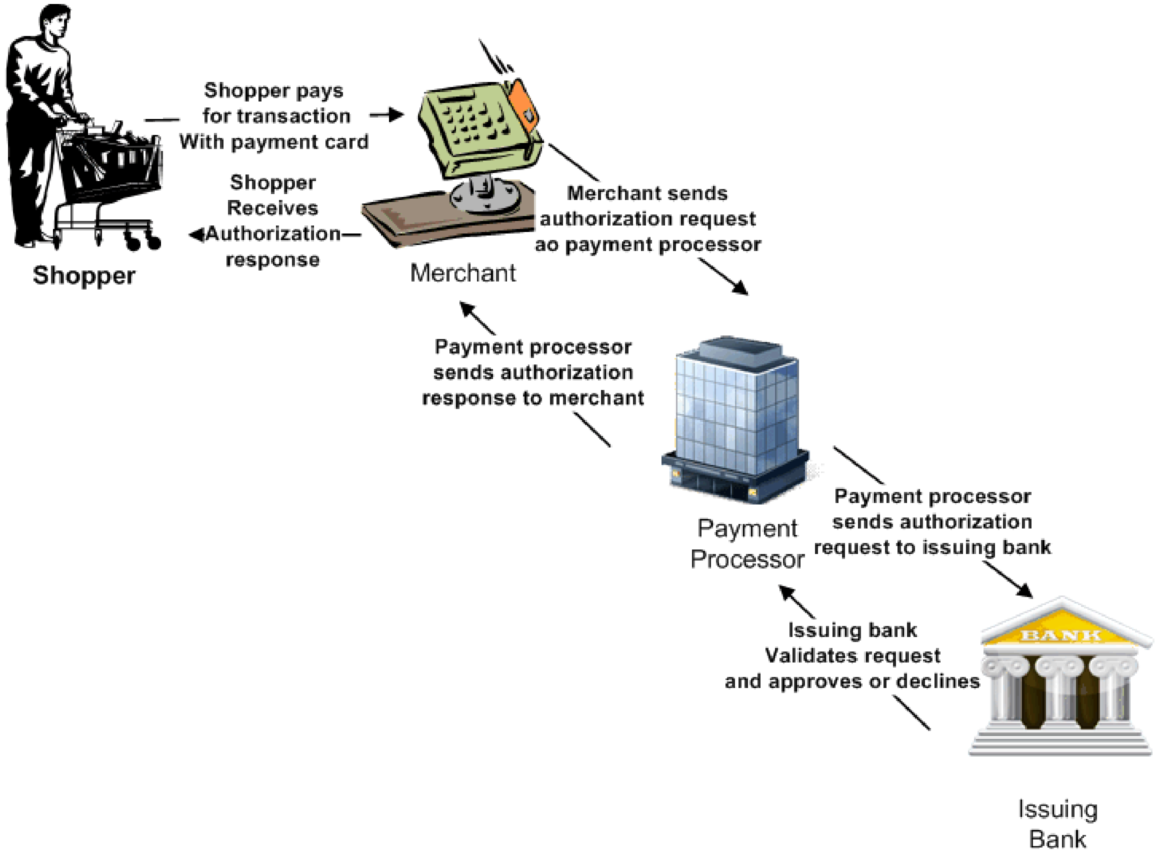

Figure 1.1: The payment card authorization process involves multiple businesses that receive and process credit card data such as card number and expiration date.

When a customer makes a purchase and pays for it with a credit card, a series of steps follows; the first steps route payment card information to the bank that issued the card:

- The merchant swipes the card or collects the credit card information and keys it into a point-of sale-device that transmits the data to a payment processor.
- The payment processor determines which bank issued the credit card and routes the authorization request data to the issuing bank.
- The bank validates the credit card, checks the customer's available credit, and performs other steps like risk analysis. (If you do not routinely buy thousands of dollars worth of electronic equipment online and ship it to addresses other than your billing address, there is a good chance such a charge would be declined).

After the bank determines whether to authorize or decline a charge, the following steps occur:

- The issuing bank sends an authorization response to the payment processor
- The payment processor forwards the authorization response to the merchant
- The merchant concludes the sale with the customer if the card was approved

This distributed method of routing information is the key to efficient and cost-effective payment card processing. The drawback of such a system is that credit card information passes through several distinct processing steps. Each step in the process is a potential target for criminals that would try to steal credit card data.

There is an obvious risk of a shopper losing his credit card. If someone found it, that person might be able to make fraudulent purchases. If the merchant keeps a copy of credit card numbers, expiration dates, and card security codes, that information could be lost or stolen potentially exposing multiple customers to fraud. The possibility for even larger-scale fraud occurs at the payment card processor and the issuing banks where large amounts of credit card data are processed. These are not just theoretical risks; there have been large-scale data breaches involving payment cards.

Well-Publicized Attacks on Payment Cards

Merchants, payment card processors, and banks have all been targets of cybercriminals looking to cash in on stolen payment card data. Victims have included:

- Hannaford Brothers, a merchant
- Heartland Payment Systems, a payment processor
- Citigroup, an issuer of payment cards

These incidents are chosen as examples, but they are not the only cases we could consider.

Data Breach at a Merchant

Hannaford Bros. is a supermarket chain based in Maine with 170 stores in New England and New York. In late 2007, the company started to suffer a data breach after company servers were infected with malware. Attackers installed malicious software that was designed to steal data from the point-of-sale systems where credit and debit cards were swiped. Over the course of 4 months, approximately 4.2 million payment card numbers were compromised. Estimates put the total cost at approximately $252 million (Source: http://www.businesspundit.com/10-most-costly-cyber-attacks-in-history/).

Data Breach at a Payment Processor

Heartland Payment Systems provides credit and debit card processing for more than 250,000 business locations across the United States. In late 2008, attackers were able to install malicious software on Heartland Payment Systems' servers and collect data on 100 million individual card numbers. The cost of recovering from this breach was estimated to be $140 million USD (Source: http://www.businesspundit.com/10-most-costly-cyber-attacks-in-history/).

Data Breach at an Issuing Bank

In the spring of 2011, Citigroup reported a hacking attack that exposed credit card data on more than 200,000 customers. Attackers were able to gain access to customer names, account numbers, and contact information. This type of a breach is particularly concerning because large banks have more resources to dedicate to security than do small merchants. Up to that time, merchants were more likely to be targeted by attackers. Reuters reports some security experts see this incident as a potential watershed after which banks will become more frequent targets for attackers (Source: Maria Aspan, "Regulators Pressure Banks after Citi Data Breach," June 9, 2011).

More than Isolated Incidents

Examples like these illustrate part of the problem. Even large companies with the resources to apply appropriate security measures can fall victim to cyber attacks. Could these just be anomalous outliers that are not representative of the experience of most companies? Perhaps that is the case, but a study by the Ponemon Institute finds widespread and severe impact of cybercrime. The researchers surveyed 50 large enterprises and found that cybercrime costs these organizations a median of $5.9 million USD per year with a range of $1.5 million to $36.5 million USD. The companies in the 2011 Ponemon study collectively experienced 72 successful attacks per week, a 44% increase over the previous year (Source: http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf). The incidents at Hannaford Brothers, Heartland Payment Systems, and Citibank are not isolated incidents—threats to the payment card industry are systemic.

Identity Theft

Identity theft is a crime that uses a victim's identity to commit fraud or gain access to the victim's personal resources, and credit card fraud is an obvious target for identity theft. The US government has tracked statistics on identity theft for at least 10 years. Some of their findings include:

- The US Federal Trade Commission received 250,854 identity theft complaints in 2010, the largest category of complaints.
- Credit card fraud was the second most common form of identity theft in 2010, surpassed only by government documents/benefit fraud.
- Credit card–related identity theft decreased by 5% between 2008 and 2010

(Source: US Federal Trade Commission, "Consumer Sentinel Network Data Book for January – December 2010", March 2011).

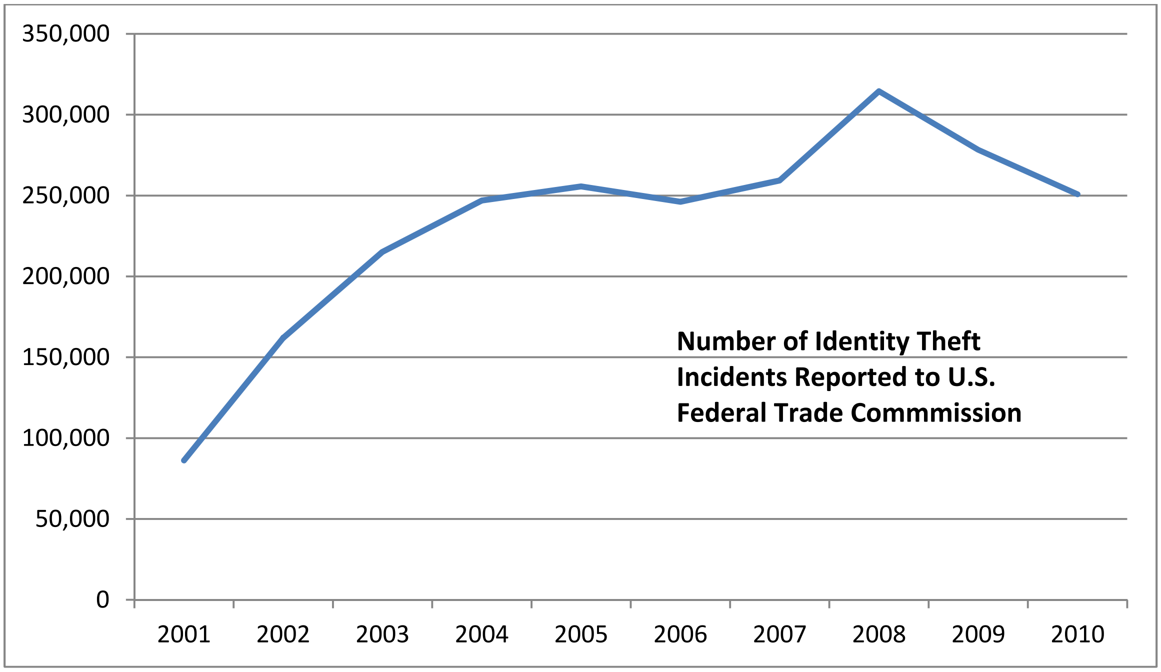

Figure 1.2: Reported identity theft incidents increased from 2001 to 2008 before beginning a slight decline (Source: http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf).

The cost of identity theft was $54 billion in the United States in 2009; worldwide, the cost to businesses was $221 billion. Victims of identity theft lost on average $4841 (Source: Jolie O'Dell "How Much Does Identity Theft Cost?"). The extent of identity theft, the cost to individuals and businesses, and the significant targeting of credit cards by identity theft thieves all contribute to the need to protect and secure payment card data.

Professional Markets for Stolen Credit Cards

As the example cases of credit card breaches show, a single group of attackers can sometimes net tens or hundreds of thousands of credit cards. The attackers can only make use of so many of these cards. The real value to the attackers is that the stolen information can be sold on cybercrime markets. These underground markets show surprising similarity to legitimate markets with specializations of labor, market-driven pricing, and a production and supply chain.

The US Federal Bureau of Investigations (FBI) has identified a wide range of professional roles within cybercrime markets as listed in Table 1.1.

Roles	Responsibilities
Programmers	Creators of malware to steal credit card and other information
Distributors	Brokers who mediate the sale of stolen information
Tech Experts	Systems administrators of the cybercrime world who keep the infrastructure up and running.
Hackers	R&D guys who search for new vulnerabilities to exploit
Fraudsters	Criminals with people skills who can craft phishing lures and other methods to trap victims
Hosted System Providers	"Businesses" that offer infrastructure services, such as servers
Cashiers	Those who provide accounts for money processing
Money Mules	Laborers who move money and complete transactions with banks to deposit the criminal profits
Tellers	Money launderers who put money through various channels, like currency exchanges
Organization Leaders	C-level execs of the cybercrime world who build and manage teams of cybercriminals

Table 1.1: Roles and responsibilities of cybercriminals in specialized cybercrime markets according to the FBI (Source: Panda Security, The Cyber-Crime Black Market: Uncovered, January 2011).

The key takeaway from this table is that cybercriminals are well organized and have created a market system with all its benefits. New providers can enter and innovators will be rewarded with more business. In addition, this market has customers who make use of these services and have a choice of providers. In case there is any doubt about the formidable challenge we face to protect against high-skilled and highly-motivated cybercriminals, let’s take a look at the kinds of revenues credit card fraud and related crimes can generate.

Cost of Fraud to Payment Card Industry

The number of payment cards in use has grown steadily over the past decade. The US Census Bureau estimates that there were 159 million credit card holders in 2000 and 173 million in 2006, and are projected to reach 181 million by 2010 (Source: Ben Woosley and Matt Schulz, "Credit Card Statistics, Industry Facts, Debt Statistics"). With so many credit cards in circulation, there is bound to significant fraud. When that happens, who pays the costs?

Consumers do not have to bear the brunt of credit fraud, at least not directly. By law, consumers are liable for only $50 of fraudulent charges unless the credit card data was stolen in a data breach, in which case they have no liability at all. That means that card issuers and merchants are left to pick up most of the cost of credit card fraud. Who ends up paying depends on whether the merchant complied with PCI DSS. When merchants follow safe practices, they are not liable for the fraud and the bank absorbs the cost. The aggregate costs of credit card fraud are substantial.

A 2010 study by LexisNexis found retailers lost $139 billion to fraud in 2009. The study also noted that for every $100 in fraudulent transactions, the total cost of fraud, including such things as card replacements, reached $310. Although consumers may not be liable for more than $50 if they report fraud within 60 days of receiving their statement, the report found consumers suffered from a $5.5 billion loss from unreimbursed expenses, legal expenses, and other charges (Source: "Retailers Lost $139 Billion to Fraud in the Last Year, According to LexisNexis Risk Solutions Study," September 2010). There is more to the story though. We all pay more to cover the cost of fraud; by one estimate, we pay an additional 2 to 4% to cover the cost of fraud (Source: Eva Norlyk Smith, Ph.D." The Hidden Costs of Credit Card Fraud" August 2011).

There have been a lot of statistics in this discussion, and they are necessary to capture the scope and magnitude of the problem. Well-publicized attacks on merchants make for compelling news stories and make us aware that a problem exists, but it does give a good picture of the extent of the problem. When we dig into the number of incidents of identity theft and consider the cost of fraud to consumers, merchants, and banks, we can see these are not isolated incidents. We should not be surprised at the magnitude of the problem. Hundreds of millions of credit cards are in use in the US alone. The value of credit card data is enough to lure and maintain sophisticated cybercrime organizations to the point where underground markets with division of labor and specializations are common place.

One way to mitigate the risk of payment card fraud is to implement information security controls that provide a base level of protection for that data. The PCI DSS is an attempt to define minimum standard protections that should be in place in the payment card industry.

What Does PCI DSS Compliance Require?

The PCI DSS is designed to set minimal protections for credit card information across the industry, so it is broad in its scope. The topics addressed by the standard include:

- Network security
- Payment card data protection
- Vulnerability management
- Access controls
- Monitoring and auditing
- Security policies and procedures

Each of these areas has specific requirements defined by the standard.

Network Security

The PCI DSS requires the use of firewalls and router configurations to protect the network transmitting credit card data. This is broken down into several tasks:

- Establishing a formal procedure for testing and approving network connections and changes to firewalls and routers
- Maintaining accurate network diagrams
- Implementing firewalls between internal networks and demilitarized zone (DMZ) segments
- Defining groups and roles responsible for network management
- Restricting inbound and outbound traffic to that required for the card processing operations
- Installing firewalls between wireless networks and cardholder data networks
- Deploying stateful inspection of network traffic
- Deploying personal firewalls on mobile devices with access to the cardholder network

Resource

This is not a full list of requirements for firewalls and routers; it is a representative sample. See the PCI DSS documentation for a complete list at Payment Card Industry (PCI) Data Standard: Requirements and Security Assessment Procedures version 2.0.

Another set of requirements for network security dictate that one should never use vendor-supplied default passwords. Also, servers should be hardened by:

- Using one server per function (for example, not having a DNS server on the same host as an application server)
- Executing only required process, service, daemon, etc. on servers
- Removing unnecessary scripts, tools, drivers, etc.
- Encrypting non-console administrative access to servers on the cardholder network

In addition to server and network configurations, one must implement controls to protect cardholder data.

Protecting Cardholder Data

As a general rule, you do not want to store any more cardholder data than you need to, and when you do store it, make sure it is encrypted and get rid of it as soon as possible. That was the short version of what is involved in protecting cardholder data; a more-detailed explanation includes specifics such as:

- Define and implement storage retention policies for cardholder data
- Do not store sensitive cardholder data such as data from a card's magnetic strip, card verification code, or a personal identification number
- Display only the first six or last four digits of a card number unless the full number is needed by an employee with legitimate need for the data
- If an account number is stored, make sure it is unreadable using strong encryption or some other equally protective measure
- Protect keys used in your encryption process so that they are not compromised
- Document key management procedures

In addition to keeping cardholder data safe when the data is at rest, we have to attend to protecting it during transmission. This requires that anytime cardholder data is transmitted, it is strongly encrypted.

Vulnerability Management

The section of the PCI DSS requirements that deals with vulnerability management covers endpoint security, antivirus, and vulnerability remediation. It calls for deploying antivirus solutions and ensuring they are current, active, and logging appropriately as well as patching for known vulnerabilities.

Businesses subject to PCI DSS regulations must also maintain patches to reduce the risk of a known vulnerability being exploited. Specific steps include:

- Keeping applications patched with the latest vendor patches
- Assessing and ranking newly discovered vulnerabilities
- Following change control procedures with application development and deployment
- Following secure coding guidelines when developing applications
- Using automated vulnerability scanning for public-facing Web applications

Vulnerability scanning tools can help identify vulnerabilities in your systems. Vulnerability scanners are designed to detect weaknesses in applications and operating systems (OSs) that can be exploited by an attacker. Vulnerabilities can arise from the way applications handle improper input (for example, input strings that are too long), from weak encryption mechanisms, and improperly configured network ports. Some tools include pre-packaged scans designed for PCI DSS.

Access Controls

Who can have access to credit card data is another issue addressed by the PCI DSS. The requirements in this area include:

- Using the least privilege principle so that users have only as much access to credit card data as they need to do their jobs
- Assigning unique IDs and passwords, tokens, or biometrics to users accessing cardholder data
- Implementing two-factor authentication for remote access
- Authenticating access to any database containing cardholder data
- Using automated access control systems to enforce the other requirements
- Using physical controls and monitoring to limit access to systems.
- Tracking visitors and using logs to track physical activities
- Maintaining controls over the distribution of media with protected data

These security controls can limit access to users, but we also needs to ensure these controls are in place and working. Monitoring and auditing are also required.

Monitoring and Auditing

The monitoring and auditing sections of the PCI DSS requirements define measures to help ensure other controls are working properly. Some of the requirements in this area are:

- Implementing audit trails in sufficient detail to be able to recreate root-level actions, access to cardholder data, initialization of audit logs, and other significant events
- Using time encryption techniques to ensure timestamps are correct and consistent across devices
- Ensuring audit trails cannot be tampered with by preventing unauthorized modifications and using file-integrity checking applications
- Performing daily review of logs
- Maintaining audit trail data for at least 1 year

In addition to implementing all of the controls just mentioned and auditing them to make sure they are operating as expected, to be PCI DSS compliant, we also need to have policies and procedures in place that document how and when these measures are executed.

Security Policies and Procedures

The PCI DSS requires documentation and training to ensure that those involved with cardholder data are aware of requirements. The standard also calls for training and communication programs. Security policies that comply with PCI DSS must be in place.

The PCI DSS addresses a wide range of security controls and practices. Compliance is not trivial. Running OSs and applications in default configurations will not meet compliance requirements. Insufficient documentation and training will not meet compliance requirements. Lack of auditing and review will lead to failure to comply. The standards and controls specified in the PCI DSS should be considered minimal requirements. Companies that have been in PCI DSS compliance have suffered data losses. Implementing the PCI DSS will help mitigate security risks, it will not eliminate them.

Focus on SSL Certificates

The full PCI DSS warrants multiple full book-length discussions. For the rest of this guide, we will focus on the role of SSL certificates in meeting PCI DSS requirements. The PCI DSS emphasizes a number of areas, such as encryption and authentication, where SSL certificates play a crucial role. For now, we will focus our attention on those topics.

The Need for SSL Certificates

SSL certificates are versatile digital assets that are used in a range of security measures:

- Network and server security
- Encrypting payment card data
- Access controls

Each of these areas is addressed in the PCI DSS, so you can expect to routinely work with SSL certificates as part of your compliance efforts.

Network and Server Security

Let's consider a hypothetical attack on the card payment processing system. An attacker decides to create a server that appears to be a legitimate server run by a payment processor. The attacker uses email scams and Trojan software to inject code that alters the way IP packets are routed so that instead of going to the legitimate payment processor server, card data is routed to a rogue server controlled by the attacker.

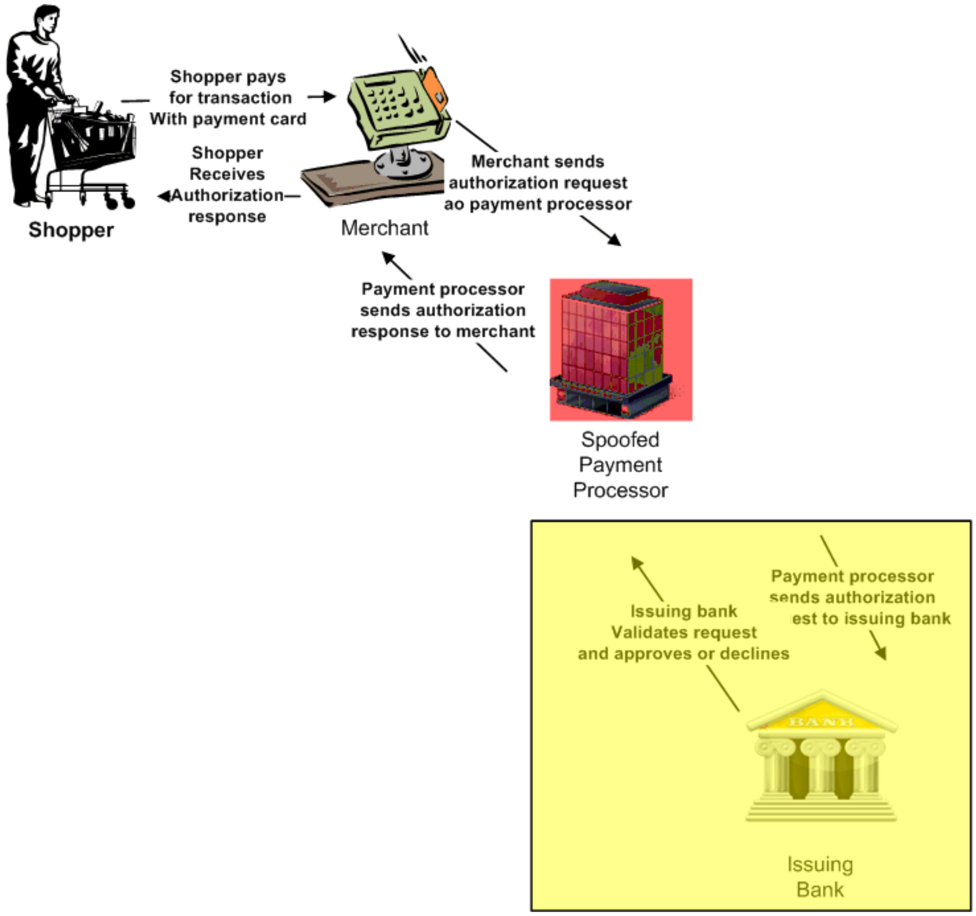

Figure 1.3: Without the ability to authenticate the servers that receive cardholder data, an attacker could launch an attack using a server that appears to be a legitimate part of the card processing system but actually just captures data sent to it. The real payment processor or issuing bank would never process the transaction in this scenario.

In this scenario, the merchant system is depending on either a domain name, for example, AcmePaymentProcessor.com, or an IP address to identify the payment processor's server. Under ideal conditions, the DNS name or IP address would route transactions to the proper server. If there were a breach in any part of the routing process, you might not know where your data is going.

One way an attacker might implement this scenario is to use DNS cache poisoning. DNS services map domain names to IP addresses. Internet service providers (ISPs) can provide DNS services; you might use a specialized DNS service provider or even maintain a DNS server in your own organization. If an attacker is able to exploit a vulnerability in the DNS system and change the address associated with a domain name, your traffic may be rerouted to a malicious site. DNS is an essential service, but it should not be used as a substitute for authenticating a server you are about to send confidential data to.

Depending on networking services to always route transactions securely and properly to your business partners is insufficient when you need to protect the confidentiality of your data. You need to authenticate devices before you send business partners data, and doing so requires an SSL certificate. SSL certificates are provided by trusted third parties and designed for specific servers or domains. Rather than assuming the network will send your transaction to the right destination, you can verify that the server you are communicating with holds a certificate that a trusted third party would grant only to the party described in that certificate.

Verifying the identity of the server or other device at the other end of a communications channel is just one part of creating a secure and trusted communication channel (see Figure 1.4). We also need to ensure that no one can intercept communications as data is sent from one device to another.

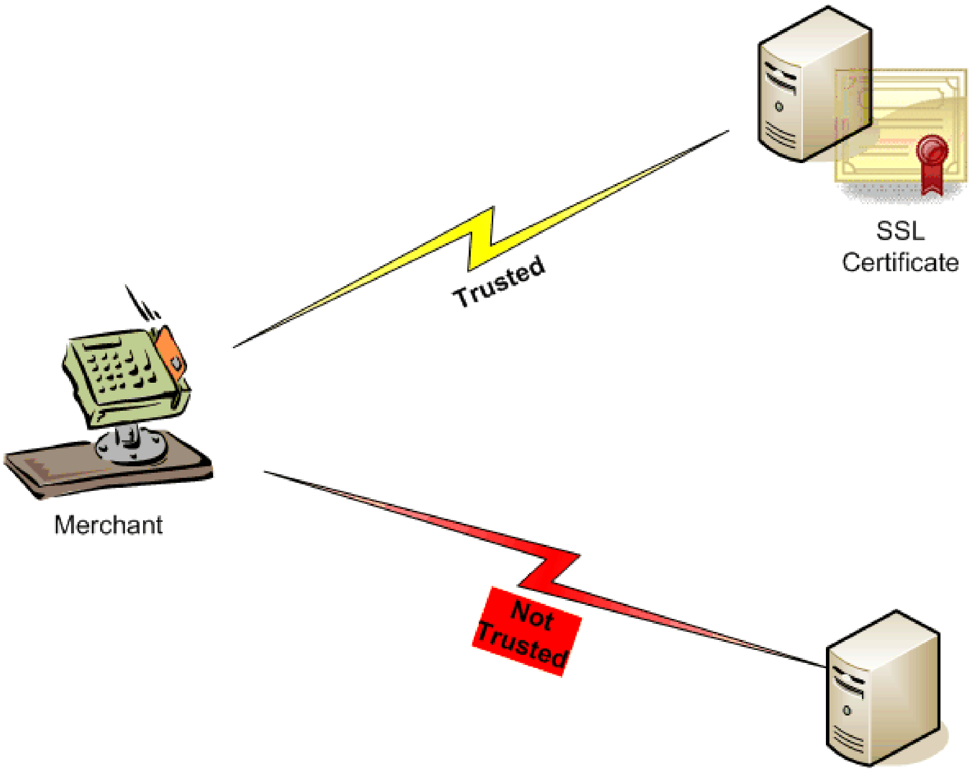

Figure 1.4: Communication partners are trusted when devices are authenticated using SSL certificates. Data must be encrypted as well to prevent eavesdropping attacks.

Encrypting Payment Card Data

SSL certificates also support the use of encrypted communication. There are multiple ways to encrypt data; one way is to use a system known as public key cryptography. This method uses two keys, one to encrypt data and one to decrypt it. The former is known as a public key and the latter is known as a private key. The public key is made available in the SSL certificate used to authenticate the device. Once a device has been authenticated, the two devices can negotiate an agreed-upon protocol for encrypting data for this session. The agreed-upon encryption method is then used to encrypt data such as a credit card number, expiration date, and security. The message will look nothing like the original data, so if it is intercepted in transit, it won't be of much value to anyone else. In theory, someone with enough time and computing power could break the encryption and discover the original data, but strong encryption techniques make that impractical in most cases.

Note

There have been exceptions with older versions of the SSL/TLS standard in which implementation vulnerabilities have been exploited; see The Register's reporting on recent research findings.

Access Controls

We have seen how SSL certificates can be used to authenticate servers and support encryption. They can also be used to control access to services. For example, a payment card processing application may only accept incoming connections from a trusted device or on behalf of someone logging who can verify their identity. SSL certificates can be used to ensure that both parties at either end of a communication session are validated before access to data or services is granted.

SSL certificates enable a combination of authentication and encryption services that are required by the PCI DSS. In the following chapters, we will delve into implementation details and practices to help you plan, deploy, and manage SSL certificates in compliance with requirements.

Summary

The payment card industry is the target of substantial fraud. Organized cybercrime groups are sophisticated and well established to the point of having created underground markets for credit card fraud software, data, and supporting services. Legitimate businesses have responded with efforts to improve the security of a highly-distributed and decentralized payment card system. SSL certificates play key roles in preserving the confidentiality and integrity of payment card data.