Realtime publishers

The Shortcut Guide™ To

Protecting Against Web Application Threats Using SSL

sponsored by

Symantec™

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: Combined Risk of Data Loss and Loss of Customer Trust

Businesses face an increasingly complex set of threats to their Web applications—from malware and advanced persistent threats (APTs) to disgruntled employees and unintentional data leaks. Although there is no single security measure than can prevent all threats, there are some that provide broad-based mitigation to a number of threats. The use of SSL encryption and digital certificate-based authentication is one of them.

Changes in the way we deliver services, the increasing use of mobile devices, and the adoption of cloud computing compounded by the ever-evolving means of stealing information and compromising services leave Web applications vulnerable to attack. SSL encryption can protect server-to-server communications, client devices, cloud resources, and other endpoints in order to help prevent the risk of data loss. A later chapter provides a step-by-step guide to assessing your needs, determining where SSL encryption and digital certificate-based authentication may be helpful, planning for the rollout of SSL to Web applications, and establishing policies and procedures to manage the full life cycle of SSL certificates. In this chapter, we turn our attention to the combined risk of losing data and losing customer trust.

Evolving Security Landscape

Business information, from customer identity information to trade secrets, is valuable to more than just the business that controls it. Attackers and cybercriminals can exploit weaknesses in IT systems, resulting in data loss, and in some cases, involving public disclosure as well. Moreover, information security attacks are not limited to one or two industries, governments, or even geographic locations. In addition to direct attacks on the interests of businesses, governments, and other organizations, there are cases of malicious attacks that are more like vandalism than theft. These may have less direct costs but can still cause concern about the trustworthiness of online resources.

The evolution of the security landscape is creating what appears to be a global, continuous and cross-industry threat. A number of factors are contributing to the advancement of cyber-security threats:

- The professionalism of cybercrime
- The ability for others to automatically scan potential targets for vulnerabilities
- Emergence of APTs

A complex phenomenon like cyber-security threats has many aspects involving multiple motivations, a wide array of technologies, and many opportunities. We will examine three, assuming that they are a representative sample of the various dimensions of the problem. They are not by any means a comprehensive list of elements that contribute to the evolving security environment we face.

Professionalism of Cybercrime

Cybercrime is a business, literally. If you were an outsider looking in on the operations of the underground market for stolen credit cards and bank credentials and you did not know the illegal origins of the products for sale, it might be hard to distinguish the operations from a legitimate business. Cybercrime has characteristics one would expect in other professions and businesses, including:

- Division of labor
- Market forces
- Diversification
- Growth

The fact that cybercrime has developed these characteristics associated with free markets speaks to the persistence, professionalism, and drive for efficiency in this arena.

Division of Labor in Cybercrime

There is a full vertical industry dedicated to credit card and bank credential fraud that includes, according to the FBI, a well-defined division of labor:

- Programmers who develop Trojans and other malware to steal financial information
- Distributors who establish online marketplaces and sell stolen information
- Fraudsters who develop phishing scams and other social engineering schemes to lure victims into revealing information
- Cashiers and "money mules" (low-level participants who use their accounts in the money transfer process

This division of labor is expected. The skills needed to create a Trojan are different from those needed to write a convincing phishing email. Ironically, the underground market must be based on trust that participants will not violate understood rules of exchange. Within the confines of the Internet crime marketplace, there is a need for distributors who can establish online exchanges and run them in a trustworthy manner. There is also a need to move money out of the underground market and into the business and consumer markets. This job requires a set of skills that allows one to bridge the underground and legitimate markets.

Market Forces

Prices appear to be set in the underground market similarly to the ways prices are set in legitimate free markets: by supply and demand. For example, Panda Security reports on the cost of a number of different "products" in their report The Cyber-Crime Black Market. Stolen credit card details will cost you between $2 and $90 (the price will vary depending on factors such as credit limit, amount of card detail available, time since the number was stolen). Bank credentials cost between $80 and $700; the higher-priced credentials come with balance guarantees. Bank transfer and check cashing services are provided at rates from 10% to 40% of the transaction total. Those criminals that like to operate in the physical realm can purchase credit card cloners for anywhere from $200 to $1000 but a fake ATM card can cost up to $35,000.

Of course, there is competition in the underground market, so there will be innovative ways to distinguish offers based on more than price. The Panda Security report noted offers sometimes come with "try and buy" demos, bulk discounts, and even customer service and support.

Another indicator of the maturity of the market is the way prices for stolen goods are influenced by the laws of supply and demand. Too much supply will drive down prices. In the spring of 2011, the Sony PlayStation network was attacked and information from 101.6 million customers was stolen (Source: https://www.privacyrights.org/data—breach—asc?title=Sony). Sony and their customers were not the only ones concerned about this massive breach—other cybercriminals were concerned that an influx of a large number of new stolen credit cards would drive down the price for their stolen goods. *The New York Times* quoted Kevin Stevens, a senior researcher at Trend Micro as reporting, "There was a lot of discussion taking place in hacker forums about the Sony data breach. Several credit card dealers are worried that the distribution of millions of credit cards would flood the market and lower prices." And a Europe-based hacker who was not further identified indicated, "We're keeping a close eye on the Sony story as it would drastically affect the resale of other cards."(Source: Nick Bolton, "How Credit Card Data is Stolen and Sold", *The New York Times,* May 3, 2011). Given the dynamics of the underground cybercrime market combined with the risk of large swings in supply, it is prudent for the risk-averse cybercriminal to diversify.

Diversification in the Cybercrime Markets

Cybercriminals can diversify in the way they attack their victims and in the way they select their targets. Cybercriminals diversify the distribution of malware and infect devices around the globe. The Anti-Phishing Working Group (http://www.antiphishing.org/) reports that more than 10 million malware samples were detected in the second half of 2010. In addition, at least 10 countries have infection rates greater than 50% (see Figure 2.1).

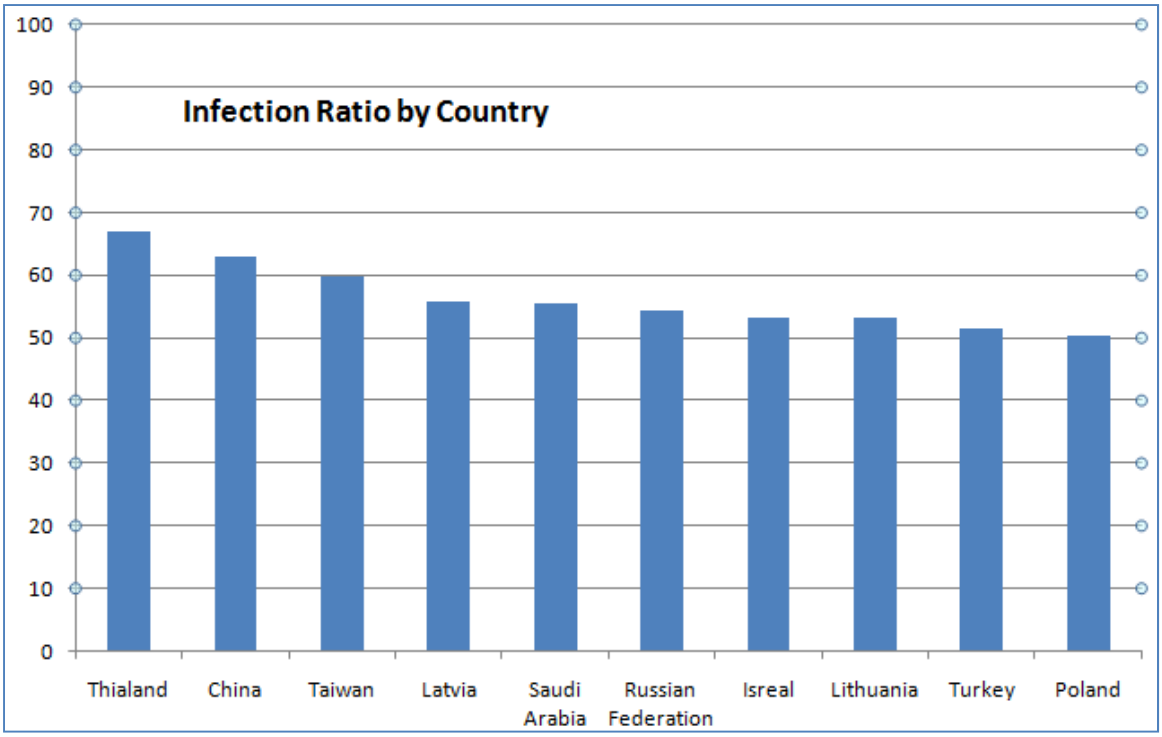

Figure 2.1: High malware infection rates (above 50%) are seen across the globe. The United States ranked 22nd in the list with a 45.32% infection rate.

Diversification is also a factor with regards to victims. At least in the United States, there is a somewhat balanced distribution in the age of cybercrime victims according to FBI statistics (see Figure 2.2).

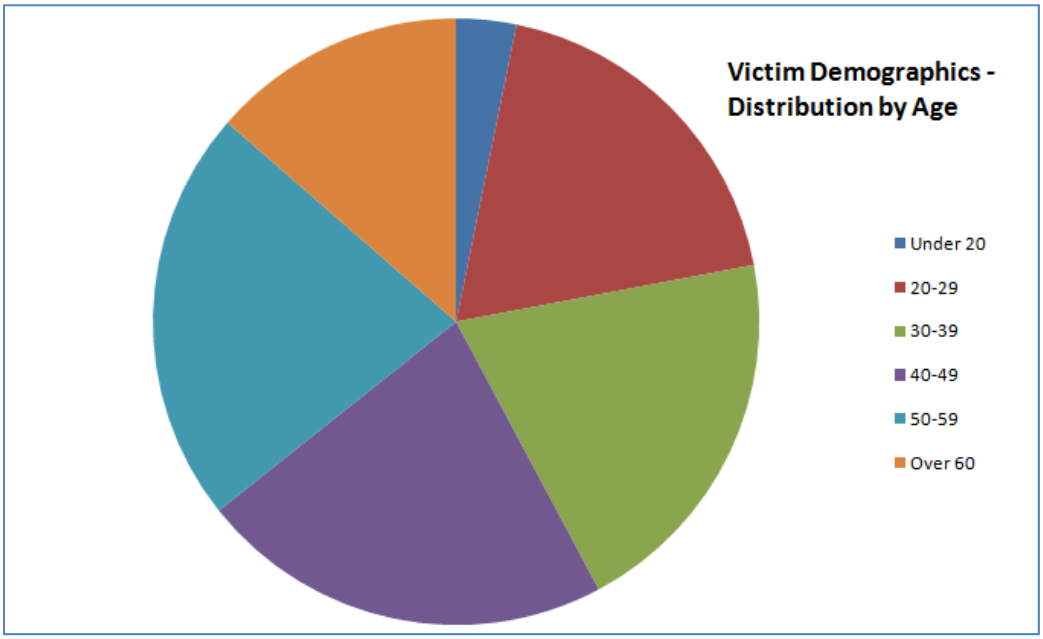

Figure 2.2: Reports of Internet crime to the FBI are fairly well evenly distributed across age groups with under 20 year olds fairing the best.

Criminals are not as diverse in the industries they targets; financial services and payment services are still leading targets for obvious reasons. Figure 2.3 shows the top targeted industries in the fourth quarter of 2010, according to the Anti-Phishing Working Group.

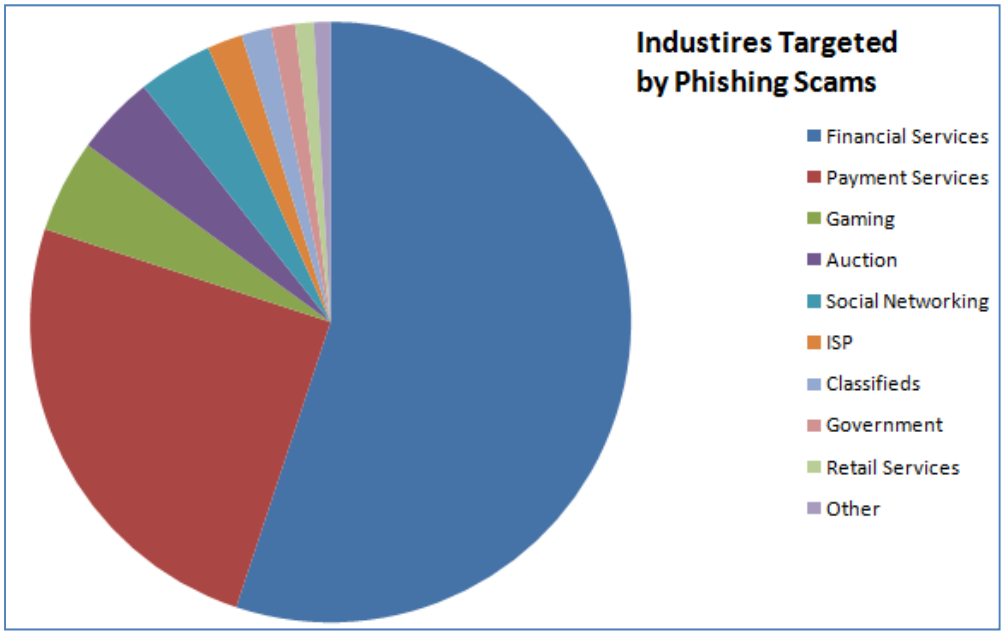

Figure 2.3. Diversity does not extend as much to the industries targeted. Financial services and payment services account for more than three-quarters of phishing scams (Source: Anti-Phishing Working Group, Phishing Activity Trends, 2nd Half 2010).

In addition to diversifying the resources used to commit cybercrime, we have witnessed a growth in the amount of cybercrime.

Growth in Cybercrime

There is little doubt that cybercrime is growing. We have already noted the increasing sophistication of underground markets, the division of labor among cybercriminals, high malware infection rates in some parts of the world, and even the effects of market forces on the criminal enterprise at large. There are also statistics that provide evidence for the increase in the number of cybercrimes. Figure 2.4, for example, shows an increasing number of cybercrimes reported per year between 2000 and 2010.

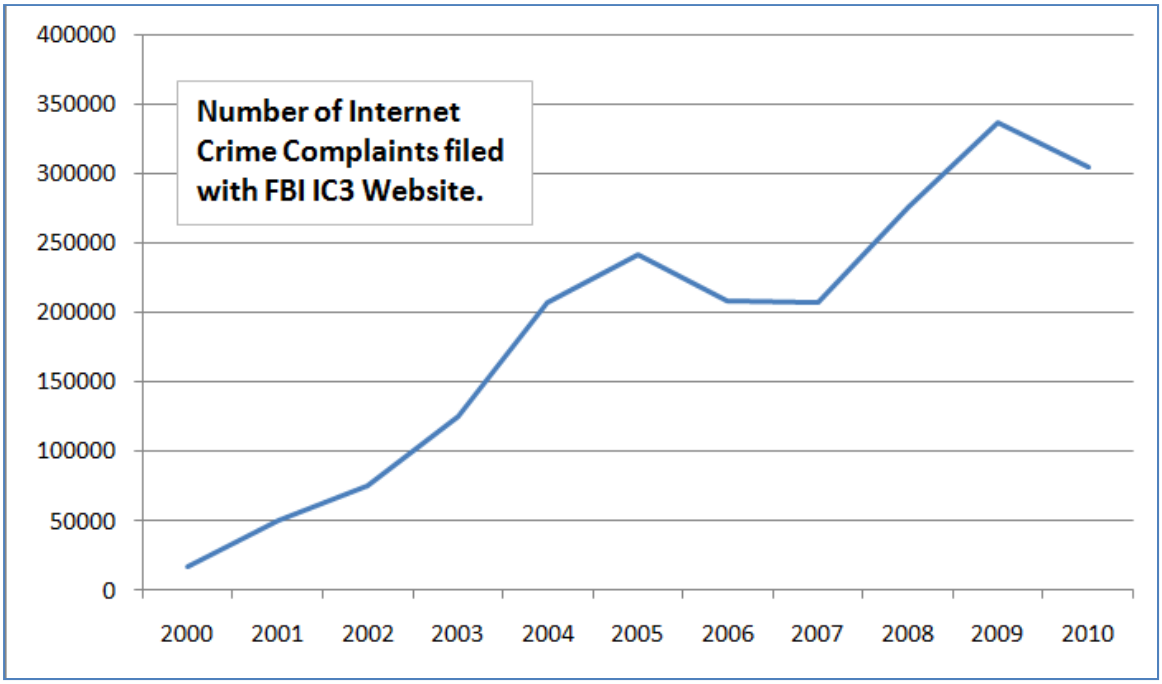

Figure 2.4: The number of Internet crime complaints filed with the US Federal Bureau of Investigation (FBI) is another indicator that cybercrime is an established, on-going, and growing problem (Source: FBI, 2010 Internet Crime Report).

There is a growing supply of malicious software and methods for distributing malware that can be used to execute cybercrimes:

- A few years ago, Panda Security reported receiving 500 new threats per day; today they receive 63,000 new threats per day (Source: Panda Security, The Cyber-Crime Black Market).
- McAfee processed 55,000 pieces of new malware every day in 2010 (Source: http://blogs.mcafee.com/corporate/cto/global—energy—industry—hit—in—night—dragon—attacks).
- In the 15-year period from 1991 to 2006, Panda Security compiled a database of 92,000 strains of malware; in 2009, that number reached 40 million; and in 2010, the number jumped to 60 million (Source: Panda Security, The Cyber—Crime Black Market).
- Symantec has found that enterprising attackers buy ad space and use traffic distribution systems (that is, vendors that buy and sell Web traffic), avoiding the need to infect Web sites. This process has become another common method for distributing malicious code (Source: Symantec, Web-Based Malware Distribution Channels: A Look at Traffic Redistribution Systems).
- The increasing use of shortened URLs helps to mask malicious sites. In one study of malicious shortened URLs posted to social networking sites, 88% of the malicious links were clicked at least once (Source: Symantec, Taking the Shortcut to Malicious Attacks).

The extent of cybercrime and the means by which it is executed are both growing and, unfortunately, there is little in the data to suggest the trend will change in the foreseeable future. In fact, as Symantec has summarized, the threats in the past decade have become increasingly sophisticated; see A Decade in Review: Cybercriminal Motivations behind Malware for a timeline of major cybercrime events in the past 10 years.

Cybercrime is clearly a well-established, professional, and illegal industry. Business data, especially personal consumer data, is a highly-valued target. This puts pressure on businesses to protect that data, and well-publicized data breaches can lead customers to question the protections in place around their information. This reality ultimately undermines trust in the ability of the business to perform online transactions without compromising personal information.

Automation of Vulnerability Scanning

The proliferation of cybercrime has been enabled, in part, by the emergence of a professionally-run cybercrime market. Another factor in favor of cybercriminals is the availability of technology for vulnerability scanning. One can imagine a (false) sense of security you could develop by assuming that with all the devices on the Internet, what are the chances an attacker would find one of my servers and detect an unpatched application or a misconfigured service? This kind of reasoning fails to account for security tools that can be used to help lock down devices or exploit them.

Automated vulnerability scanning tools can be used to discover devices, assess configurations, detect access to sensitive data, and determine whether a vulnerable version of an application with a known vulnerability is running on a device. Vulnerability scanning tools are valuable to security and network professionals working on identifying and correcting weaknesses. They are equally useful for cybercriminals in identifying and exploiting weaknesses.

Cybercriminals function under similar business drivers as legitimate businesses, including the need to perform operations more efficiently and to develop business practices that allow them to scale to market demands and opportunities. Automation of repetitive tasks, such as looking for vulnerabilities in Windows and Linux servers, is one way to improve attacker productivity. Automated vulnerability scanning can be used to scan a wide range of IP addresses looking for vulnerable systems and applications or they can be used in more targeted attacks.

Emergence of APTs

A common motive in modern heist movies is the need for strategic planning and detailed tactical moves before the theft can be accomplished. Movies about 1920s bank robberies could work with a handful of bank robbers rushing into a bank with guns and minutes later running out to the getaway car with bags full of cash. That storyline needs to be revised in order to seem realistic by today's standards. Security at modern banks, casinos, and other likely targets demand more insider knowledge of weaknesses and finesse when it comes to execution. This applies to cybercrimes as well.

Well-funded and determined attackers can use an attack structure known as an APT to breach security of a highly valued target. APTs are characterized by:

- Targeting a single entity
- Intelligence gathering
- Multiple modes of attack
- Incremental breaches
- Exploiting humans with social engineering attacks

Malware plays a central role in APTs, but they are more than viruses. Malware can be injected into a victim's device by luring the victim to a site controlled by the attacker and convincing the victim to download a file or by finding a weakness in perimeter defenses or a vulnerability in an application that allows malware to be injected. Chances of an antivirus program detecting the malware are reduced by the fact that malware developers can test their Trojans and other malware against antivirus software before it is deployed and craft the malware to avoid detection.

The scope of an APT can be substantial:

- In 2009, a coordinated attack using social engineering, intelligence gathering, breaches of perimeter defenses, and SQL injection attacks were used against oil, gas, and petrochemical companies. The attack targeted resources and personnel in the United States, the Netherlands, Kazakhstan, Taiwan, and Greece (Source: McAfee, "Global Energy Cyberattacks: Night Dragon", Feb. 10, 2011).
- In 2010, researchers discovered a coordinated attack on business, government, and academic computers targeting politically-sensitive information related to the Indian government and the Dali Lama's office (Source: Info—War Monitor, "Shadows in the Cloud: An investigation into cyber espionage 2.0").
- In 2011, McAfee reported on Operation Shady Rat, a multi-year APT that targeted more than 70 business, government, and even non-profit organizations (Source: McAfee, "Revealed: Operation Shady Rat").

Not all APTs are broadly targeted, though. In 2011, Symantec made public its analysis of the Duqu malware, which uses pieces of the well-known Stuxnet malware that targets industrial machinery controls. Duqu is designed to gather intelligence on specific industrial targets (Source: Symantec, Duqu: The Precursor to the Next Stuxnet). Such attacks may not garner attention-grabbing headlines but they pose significant risks to the targeted victims.

The impact of APTs can be substantial because intellectual property is often the target. Competitors who can steal bids for major contracts or product designs can negate any competitive advantage the victim may have had. Until recently, APTs have not garnered the attention of the press in the same way data leaks do. Reporting on the loss of millions of customers' personal data is relatively easy, but tracking down and explaining the details of a long-term, sophisticated cyber attack is much more difficult.

The evolution of cybercrime has reached a point where threats are continuous, targeted, and increasingly well known. Data breaches are readily understood even for those without a background in IT, and can undermine confidence in customers' ability to conduct business online. The sophistication of APTs threatens businesses ability to conduct internal operations without loss of information confidentiality and information integrity. Next, we will examine ways in which confidentiality and integrity can be compromised.

Risk of Data Loss and Threats to Information Security

Data loss can occur in many ways, from eavesdropping and mistaken identities to insider abuse and improperly managed access controls.

Intercepting Communications

Communications and data transfers can follow many routes from one point to another. Remote sites and traveling executives may have to use the public Internet to access resources at corporate headquarters. This can present an opportunity for an attacker who has targeted that business or executive. Unless the communications are encrypted, typically using an SSL-based mechanism, it is at risk of interception by a man-in-the-middle attack (see Figure 2.5).

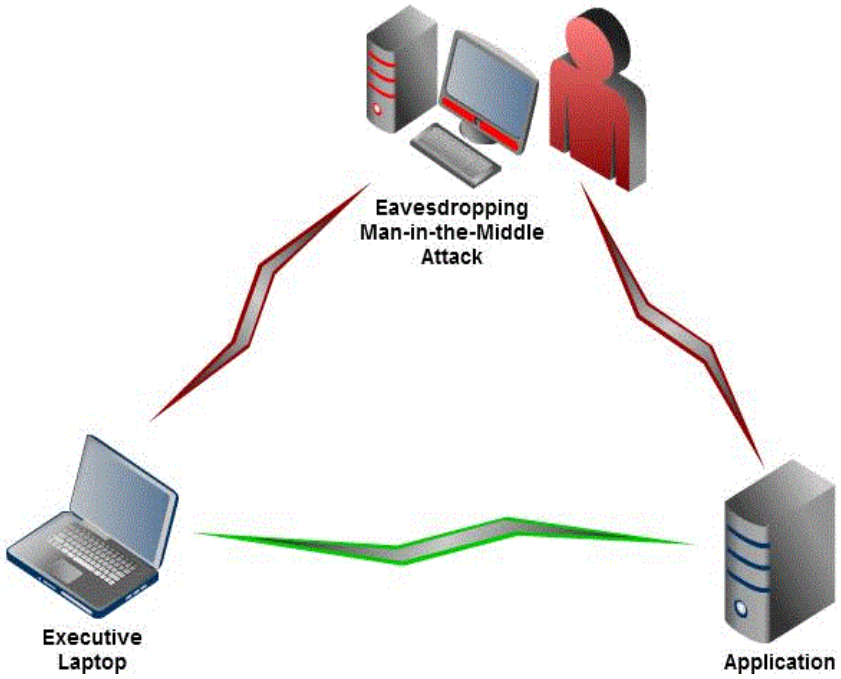

Figure 2.5: Unencrypted communications can be intercepted using a man-in-the-middle attack. A user believes there is a direct and secure line of communications (green) when in fact the line of communication is being intercepted (red).

This type of attack can be avoided by deploying communication services that encrypt data before it is sent over the Internet. Virtual private networks (VPNs) can do this for all network communication. Alternatively, users can establish secure connections to servers that have an SSL certificate and can establish encrypted communications channels with other devices.

Spoofing

Spoofing is another way of stealing information that depends on tricking users into believing a malicious server or other device is actually a legitimate device. Spoofing can be avoided by deploying SSL certificates on servers. Doing so allows users to authenticate the server (that is, verify the server is actually the one it appears to be) before transmitting sensitive data. SSL certificates can be provided by trusted third parties who verify the identity of the organization requesting the certificate. The certificates are designed to identify a server (or group of servers depending on the type of SSL certificate). If a digital certificate for one server was stolen and placed on another server, a warning message would be generated during the authentication process.

Common Internet browsers are all configured with information about the major SSL certificate providers. If a user were to navigate to a spoofed server with an invalid certificate, the browser could immediately display a warning indicating the spoofed server is not actually the one it purports to be.

Directed Attacks: APTs and Insider Abuse

Another set of risks to businesses, governments, and other organizations is directed attacks. In addition to APTs, another potential avenue of data loss is insider abuse.

Insiders are employees, contractors, and others with legitimate access to information. The ways insiders can steal or leak sensitive data is limited only by their imagination. The Privacy Rights Clearinghouse (http://www.privacyrights.org) maintains a database of breaches that includes details on the ways data is lost. Some of the more recent cases of insider abuse have included:

- A waiter stealing credit card details of customers.
- A Veterans Affairs worker using personal patient information to create fraudulent dependent information and then using his tax preparation business to submit fraudulent tax returns.
- A medical center employee stealing information about persons responsible for medical bill payment, which was then used by co-conspirators to open credit cards and obtain cash advances.
- A bank employee disclosing customer names, Social Security numbers, driver's license numbers, bank account numbers, and other details to co-conspirators in an identity theft ring.

Even when sound practices are employed, such as limiting access to data to only those that need it and separating duties to reduce the risk a single person could commit fraud, determined insiders can still succeed in stealing sensitive information.

Improperly Managed Access Controls

Another risk for data loss comes from improperly managed access controls. A telling example was recently reported by the Associated Press in "New Data Spill Shows Risk of Online Health Records." The article describes a case in which medical information about 300,000 Californians was available for public viewing. A privacy researcher, Aaron Titus, found the information using Internet searches and then contacted the firm hosting the data (as well as the press). The data was intended to be used only by employees with legitimate need for the data, but proper access controls were not in place, in violation of the firm's policies.

Poorly managed and implemented access controls will not necessarily result in public disclosure but they can create additional risks nonetheless. For example, when an employee who is responsible for accounts payable is transferred to work on accounts receivables, his access permissions should be revised to prevent access to accounts payable systems. Failure to do this can undermine the separation of duties principle and create an opportunity for abuse. There are a wide variety of risks to the confidentiality and integrity of data, from intercepted communications and spoofing to insider abuse and mismanaged access controls.

Impact of the New Security Landscape on Customer Trust

We could easily keep our focus on the internal consequences of the new security landscape. We could concern ourselves with hardening our defenses, improving our auditing and monitoring procedures, and other measures that reduce the risk that an attack would be successful. We could do this and we would be justified in doing it, but we would also be missing an important aspect of these risks: their impact on customer trust.

Well-Publicized Data Breaches and Attacks

You do not have to be an IT professional to be aware of the state of information security these days. The popular press seems to have an almost steady stream of stories about security risks, data breaches, and hacking attempts.

It is not just the American press that is publishing information security stories; this is a global phenomenon:

- The Hong Kong Stock Exchange suspended trading on seven stocks after the exchange's Web site was attacked and "sensitive results" were released according to TG Daily (Source: Hong Kong Stock Exchange Hacked, Aug. 10, 2011).
- Private information on 35 million customers of Epson Korea was stolen after the company Web site was hacked. Information disclosed included "names, user IDs, passwords and resident registration numbers" according to the Yonhap News Agency (Source: Epson Korea says 35 Million Customers' Data Hacked, Aug. 20, 2011).

Stories about financially motivated attacks are complemented by what might be called human interest cybercrime cases:

- *The Guardian* reports on a case demonstrating that attacks are not always financially motivated, describing a 33-year-old attacker's actions, "He accessed highly personal data and photographs in a sophisticated email scam from his mother's front room, taking control of some victim's webcams remotely to see inside their homes, at one point boasting to a friend that he made a teenage girl cry by doing so." (Source: Computer Expert Jailed after Hacking Victims' Webcams, Nov. 23, 2010).
- Following the phone hacking scandal at the British newspaper *News of the World* that became public in the summer of 2011, Scotland Yard began an investigation into computer hacking by the organization, according to *The Guardian*. This was spurred in part by allegations that a former army intelligence officer received an email with a Trojan program that copied emails from the victim and sent them to the attacker (Source: Scotland Yard to Setup up New Computer Hacking Task Force,, July 29, 2011).

Governments and political organizations have also been targeted for organized attacks. Examples include:

- Deutsche Welle reports in 2010 that new national identity cards provided to German citizens which were supposed to improve security for online transactions were easily hacked by members of the Chaos Computer Club (Source: New German ID card easily hacked by ordinary computer nerds, Sep. 23, 2010).
- A Taiwanese presidential campaign was attacked and the attack targeted planning information. Police were investigating allegations that the attackers were "backed by the Chinese state" according to the Times of India (Source: Taiwan Police Probe China Hacking Claim, Aug. 11, 2011).

Based on even this small sample we can begin to see that the concern about data breaches and persistent cybercrime exists to some extent anywhere there is Internet access and online transactions.

Well-Publicized Cybercriminal and Hacking Organizations

Decades ago, only insiders would recognize the name of hacking groups like the Chaos Club, but today, groups like Anonymous and LulzSec are making headlines along with more threatening organizations, such as the "Russian Business Network" (RBN) and state-sponsored groups.

LulzSec has claimed responsibility for stealing information from law enforcement agencies, most notably the Arizona Department of Public Safety, as well as businesses such as News Corporation. When compared with organized crime syndicates which commit cybercrimes, groups like LulzSec are more akin to vandals than serious felons. Anonymous has made news with public releases of stolen documents from Bank of America and attacks on Sony, both in response to what the group considered objectionable corporate behavior.

Other organized groups are far more threatening. The RBN is reported to be a group based in Russia that has a history of developing malware, conducting Denial of Service (DoS) attacks, and providing spam services. They have also been implicated in the theft of tens of millions of dollars from Citibank in 2009 (Source: *ComputerWorld*, "Report: Russian Gang Linked to Big Citibank Hack," Dec. 22, 2009).

More recently, news stories highlighted Operation Shady Rat, the widespread APT attack on more than 70 organizations, and Night Dragon, the target attack on gas, oil, and petrochemical companies. These attacks have implicated state actors.

Stories about organizations ranging from cyber-vandals to state-sponsored cybercriminals will likely add to the popular concern about information security generated by a near continuous stream of stories from around the globe about data breaches and cyber attacks. This is not just a law enforcement problem or a public policy issue. How we as consumers and customers respond to these threats can directly impact the effectiveness of online services.

Potential Impact to Building Trust Online with Customers

Customers are justified if they are concerned about the security of their personal and financial information online. It is not unreasonable to think that customers will make choices based on how well they think a company will protect their information in much the same way they now consider price, product quality, and customer service.

Businesses should consider how new evaluation criteria that include security considerations will affect them. One can begin by understanding the security concerns customers may have, such as:

- Concern for identity theft
- Concern for credit card fraud
- Loss of privacy

Organizations such as banks and hospitals that require more personal and financial information than many businesses are likely to be especially aware of concerns about identity theft. Businesses that provide services to banks, hospitals, governments, and similar organizations that may house substantial amounts of confidential information must ensure it stays protected. For example, the inadvertent release of patient data in California occurred at a firm providing services to medical providers; it was not a medical provider itself.

The need to protect credit card information is more widespread. Many of us use credit cards and debit cards routinely during the day. The payment card industry has established data security standards that card processors must comply with. These are designed to protect both customers and banks from fraud and abuse. The payment card industry is built on a web of trust. Customers and vendors trust the bank to pay the vendor, banks trust customers to pay their bills, banks trust vendors to charge accurately, and they all trust each other to maintain the integrity of the system.

The loss of privacy can be even more of a threat to some people than the financial risk associated with credit card fraud of identity theft. Someone with a history of psychiatric treatment may fear for his job if an employer were to find out about it. Someone who lives in fear of abuse may not want her address disclosed. The disclosure of private information can have unknown and severe consequences for customers, clients, and patients.

Information security threats are real and substantial. Customers would not be irrational to consider how they can best protect themselves from personal or financial harm, and that may include assessing which businesses to trust with their information.

How Businesses Can Respond to Information Loss

It is clear that it is in the best interest of businesses, governments, and other organizations to mitigate the risk of information loss. The question is How? Answering that question is the subject of many books, articles, conference presentations, and other resources—which is an indication of just how difficult the task is.

Although we cannot give a detailed answer to that question, we can outline some of the characteristics of the answer. First and foremost, there is no single solution, no silver bullet. Protecting information in today's online eco-system requires a wide array of security controls and measures, such as:

- Reliable and trustworthy authentication of persons and devices
- Strong encryption for data at rest and data in transit
- Access controls appropriate with the need to perform business functions
- Separation of duties
- Malware protection
- Properly configured and patched operating systems (OSs) and applications
- Constant monitoring and analysis
- Vulnerability scanning and automatic remediation to correct known vulnerabilities
- Intrusion detection to detect potentially malicious activities

In addition to these technical measures, organizations should have well-defined policies and procedures in place that document when to use authentication mechanisms such as SSL certificates, what kinds of information should be encrypted, and what kinds of monitoring procedures should be in place. Policies that are not enforced are of no help. Governance practices need to be in place to ensure that policies are implemented as expected. It is little consolation to a customer who has her personal financial information disclosed that the business had an outstanding privacy protection policy but it just wasn't followed.

Many of these measures are essentially "behind the scenes" from the customers' perspective. Security provided by SSL certificates, like authenticating a server or encrypting a browser session, is visible to customers, thanks to cues like locks and green bars used with Extended Validation SSL Certificates, as Figure 2.6 shows. (There will be more on this topic in the next chapter).

Figure 2.6: Visual cues, such as the lock and green-colored text can help to indicate to customers that a site has been authenticated and communication between the browser and the Web site are encrypted.

Summary

Businesses face a double threat from cybercriminals: the loss of information and the loss of customer trust. You do not have to be an IT professional to have an understanding of the risk of data losses and the subsequent fraud and identity theft that can follow. The security landscape is becoming increasingly complex and threatening. Cybercrime is highly professional, to the point where underground markets function much as legitimate business markets do. Organized crime and state actors are realizing the benefits of information theft. The potential payoffs are substantial and as a result organized entities are willing to spend considerable time and money to launch APTs. Meanwhile, the public catches glimmers of what is happening through a fairly steady stream of news stories from around the globe about data breaches and hack attacks. In addition to security measures, businesses can help mitigate the impact of cybercrime by taking steps to build and preserve customer trust.

Chapter 2: How SSL Certificates Can Protect Online Business and Maintain Customer Trust

What underlies SSL certificates is a well-established method for securing communication and authenticating services. To better understand how SSL certificates can protect online business, it helps to know something about the inner workings of SSL. Working with SSL certificates is a bit like driving a car—you do not need to be an auto mechanic to drive a car, but it can help to know the basics of how your engine and transmission work.

This chapter is organized into three sections:

- How SSL certificates work
- Web applications with and without SSL certificate protection
- Authentication and trust

The first section looks under the hood of an SSL certificate to describe its components and how they work to secure communications and support authentication. The second section continues the look-under-the-hood approach and considers how an application without SSL certificate protections operates differently than one using SSL certificates. In the third section, continuing our regimen of delving into the implementation details of SSL certificates, we look at how SSL certificates are created, the different types of SSL certificates, and the role of SSL certificate providers in establishing and maintaining a trust relationship between providers of SSL certificates, businesses that use them, and customers that expect the kinds of protections they provide.

How SSL Certificates Work

When we receive an SSL certificate from a provider, we receive a file. That may seem like a bit of a letdown at first. After all, this is something that will be used to encrypt communications and provide evidence for identity claims of servers. These are fairly important tasks, and they are all enabled because of one small file? Well, yes and no.

Yes, the SSL certificate file is essential for providing encryption and authentication services, but it is really just one part of a more complex set of protocols. Actually, an SSL certificate by itself would be of little use to you if it weren't for the established protocols that make use of the information stored within the SSL certificate file. The important security tasks are not enabled solely because of an SSL certificate file. It is the combination of the SSL certificate and the protocols that define how it is used that provide the security controls we seek. Let's take a look inside an SSL certificate and then examine the protocols that make use of it.

Components of an SSL Certificate

Figure 2.1 show the components of an SSL certificate. SSL certificates use the X.509 certificate structure, which includes information about the subject, such as a domain, and the encryption algorithm used to create encrypted data that can uniquely identify an entity (these are known as signatures):

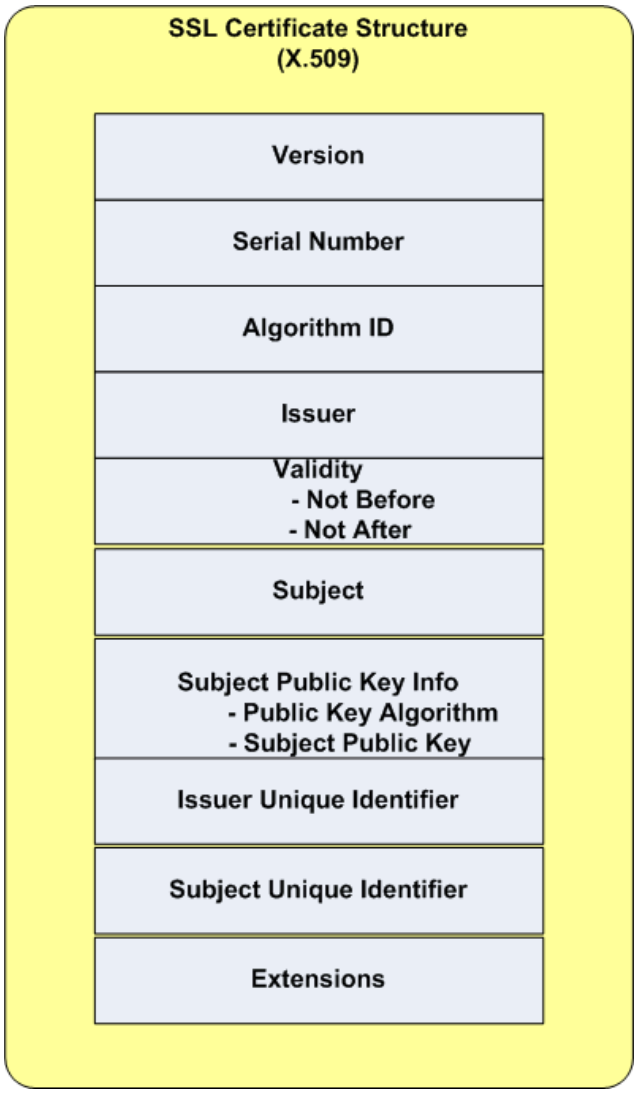

Figure 2.1: The data structure for representing an SSL certificate is based on the X.509 certificate standard.

- The version number indicates which version of the X.509 specification is used. Newer versions support additional extensions and a unique identifier.
- The serial number is a unique number assigned by the certifying authority that issued the certificate. Certifying authorities are responsible for tracking these numbers so that the combination of issuer and serial number is unique across all X.509 certificates.
- The algorithm ID (referred to as a "signature" in the X.509 specification) is the identifier of the algorithm used by the certifying authority to generate the certificate.
- The issuer is the name of the certifying authority that issued the certificate. In addition to the name of the issuer, this field can contain the location of the issuer and the organizational unit within the issuing company that was responsible for creating the certificate.
- The validity section includes two dates, one marking the start period for which the certificate is valid and one indicating the end date that it is valid.
- The subject field is the name of the entity requesting the certificate. This name is in the form of a distinguished name that is unique to that entity within the certifying authority. Like the issuer field, this attribute can contain information about the subject's location and the organizational unit within the entity that requested the certificate.
- The subject public key field contains a public key, which is a string of characters, and the name of an algorithm with which the key is used. Why do we need this string of characters known as a public key? This key is part of the technology known as public key cryptography. We do not need to delve into too many details, but it is important to understand the basics. Here is how it works: When someone wants to send you an encrypted message that only you can read, that person would get your public key from your digital certificate. (Actually, she would use a program such as PGP to do this). With that key and the name of the encryption algorithm, the person can then encrypt the message. The public key is not like a key used to open and lock doors. The public key is a one-way key. It's only good for "locking" (that is, encrypting) but it cannot be used to "unlock" (that is, decrypt) the message. For that, we need a private key.
- The private key is created at the same time as the public key. You can share your public key with anyone who might want to send you an encrypted message and you do not have to worry about them reading an encrypted message someone else sent to you. The only way to decrypt a message encrypted with a public key is to use the corresponding private key. As long as no one else has your private key, they cannot read your encrypted messages.

With Enough Time and Resources

It is not theoretically impossible to read someone else's message without the private key. If you have enough cryptographic knowledge and access to large-scale computing resources (think large secret-government-agency-level resources), you could eventually decrypt a message without the private key. Unless you are passing around state secrets, the value of the decrypted message probably would not justify the time and expense necessary to try to crack the message. By one estimate, if you could check a billion (1,000,000,000,000,000,000) AES keys per section it would take 3,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000 to try all possible keys (Source: Wikipedia, Brute Force Attack).

- The issuer and subject unique identifiers are used to store identifiers that would uniquely identify an issuer or subject in cases where the name of either entity is reused.
- Extensions were added in version 3 of the X.509 standard and support the use of additional attributes that can be used to store several common extensions as well as private information used within a community of users.

X.509 Certificate Specification

For a more detailed and formal description of the X.509 certificate, see the Internet Engineering Task Force RFC at http://www.ietf.org/rfc/rfc2459.txt.

An SSL certificate contains three broad types of data:

- Information about the subject that owns the certificate and is identified by it
- Information about the certifying authority that issued the certificate
- Cryptographic information such as the subject key and algorithm

You can examine certificates on your Windows devices using the Microsoft Management Console (MMC) and the Certificates Management snap-in (see Figure 2.2). Even if you haven't installed any certificates yourself, you can still view certificates that are installed with the Windows operating system (OS). These are typically for trusted entities like certifying authorities. Your organization may also have installed additional certificates.

Resource

If you are not familiar with the MMC, see Microsoft Management Console 3.0 at Microsoft Technet.

Now that we've covered what is in an SSL certificate, let's take a look at how this information is used.

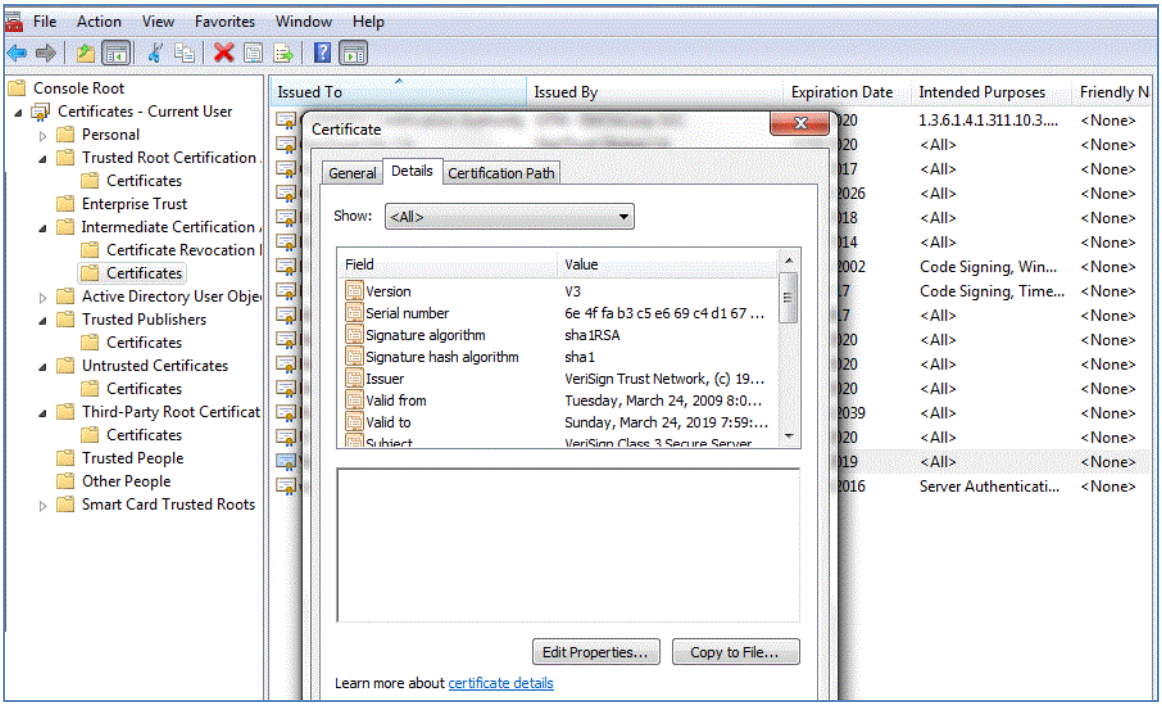

Figure 2.2: The MMC Certificates snap-in tool provides a viewer for reviewing the contents of SSL certificates.

Overview of How SSL Certificates Secure Communications

SSL certificates play a key role in establishing secure communications. They actually provide two services: identifying a party in the communication and providing a public key that can be used to encrypt messages sent back to the server. As we will see, the public key is used to set up a secure communication channel, which is then used to further exchange information and establish an efficient and secure channel for exchanging data.

> **SSL and TLS: A Rose by Any Other Name?**
>
> The Secure Sockets Layer (SSL) protocol is the predecessor of the Transport Layer Security (TLS) protocol. They both are used for securely communicating over the Internet. Although they are different protocols, the general descriptions here address concepts common to both. "SSL certificates" is a common term used to describe digital certificates used for encryption and authentication, so this guide will use the term "SSL" as synonymous with "TLS," as is typically done.

When you navigate to a server using a secure protocol, such as Hypertext Transfer Protocol over SSL (HTTPS), your computer, which we'll refer to as the client, will perform a handshaking protocol to set up a secure communication channel. The steps are as follows: The client requests a secure connection to a server and presents a list of security mechanisms it supports. These are known as encryption cipher suites that have functions that the client can work with. From the list, the server chooses the most secure option that it is able to support and sends its choice to the client. The server sends its SSL certificate, which includes the server's name, public key, and the identity of the certifying authority. Next, the client might send a message to the certifying authority to verify that the certificate is still valid. This option is available because it is possible for a certificate to be revoked during its valid period. Revoked SSL certificates can be checked using either the Online Certificate Status Protocol (OCSP) or certificate revocation lists (CLRs).

At this point, the client has authenticated the server and agreed on a cipher suite. The server may optionally request a client's certificate for mutual authentication. This is more likely in cases where the client should be known, such as when using a virtual private network (VPN); mutual authentication is less likely in cases where the client is contacting a public Web site set up for general commerce (see Figure 2.3).

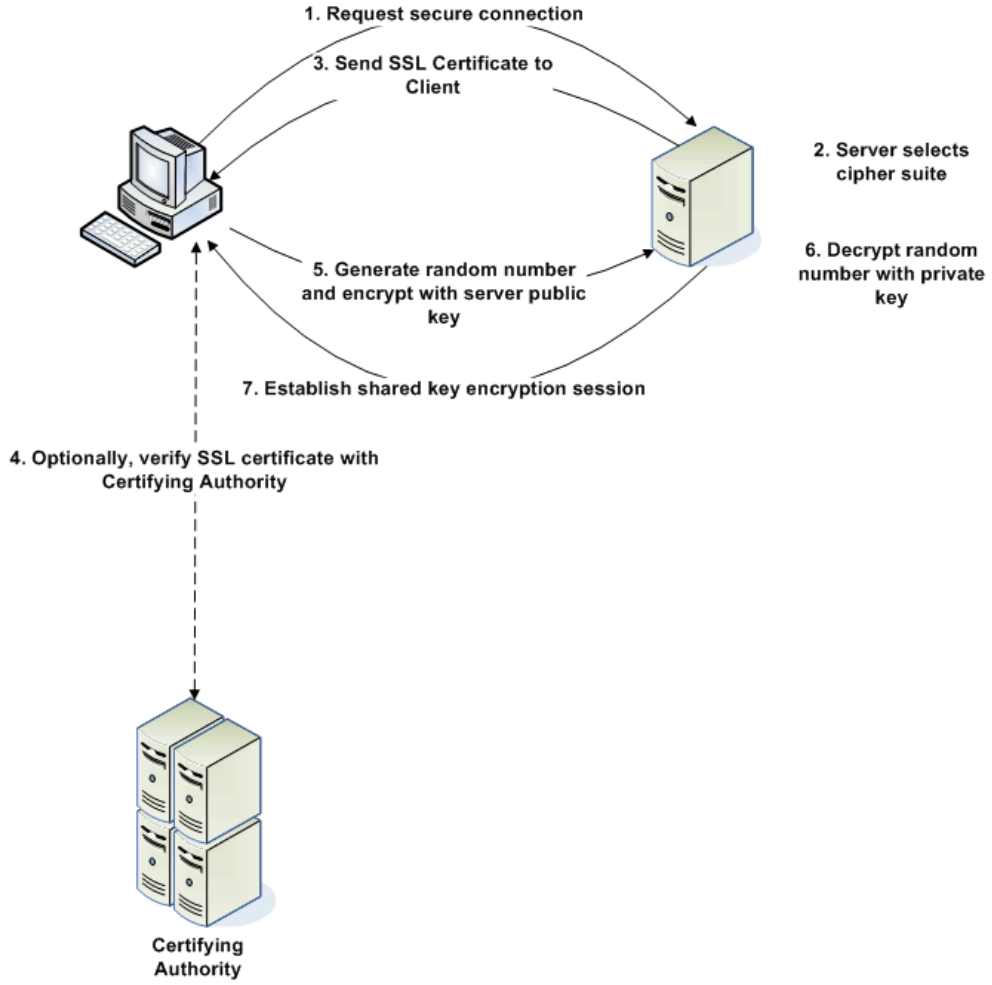

Figure 2.3: Steps to establish a secure connection using SSL certificates.

After the client and server have a secure channel, they can securely exchange information that allows them to create a secure session that is more computationally efficient. The more efficient methods, known as symmetric key cryptography, are faster but require both the client and server to know about a shared key. The next steps allow the client and server to securely exchange such a shared key:

- The client generates a random number and encrypts it with the server's public key.
- The server decrypts the encrypted random number using its private key.
- The client and server establish a secure communication using a shared key and an encryption method that requires only one key for both encryption and decryption.

After completing these steps, the client and server are ready to securely exchange data.

Overview of How SSL Certificates Support Authentication

Peter Steiner's iconic 1993 New Yorker cartoon of a couple of dogs in front of a computer with the caption "On the Internet, nobody knows you're a dog" captures a fundamental problem with the Internet: How do we know who we are interacting with? Let's skip the philosophical issues about how we can know something and settle for trusting that someone (or something like a server) is who or what it purports to be.

We have a bit of a circular problem here. We want to know how we can trust someone online when we don't trust them in the first place when they assert to be someone or something. Any of us can set up a server and put up a Web page proclaiming to be a bank. We might even produce an authentic-looking site by copying pages from a real bank. How will customers know the difference? They will know because we will not be able to get an SSL certificate from a trusted certifying authority that vouches for our identity. The major browsers change the display of the navigation bar when displaying content from a site that uses SSL for identification and encryption (see Figure 2.4). Locks are used to indicate encrypted communication. The "green bar" indicates the use of a special type of SSL certificate known as Extended Validation (EV) SSL certificate, which we'll talk about a bit later in this chapter.

Figure 2.4: Browsers automatically change the navigation bar display when rendering content from a site with a trusted SSL certificate using encrypted communication.

The changes in the browser display are a visual cue that the site has an SSL certificate that has been provided by a trusted certifying authority. Browsers come preconfigured with a set of trusted certifying authorities. When a connection is made to a server, the server sends its SSL certificate to the browser. The browser then makes a number of checks:

- Verifying that the domain name of the site matches the domain name of the SSL certificate
- Verifying the current date is within the valid date ranges
- Checking the issuer and verifying it is one of the trusted certifying authorities known to the browser

When a certificate is issued by a certifying authority that is not trusted by the browser, most browsers will display a warning message (see Figure 2.5).

Warning messages such as the one that Figure 2.5 shows as a rule should not occur when working with trusted commercial or government sites. You are likely to see a warning if you navigate to a site that is using an invalid certificate or a certificate that was generated by an untrusted authority. Certificates may be invalid because they have expired or the domain name of the site does not match the subject name on the certificate. You may also see such messages when using self-signed certificates, which we create for ourselves, for example, in a development environment.

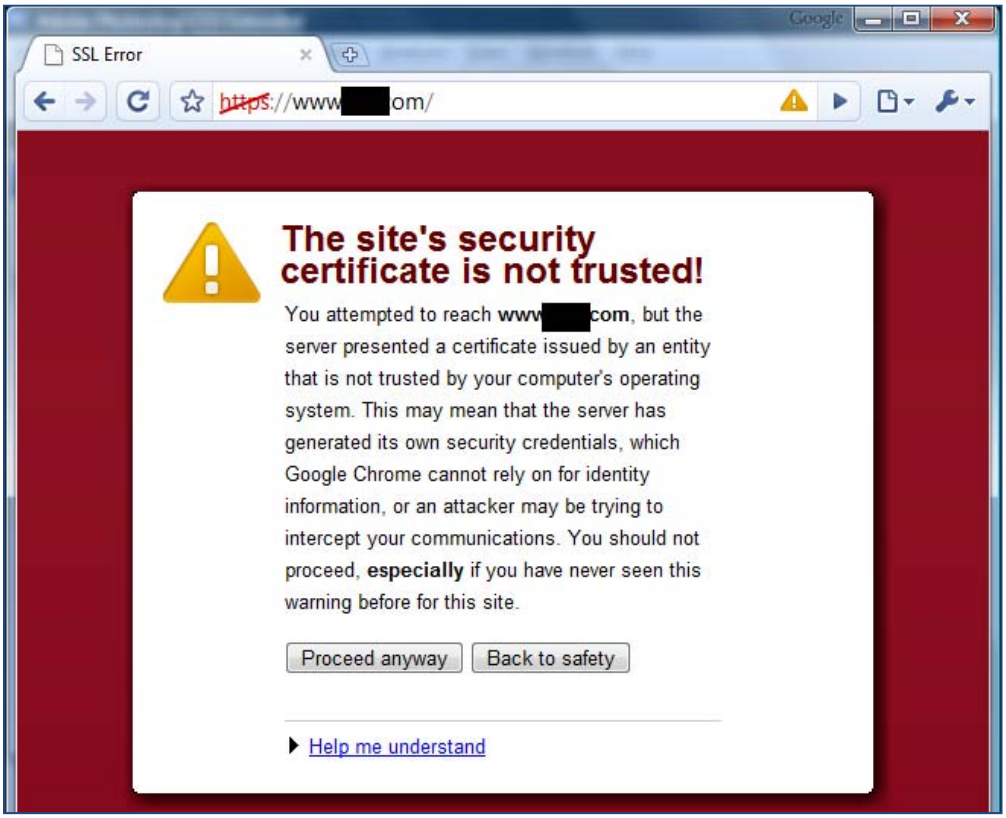

Figure 2.5: An example warning message presented by a browser when an SSL certificate is used by a certifying authority that is not trusted by the browser.

Now that it has been established that SSL certificates provide the means to encrypt communications and authenticate servers, it is time to consider how these capabilities work with Web applications.

Web Applications Without and With SSL Certificate Protection

Let's consider two scenarios: Web applications without SSL certificate protection and Web applications with their security benefits. We'll start with the unsecured examples.

Scenario 1: Web Applications Without SSL Certificate Protection

Consider an executive working with a Web collaboration application. The application supports common functions needed for group work including the ability to upload files, search collections of documents, and add notes and other metadata about the documents. The collaboration application does not use SSL certificates and instead relies on other security measures, such as access controls and network security, to protect its users.

The executive in our scenario is working on a proposal for a new client. The value of the potential contract is substantial, and there are multiple competitors vying for the work. Today, the client decides to get away from the office to work on the proposal. She heads to the coffee shop down the street and sets to work. After a couple of hours, the executive is ready to upload the proposal to the collaboration server. She connects to the coffee shop's WiFi, starts the collaboration application, and uploads the proposal. Unknown to her, someone else in the coffee shop was monitoring network traffic in search of some useful competitive intelligence. Figure 2.6 illustrates this scenario.

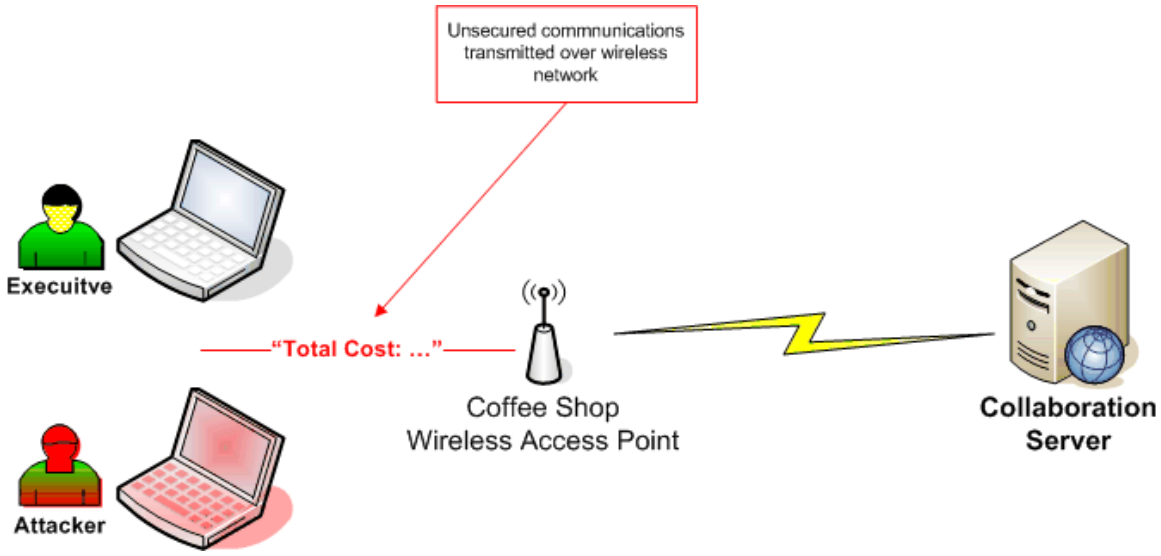

Figure 2.6: Unsecured communications can be detected and captured by others.

The communication was not encrypted by the application server or on the WiFi network, so the document was sent as clear text. This allowed a third party to pick up the network traffic and discover the contents of the document. Whatever competitive advantage the executive's firm had could have been undermined by this data leak.

> **Note**
>
> Although this example is fictitious, this kind of attack is not. See, for example, cyberattacks on energy companies for proposal data.

Unauthorized monitoring of communication is only one problem with not using SSL certificates. Another problem is the potential for someone creating a server that appears to be legitimate but is actually only *masquerading* as a legitimate server. This is known as spoofing.

Consider another scenario. One of your regular customers decides to come to your company site to place an order. She has done this dozens of times and doesn't think much about it. She types in your site's domain name and sees the usual order page. She tries to start a new order but receives an error message. It seems, according to the Web page displayed, that your company has lost some customer data including hers. She is prompted to enter her name and bank account information. The problem is, this is not your business' site and your customer has no way to tell.

Unknown to the customer, the service that translates domain names into Internet addresses (domain name system—DNS) for her has been compromised. It seems her company has been the victim of a DNS cache poisoning attack. DNS servers translate domain names, such as www.example.com, into a numeric address, such as 192.169.0.1. When a DNS cache is poisoned, someone changes the legitimate numeric address to one assigned to an attacker-controlled server. Your customer's traffic is routed to the attacker's server with no obvious indication something is wrong as Figure 2.7 shows.

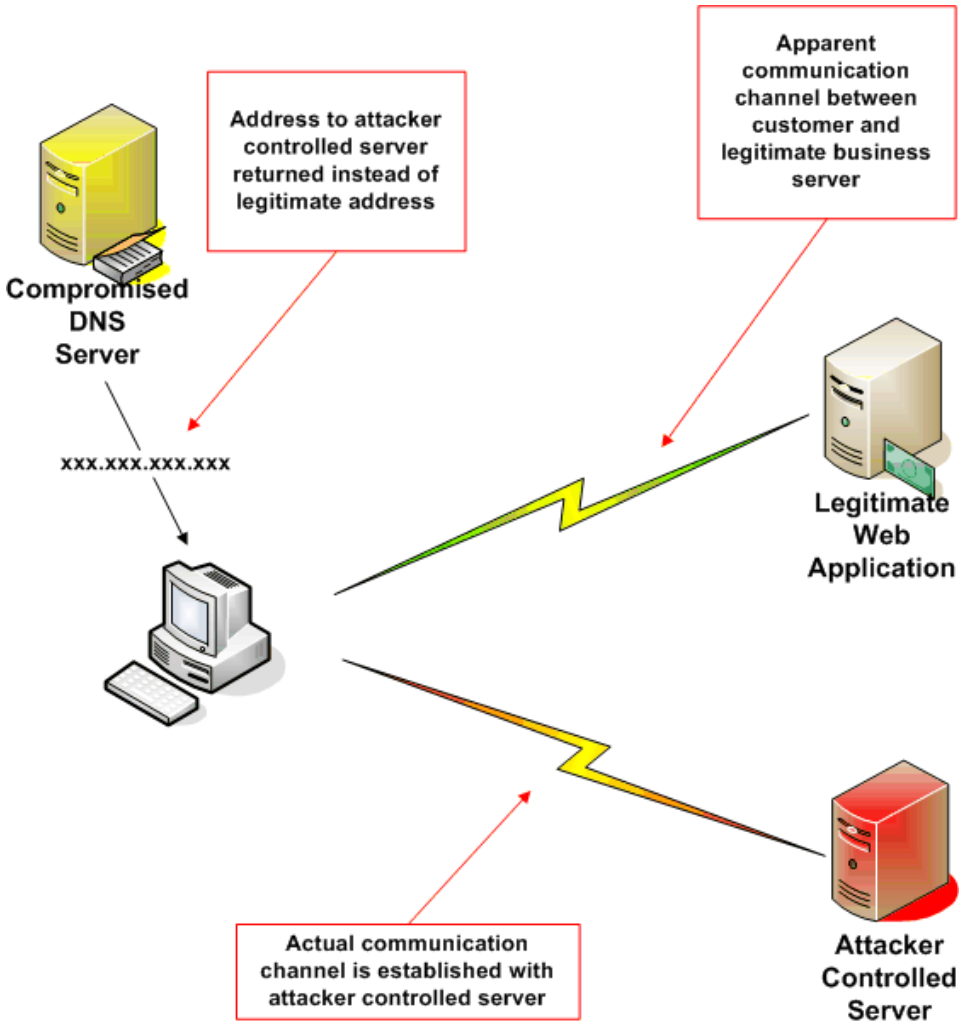

Figure 2.7: Without authentication provided by SSL certificates, users can be lured to use spoofed servers and applications that appear to be legitimate servers and applications.

In case you might be tempted to think that eavesdropping on your communications or server spoofing is only a theoretical problem that is not likely to affect you, consider these additional points:

- Sidejacking attacks involve using unencrypted data to allow an attacker to steal your session information and interact with a Web site as if the attacker were you. See the Firesheep tool for a demonstration of how this can be done.
- Attackers can find wireless networks with tools like NetStumbler, and even if the networks are not broadcasting identification data, tools like Kismet can be used to get that data.
- Auditing and testing tools, such as DSNiff can be used to scan network traffic—great for testing weakness in your network but these tools are just as useful to attackers with malicious intent.

Without the encryption and authentication protections enabled by SSL certificates, we and our customers and collaborators are vulnerable to a variety of attacks. Let's consider the earlier scenarios but with SSL certificates in place.

Scenario 2: With SSL Certificate Protection

In the case of the executive working in the coffee shop, had the collaboration server used SSL certificates, the executive could send secure communications to the server. In the event that an attacker intercepted the traffic, it would appear to be a random stream of data, not a valuable and confidential business proposal (see Figure 2.8).

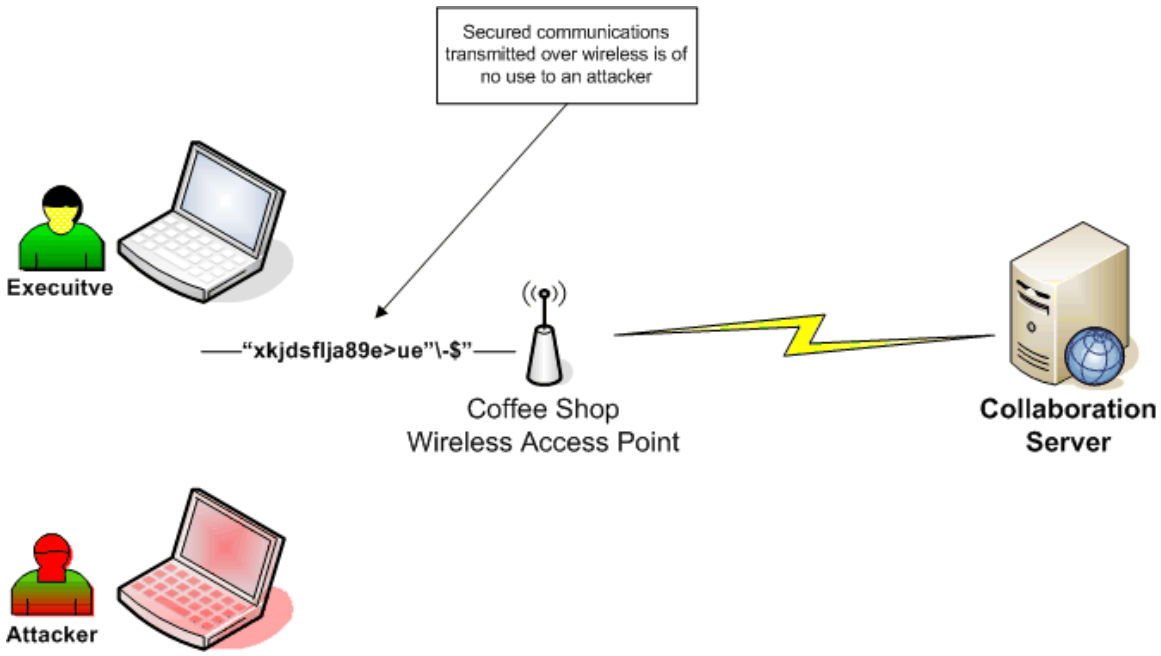

Figure 2.8: With SSL certificate-based encryption, data transmitted over wireless networks will appear to be more like random data than what it actually represents.

The case of the customer who maliciously redirected from her intended target to an attacker-controlled Web site would turn out differently as well if SSL certificates were used. One of the problems for the customer was that there was no indication that she was at a malicious site. With SSL certificate authentication, she would have received a warning from her browser that something was not consistent with the malicious site.

If the malicious site was using an SSL certificate, it would have inconsistent information because either the certificate subject entity would be something the attacker could get a certificate for, which would not match the spoofed domain name, or the attacker acquired an SSL certificate from an untrusted provider. In either case, the user would be alerted to the fact that something was not as it usually is.

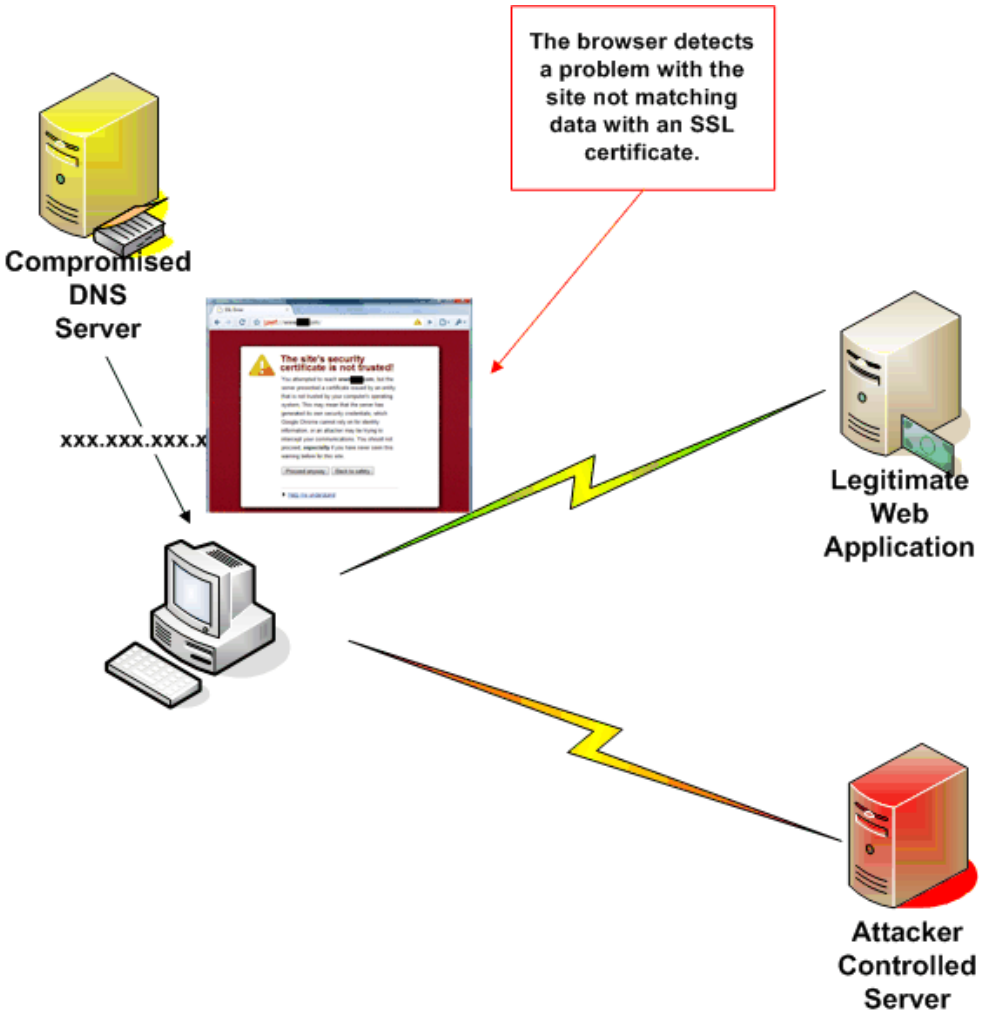

Figure 2.9: A spoofing attack would trigger an error on the client browser and alert the customer to the fact that there is some kind of problem with the site.

SSL certificates enable encryption and authentication, but businesses need more than that. Businesses need to know they can trust who they are dealing with. That is the ultimate reason we deploy SSL certificates.

Authentication and Trust

Trust cannot be reduced to digital certificates or encrypted messages. Trust is established over time and requires one party to be confident that another party will function as expected. We can't have trust with businesses or individuals we never met or have not heard of. We can, however, establish a trust relationship with an unknown party when we trust a third party and that third party assures us that the unknown party is trustworthy. This role of trusted third party is played by certifying authorities. These are companies that have built a business and a reputation around the business of verifying identities.

How Certifying Authorities Authenticate

The Internet community has different levels of need when it comes to verifying identities. For example, we might be ready to put information about our calendar into a site established to schedule company softball games with minimal verification but we are much more careful about our online banking practices. Certifying authorizes have created different procedures for verification, depending on the level of trust that is needed:

- Domain-level verifications are used when the certifying authority needs to establish that the requestor of a certificate is the owner of a domain name. Checking the domain registry may be sufficient for this. (See whois.net or any one of many other services that provide details about domain owners.)
- Business verification is used when a certificate is to be provided to a business and more evidence than domain ownership is required to establish identity.
- Extended validation (EV) certificates require the most comprehensive verification, including legal documentation and checks on the physical location of the business.

Certifying authorities go through varying levels of due diligence to verify the identity of domains or businesses that receive their certificates. That is only one part of the process for establishing trust. Another part is educating users about these practices and providing information on how to ensure that legitimate certificates are in place.

Developing Trust

Businesses have long used marks to indicate a product or service is trustworthy. Marks ranging from the Underwriter's Laboratories "UL" symbol to the Better Business Bureau logo have been used to indicate the safety of products and the trustworthiness of businesses. With the emergence of online business activity, it would help to have trust marks suitable for the Internet. We have trust indicators with SSL certificates, which use a lock in the browser address bar to indicate a secure communications channel. Green bar indicators are used with EV SSL certificates. Businesses can help promote knowledge about these trust marks by educating customers about their use and by using them on business sites as well as promoting other safe online practices. Trust can be further reinforced with trust marks such as a trusted seal from a certifying authority or an established organization such as the Better Business Bureau.

Businesses should also use the appropriate type of SSL certificate for their needs. When low trust is required by users, a simple domain certificate can be used. Sites that do not collect confidential or private information, do not require financial information or credit card data, and do not deal with other highly-valued data may be well served by conventional domain- or business-level certificates. When additional verification is required to help assure users that the site is legitimate, EV certificates should be considered because they provide highly-visible trust indicators such as the green bar and the display of the organization name.

Also, to develop trust, try to avoid situations in which your SSL certificates will generate error messages on customer browsers. These can occur for a number of reasons, so be sure to follow basic guidelines for good SSL certificate management:

- Do not use self-signed certificates for customer or other externally-accessed servers
- Use certificates from certifying authorities recognized by all major browsers
- Keep certificates up to date and renew them before they expire

A combination of factors goes into establishing trust: working with known and trusted certifying authorities, using the appropriate types of SSL certificates, and using trust marks and educating users about risks.

Summary

SSL certificates enable encryption and authentication. These are essential for securing Web applications and protecting customers from eavesdropping, data leaks, and spoofing attacks. SSL certificates enable key functionality required to build a trust relationship between business partners that might not have a pre-existing relationship. The best-designed application can have all the features and capabilities that users want, but if users do not trust the application, those features may not be used.

Chapter 3: Planning, Deploying, and Maintaining SSL Certificates to Protect Against Information Loss and Build Customer Trust

SSL certificates can play an important role in securing Web applications but as with any IT system, especially security mechanisms, it pays to plan how you will deploy and maintain that system. In the previous chapters, we have examined how data loss can undermine customer trust and how SSL certificates can be used to protect online business and maintain customer trust. Now that we have covered the conceptual elements of what SSL certificates do and how they work, it is time to discuss implementation details.

This chapter will assume you understand the basic components of an SSL certificate and how it works, and are interested in implementing SSL certificates to protect your Web applications. This chapter is divided into four main sections:

- Planning for the use of SSL certificates
- Deploying SSL certificates
- Maintaining SSL certificates
- Choosing the right type of SSL certificate for your needs

This chapter will provide guidance to help you deploy SSL certificates in a way that can be sustained for the long term without creating undo management burdens. There will even be tips and instruction on how to do basic SSL certificate management tasks in Windows and Linux operating systems (OSs); however, this chapter is no substitute for system documentation.

Planning for the Use of SSL Certificates

The planning stage of deploying SSL certificates consists of two main tasks: identifying applications and servers that will benefit from having an SSL certificate and determining which type of SSL certificate is appropriate for each use case.

Process and Asset Inventory

This may sound strange, but for the next several paragraphs forget about SSL certificates. SSL certificates are tools—they are a means to an end. For the rest of this section, we are not interested in how SSL certificates can protect our Web applications. Instead, our sole focus is on what needs to be protected and why it needs to be protected.

To understand our needs, we will start with a few basic questions. First, what applications and servers are accessed by customers? These might include:

- Company Web site
- Online catalog
- Customer support services portal
- Customer feedback application
- A shipment tracking application
- Product documentation

This is a wide variety of application types and each has a different pattern of customer interaction. Consider how you would work with each of these if you were a customer.

The object of this exercise is to understand your risk tolerance with regards to using SSL certificates. In some cases, an organization may want to use SSL certificates on every server and workstation. This would be reasonable in cases where an unusually high level of security is required. A middle ground approach is to install SSL certificates on all Web accessible servers. An organization with a high tolerance for risk may pick and choose which of their Web facing servers warrant an SSL certificate. In the following sections, we will consider factors that may influence such a decision.

Company Web Site

The company Web site is the online public face of the company. It probably contains the usual information like a description of the company, news and events, product descriptions, and if you have physical locations, services such as store finders. It will likely include links to online catalogs, customer support, and other applications, but those are not considered part of the company Web site for our purposes. Those are substantial applications that have their own design, deployment, and maintenance life cycles independent of the company Web site. For this exercise, the company Web site provides the relatively static information about a company as well as links to other Web applications, such as an online catalog.

When customers or other users come to the company Web site, they are probably looking for basic information, such as contact names and email addresses, product information, locations, times of operations, etc. Businesses often take advantage of this customer interaction to collect information for mailing lists, surveys, and so on. If the site is not protected with SSL certificates, customers may be hesitant to provide personal information, leaving the business to pursue more costly means to collect that information. A company with conventional risk tolerance would want customers to be able to authenticate the company's Web site (see Figure 3.1).

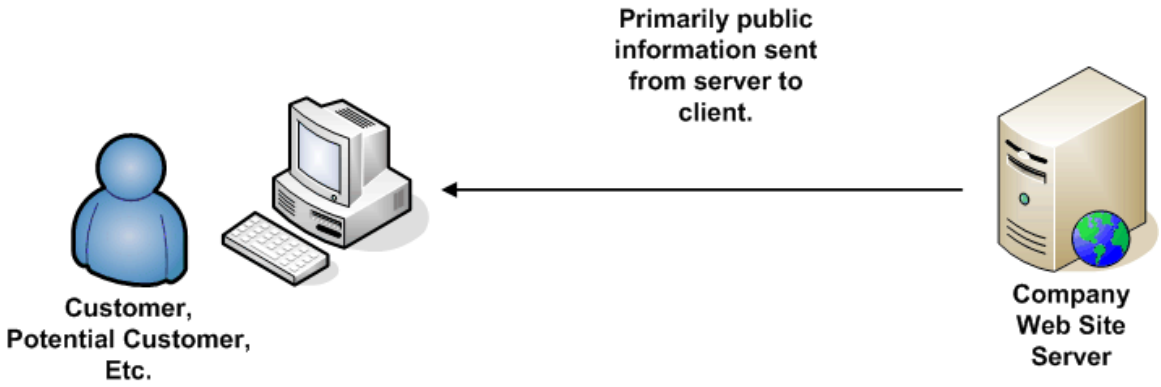

Figure 3.1: SSL certificate protection is not required when primarily public information is exchanged but there is a need to authenticate the server when collecting customer data, such as names and addresses.

Online Catalog

The online catalog allows customers to browse and search for products, collect sets of items to buy, pay for them, and then have them shipped. There is probably some type of database application behind this Web site as well as links to supporting services such as credit card processing services. The user's interactions with an online catalog are substantially different from those with a company Web site. For example, a customer is likely to:

- Browse a particular type of product or search for a specific product
- Review multiple products
- Read descriptions, reviews, and other material about products
- Select items for purchase
- Provide personal information including names, addresses, and credit card numbers

The interactions in this case includes both getting information from the application, similar to what we saw with the company Web site, and providing information to the application.

The fact that the customer is providing information to the business is a fundamental difference among applications. When it comes to personal information, such as names, addresses, and payment account information, it is probably a good bet to assume that the customer wants to keep that private. As your customer, I may have no problem sharing my credit card number with you, but I don't want anyone else to have access to it.

Depending on the size of the transaction (and the credit limit on the payment card), customers may be particularly cautious about providing payment card information to an unfamiliar company. If the customer is shopping at the online store for a national retail chain, she may feel confident that the site and the business behind it are legitimate. If this is the first time the customer has visited this site or it is not well known, major brand there may be some hesitation about trusting this site.

This application collects confidential information, so the Web and application servers supporting it should be authenticated with SSL certificates (see Figure 3.2). They would also be used to enable encrypted communication between the application and the customer. The business should consider and Extended Validation (EV) SSL certificate to demonstrate compliance with stricter identity verification standards.

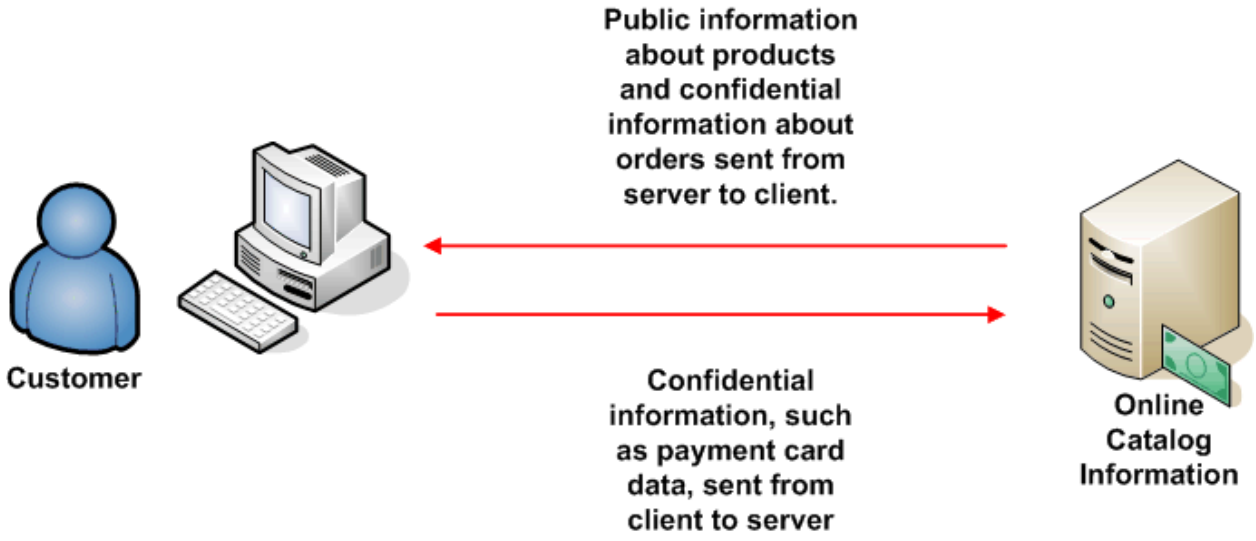

Figure 3.2: Confidential information is exchanged, so there is a need to authenticate the server and provided encrypted communications. An SSL certificate is required in this scenario even for highly risk tolerant organizations.

Customer Service Support Portal

The customer service support portal is a Web application designed to allow customers to manage their accounts, review past purchases and invoices, and set preferences, such as shipping and billing methods. Customers will want to keep their information private, so access controls are in place and customers will have access only to their account information. These access controls will keep customer data private when it is stored in the application database but does not help when data is transmitted from the application to the customer, so encryption is required for all transmitted data.

This application collects confidential information, so the Web and application servers supporting it should be authenticated with SSL certificates. They would also be used to enable encrypted communication between the application and the customer.

Customer Feedback Application

The customer feedback application collects comments and emails them to a special email account created to track such messages. These comments should be considered private and confidential because the business would want to collect frank and clear comments, which a customer might not want to disclose to others. This application should be protected with SSL certificates to ensure data is encrypted during transmission. The authentication service enabled by the SSL certificate will help assure the customer that she is working with a legitimate application. Here again, risk-adverse organizations will use SSL certificates to authenticate their company's applications.

Track Shipment Application

In some cases, a track shipment application is a relatively simple application that acts as a front-end to services provided by the major shippers used by the company. Customers enter an order number and the application looks up the shipping company for that order, contacts that company's tracking Web service, and displays the results. In more complex tracking systems, customers may provide feedback, which should be considered confidential, so SSL-based encryption should be used.

SSL certificates are not required for simple track shipment applications in highly risk-tolerant organizations, but for moderate-risk tolerance profiles or in cases where confidential information is exchanged, SSL certificates should be used. In addition, the shipping companies should use SSL certificates for their servers so that companies such as the one described here can authenticate the server they are communicating with.

Product Documentation

A product documentation application allows customers and employees to search a database of content of user manuals, technical documents, and other material to help customers and employees use products sold by the company. Product documentation is often considered proprietary information and should be protected as such.

In this scenario, the company is concerned about maintaining the confidentiality and integrity of the documentation. They have established strict access controls to mitigate the risk of incorrect documentation being placed in the database. There is some concern that if a malicious prankster spoofed the site and lured customers to a fake version of the site, the company's reputation could be damaged.

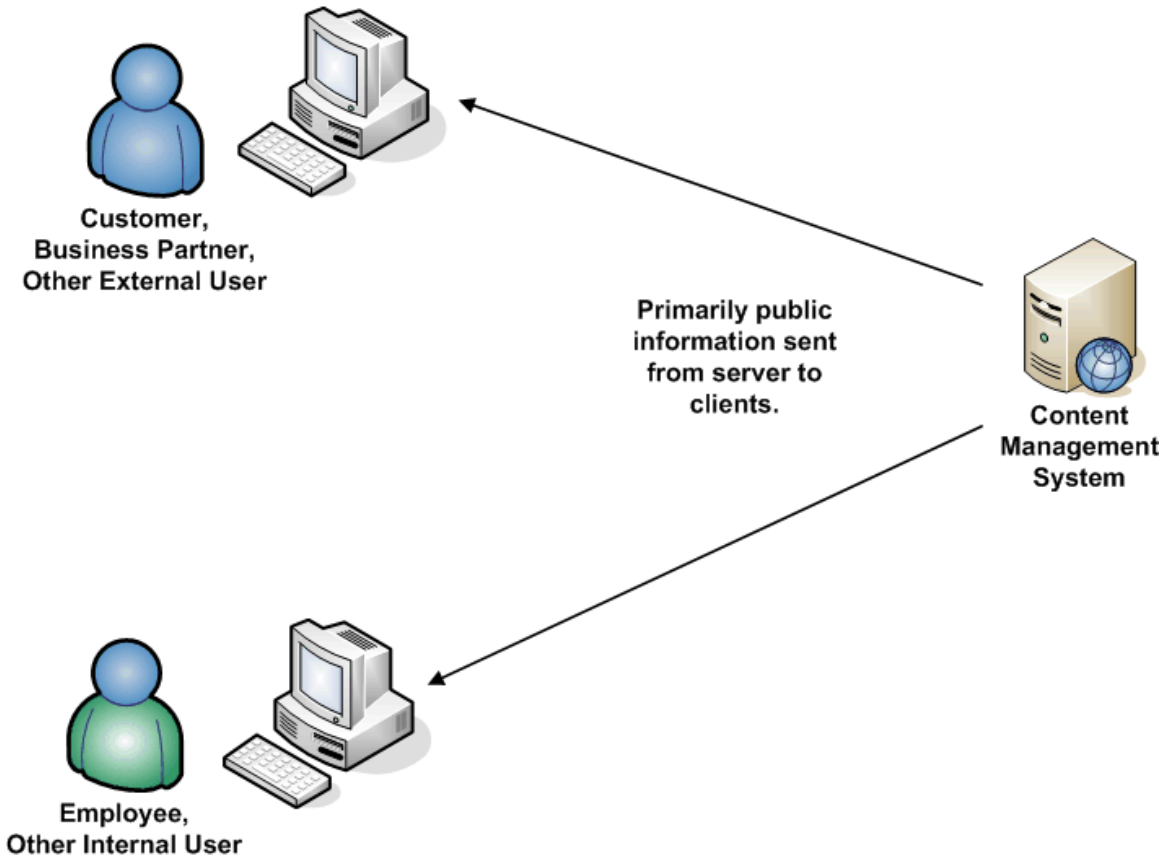

Figure 3.3: Public information distributed to both internal and external users does not require SSL certificate protection.

SSL certificate protection is required for encryption and authentication. If the perceived risk is high and the expected impact of a possible spoofing attack is great enough, an SSL certificate should be used for authentication.

Multi-Tier Applications

Having completed the application-based assessment of our SSL certificate requirements, we next have to delve into server-level requirements. In cases of simple applications that run on a single server, one would only need a certificate for that server. Many business applications, however, require multiple servers such as Web servers, application servers, and database servers.

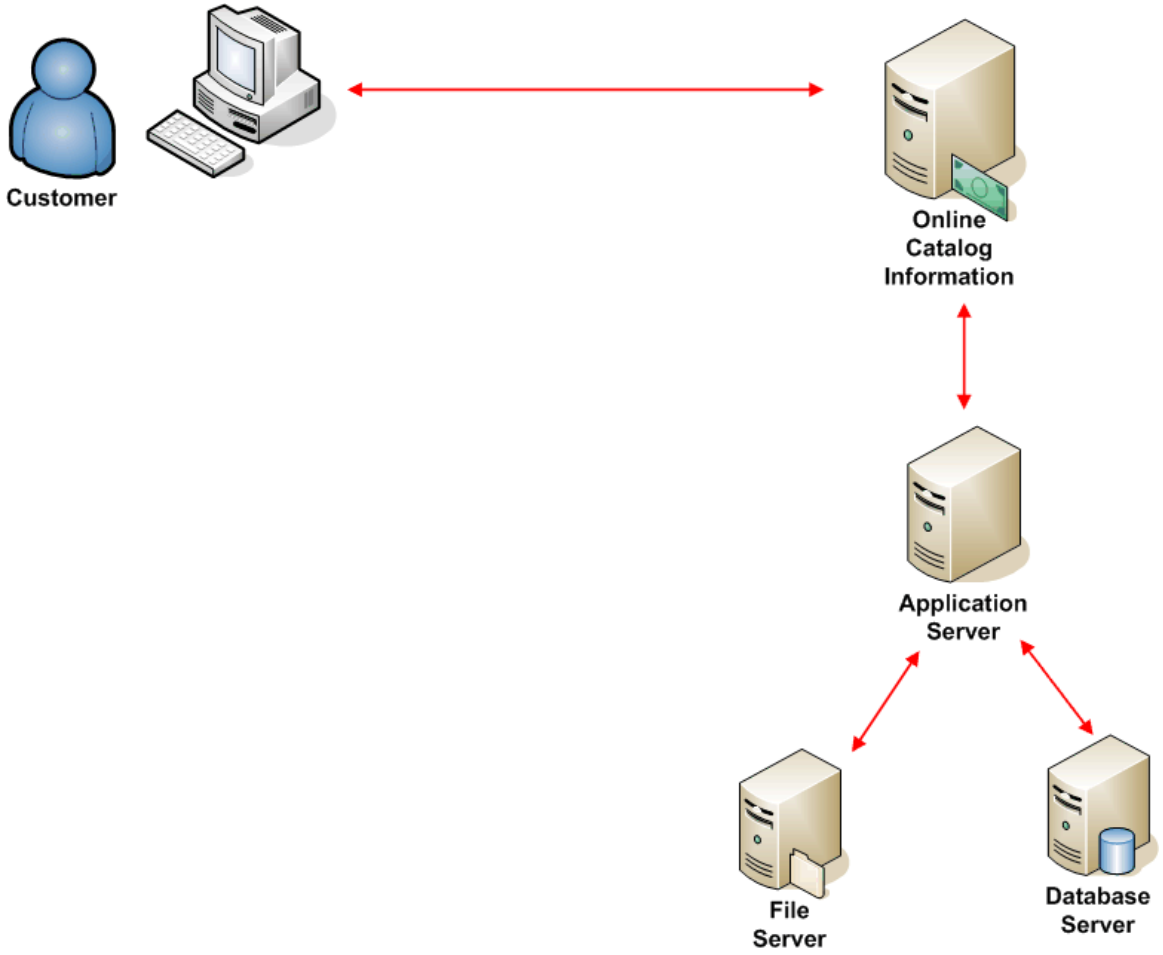

Figure 3.4: Multi-tier applications depend on multiple servers. If the application requires SSL certificates, then usually all servers will require SSL certificates.

Figure 3.4 shows a multi-tiered application. In this scenario, confidential data, such as payment data or customer account data, moves through several servers. The trust that a customer has in the application has to build on trust in the servers that implement the application. In such cases, the most secure option is to use SSL certificates on all servers in the multi-tier architecture. It is conceivable that there may be a server providing some basic function that never receives or processes confidential information. In such a case, one could argue against authenticating that server via an SSL certificate; however, given that requirements might change and that consistency often eases management burdens, it might be worthwhile using SSL certificates on all servers in the architecture.

In general, the planning process consists of a similar exercise to the one described earlier. Assess the way private and confidential information flows from the business to customers and from servers and devices implementing the application. Specifically, be sure to ask the following questions:

- What applications and servers are accessed by customers?
- What applications and servers are accessed by other trusted applications?
- What applications access confidential, private, or sensitive data?

With answers to these questions, we can determine which applications and servers need SSL certificate protection. The next question to address is what type of SSL certificate should be used.

Determining the Type of SSL Certificate Required

Although all SSL certificates are fundamentally the same in terms of form and function, there are differences. There are certificates for single servers, for multiple servers within a domain, and there are even some that work especially well with email servers. Let's look at criteria for choosing between these.

A single server certificate is appropriate for a server that is managed and deployed relatively independently of other servers. A domain wildcard certificate allows multiple servers to use the same certificate. These servers use a subjects such as "*.example.com" which matches any server in the example domain. This is useful when a number of servers in a domain require certificates. Use these carefully, though. This certificate can be copied and used on any server in the domain, which could result in either unauthorized use and/or difficult-to-manage certificates if they are not properly tracked.

EV SSL certificates are appropriate for customer-facing Web sites and applications that will process high-value private and confidential information, such as bank account information or personal health care information. Businesses and organizations that may be targets for cybercriminals should consider the value of having an EV SSL certificate and the corresponding visual cues presented to customers. This is one way to help customers distinguish between a legitimate site and a fraudulent one.

At the other end of the trust spectrum from EV SSL certificates are self-signed certificates. These certificates do not involve a trusted third party as a certifying authority—instead someone within a company creates an SSL certificate himself. There is not much point in having an SSL certificate that asserts "Trust me because I say so" on a public-facing Web site. External-facing applications need an SSL certificate that asserts "Trust me because a trusted third party has vouched for my identity." Self-signed certificates are used for internal purposes such as development and testing.

Self-signed certificates have a number of advantages for development and testing:

- They can be created quickly
- They incur minimal, if any, cost
- They can be customized to meet specific needs; for example, validation periods, wild card subjects, etc.
- They are managed completely internally and do not depend on interactions with a third party

Planning SSL certificate deployments is a critical step that allows you to identify which applications and servers need SSL certificates. This step in turn allows you then to select the best type of SSL certificates for your requirements. The next step to follow after this process is to actually deploy the SSL certificates to your servers.

Key Points About Choosing and Deploying SSL Certificates

As you are planning, deploying, and managing SSL certificates, keep in mind several key points about choosing and deploying them. SSL certificates are used for two security operations: securing communications and authenticating systems.

Secure communications are required for when confidential or private information is exchanged. This is certainly the case when data such as credit card numbers are exchanged, but this is not the only scenario. Sometimes attackers can piece together information incrementally over time. There may be no case where a single transaction had all the details the attacker needed to steal information or compromise a system, but if the attacker has access to multiple transactions or data exchanges, it is possible to cull useful information to further the attacker's objectives.

Authentication with SSL certificates allows client devices to verify that the server they are working with possesses a certificate from a trusted third party created for use on only that server (or set of servers in the case of wildcard or SAN certificates).Confidence you are working with a legitimate server is a building block to something more important: building the trust between a customer and a business.

We use SSL certificates to mitigate the risk that users will be lured into using illegitimate or otherwise malicious devices. Customers have visual cues, such as locks and green bar indicators that reinforce the idea that particular security measures are in place to protect this customer. Ideally, customers will understand that lack of such cues on sites that usually have them is an indicator of a potential problem.

SSL certificates are like any IT asset, they require maintenance. Fortunately, this is minimal. The key things we need to keep in mind once we have selected the appropriate type of certificate is to monitor the valid dates of use and to track the use of wildcard certificates so that they are not used on servers for which they are not intended. Also consider whether you have special requirements that might necessitate a SAN SSL certificate.

Summary

Web applications often require the use of SSL certificates in order to enable basic authentication and encryption services. Planning how to best deploy SSL certificates begins with assessing the kinds of operations performed by applications. Do they exchange private or confidential data, such as credit card information? If so, then SSL certificates should be used to enable encryption and preserve confidentiality. Is there a risk of customers being lured to malicious sites that appear to be one of your business' sites? If so, then SSL certificates are needed for authentication.

Deploying SSL certificates is not difficult, but the process is often specific to your OS or application. Some applications, such as Microsoft IIS, have specialized tools for managing SSL certificates. Fortunately, once SSL certificates are deployed, they have relatively low-maintenance requirements.