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).

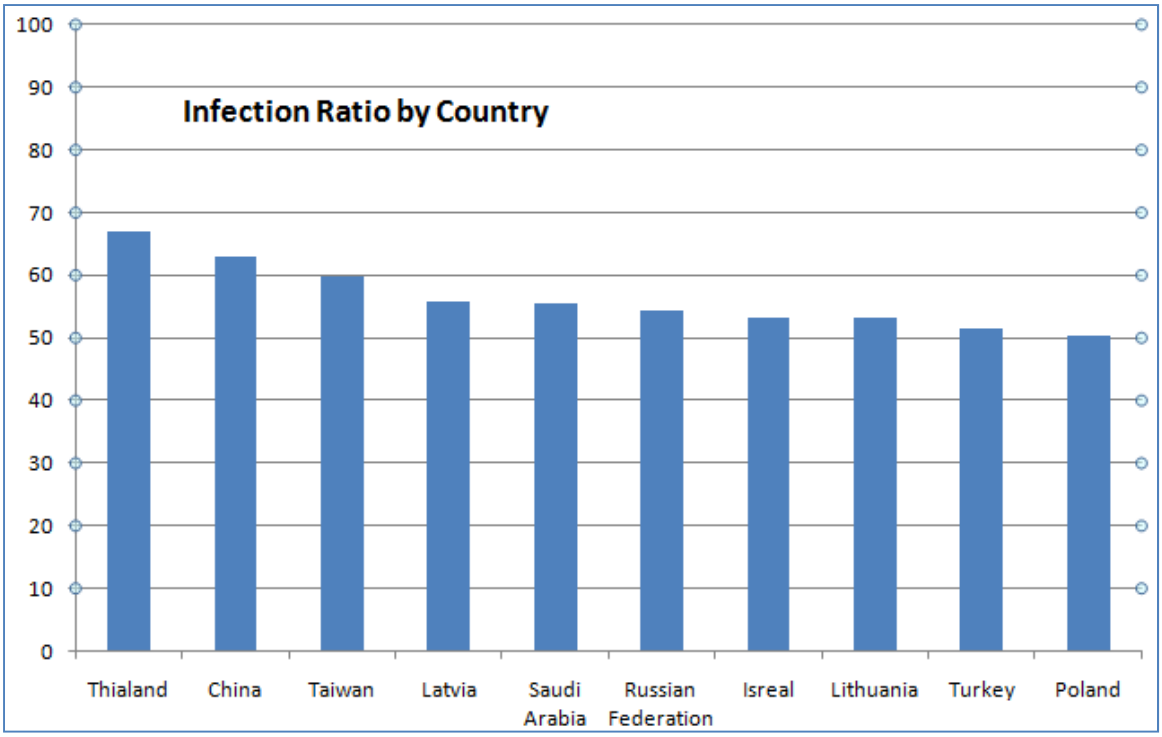

Figure 2.1: High malware infection rates (above 50%) are seen across the globe. The United States ranked 22nd in the list with a 45.32% infection rate.

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).

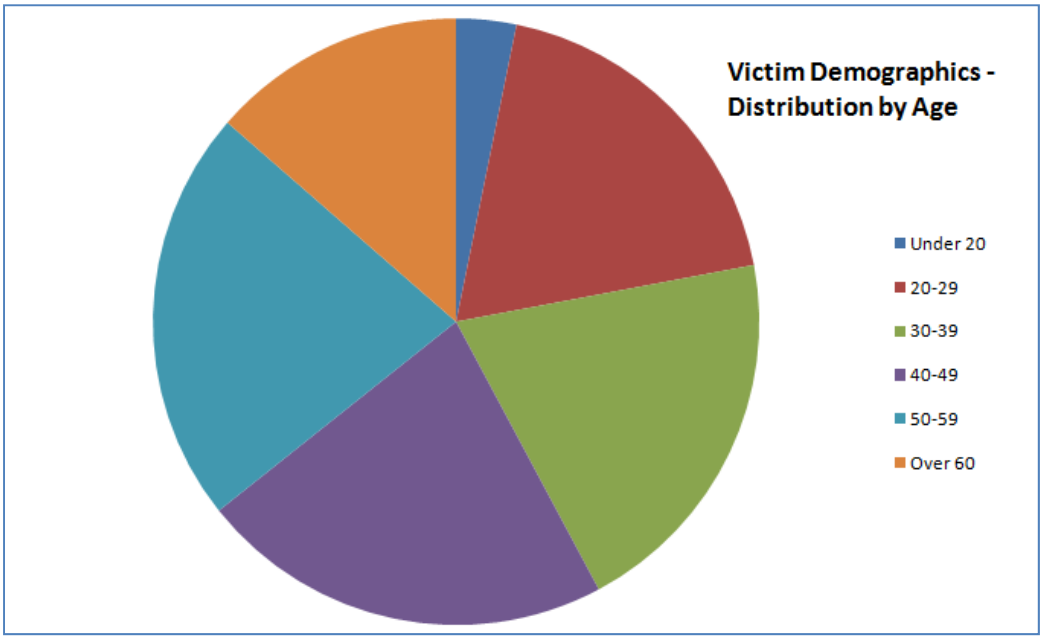

Figure 2.2: Reports of Internet crime to the FBI are fairly well evenly distributed across age groups with under 20 year olds fairing the best.

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.

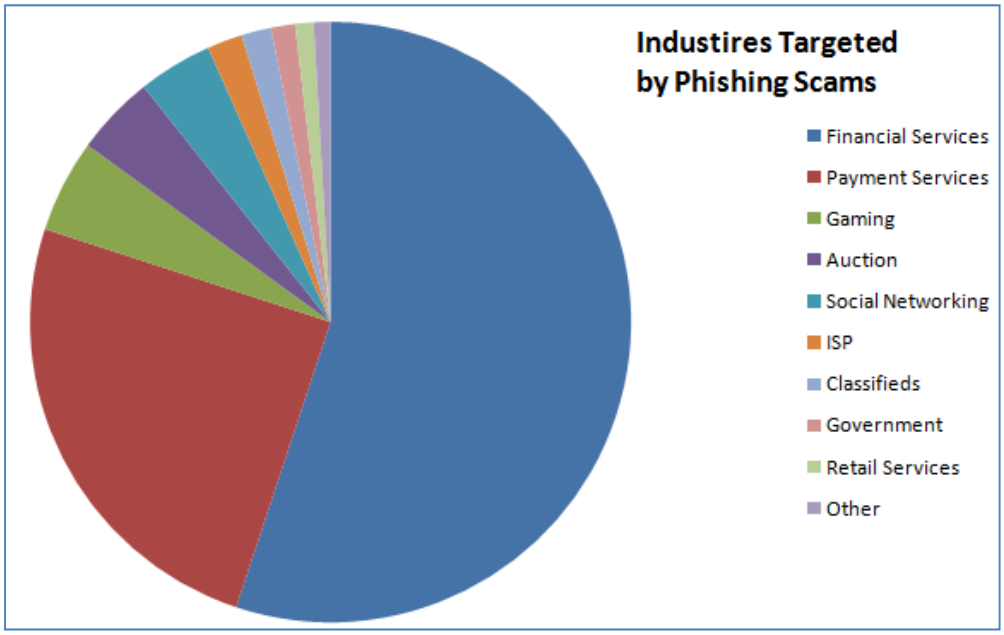

Figure 2.3. Diversity does not extend as much to the industries targeted. Financial services and payment services account for more than three-quarters of phishing scams (Source: Anti-Phishing Working Group, Phishing Activity Trends, 2nd Half 2010).

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.

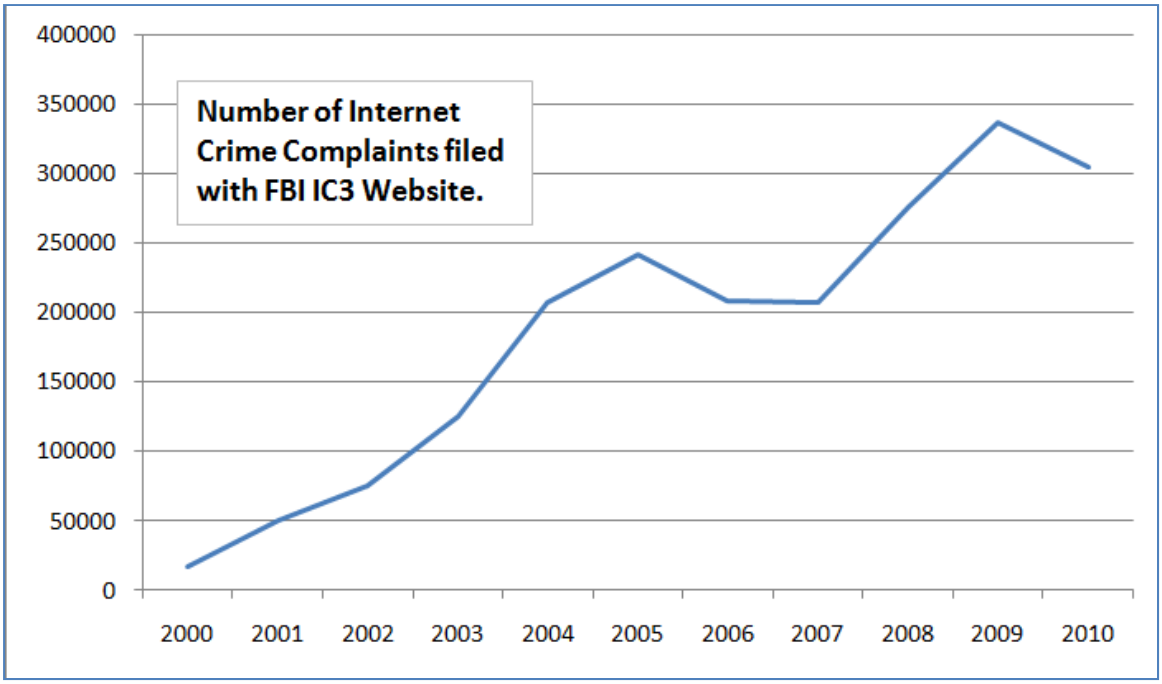

Figure 2.4: The number of Internet crime complaints filed with the US Federal Bureau of Investigation (FBI) is another indicator that cybercrime is an established, on-going, and growing problem (Source: FBI, 2010 Internet Crime Report).

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).

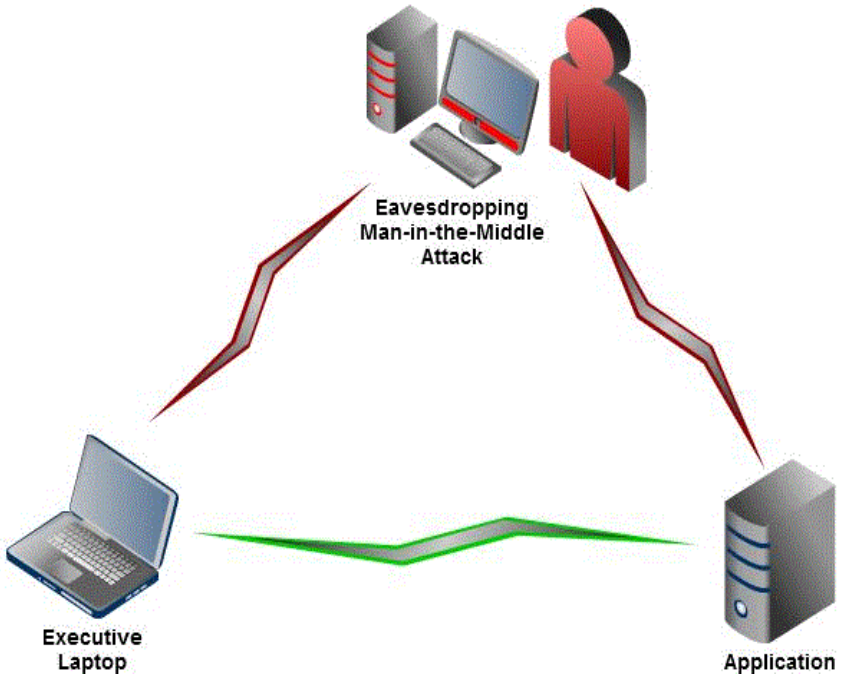

Figure 2.5: Unencrypted communications can be intercepted using a man-in-the-middle attack. A user believes there is a direct and secure line of communications (green) when in fact the line of communication is being intercepted (red).

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.