

Realtime
publishers

"Leading the Conversation"

The Shortcut Guide™ To



Extended Validation SSL Certificates

sponsored by



Dan Sullivan

Introduction to Realtimepublishers

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

Introduction to Realtimepublishers.....	i
Chapter 1: Security Challenges and the Business Case for EV SSL Certificates.....	1
Web Security Challenges.....	2
Evolution of Attacks.....	3
Phishing Attacks.....	4
Establishing Trust.....	5
Convincing Users to Take Action.....	7
Collecting Confidential Information.....	7
Man-in-the-Middle Attacks.....	7
Double Vulnerability: Lack of Encryption and Poor Password Practices.....	8
Phishing by Proxy.....	9
Replay Attacks.....	10
Loss of Privacy and Confidentiality.....	11
Implications of Security Threats for Business.....	12
Reduced Potential for Online Business Due to Lack of Trust.....	12
Fraud and Identity Theft.....	12
Damage to Brand and Reputation.....	13
Requirements for a Business-Grade Web.....	13
Authenticated Identities.....	15
Confidential Transmission.....	15
Integrity of Transactions.....	16
The Role of EV SSL Certificates.....	16
Summary.....	17

Copyright Statement

© 2007 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

Chapter 1: Security Challenges and the Business Case for EV SSL Certificates

The Internet has rapidly become an integral part of day-to-day business and is now, along with shipping, manufacturing, and financial accounting, a critical component to business operations. The Internet, however, poses unique security challenges that threaten to undermine its ability to support business-grade services. The risks of unchecked security weaknesses can range from fraud and identity theft which may ultimately damage a company's brand and reputation. Mitigating these risks requires a wide array of measures.

Broadly speaking, security measures are designed to protect three fundamental aspects of information:

- Confidentiality of information
- Integrity of information
- Availability of information resource

Confidentiality and integrity are especially important to establishing and maintaining trust among businesses and customers. Customers must be comfortable sharing information with businesses and be confident that it will not fall into the hands of hackers and thieves. When a customer makes a purchase in a store, the customer can see exactly what he is buying, he hands his credit card to a human who hands it right back, and the customer knows that if there is a problem a manager is probably nearby. Aspects of in-person commerce such as this help establish trust between customers and businesses.

Similar levels of trust can exist when online transactions are used as well, but the processes are different. You don't see employees who provide services; you've likely never met managers of an online service in person. Instead, you depend upon factors such as brand recognition and loss limits on credit cards to provide some level of confidence that your financial transactions are secure and your risks are limited.

Peter Steiner's 1993 *New Yorker* cartoon depicting two dogs in front of a computer with the caption "On the Internet, nobody knows you're a dog" captured the double-edged sword of online business. On the one hand, the Internet enabled small businesses to offer similar services and products as large corporations. However, this same development made it more difficult for customers to know which sites are actually created by reputable firms. You need online-specific methods for creating and establishing trust between customers and businesses.

This guide addresses one method for establishing trust: the use of Extended Validation Secure Sockets Layer SSL (EV SSL) certificates. The guide consists of five chapters:

- Chapter 1 examines the security challenges to business on the Internet and the role of EV SSL certificates in establishing a more trusted business environment on the Internet.
- Chapter 2 describes, in detail, how SSL certificates work and identifies weaknesses that still exist with the use of those certificates. The chapter concludes with a discussion of how EV SSL certificates correct for those weaknesses.
- Chapter 3 examines the authentication and verification process used when issuing an EV SSL certificate.
- Chapter 4 describes the user experience when conducting business with an EV SSL certified organization. It also examines differences in browser implementations of the EV SSL.
- Chapter 5 concludes the guide by looking into the future of EV SSL with particular attention to the development of the EV SSL standard and the potential for improved user experience.

This chapter examines four related topics:

- Web security challenges
- Implications of these security challenges to business
- Requirements for a business-grade Web
- Role of EV SSL certificates

Let's begin with security threats that are especially problematic for maintaining a trusted environment for conducting business on the Web.

Web Security Challenges

The Internet's utility stems in part from the wide variety of services available from Web browsing and email to custom catalog, order processing, and customer support systems. The applications underlying these services are sometimes vulnerable to attacks. Although the specific details of particular attacks are not important here. While each instance may be different, there are common patterns among attacks. These include:

- Phishing
- Eavesdropping and tampering, known as man-in-the-middle attacks
- Attacks resulting in loss of confidentiality and integrity

Technically, phishing is a type of man-in-the-middle attack. For the purposes of this guide, we use the term man-in-the-middle-attack to refer to eavesdropping and tampering attacks. Each of these will be described in detail, but first let's examine a recurring pattern in the history of information security.

Evolution of Attacks

Security practices and tools have evolved in large part as a response to attacks by hackers and cybercriminals. Attackers, in turn, respond by creating new techniques that circumvent emerging countermeasures. This is an important pattern in the history of information security for two reasons. First, it occurs repeatedly and across different areas of information security. Second, because of it, the tools and techniques that may have worked at one time may no longer be sufficient to protect us today.

Take, for example, the changes in computer viruses over time. The following list highlights major developments in the history of this kind of malicious software, known as malware:

- After computer viruses emerged, security researchers developed techniques for identifying viruses based on unique signatures or fingerprints of viruses.
- In the next stage, virus developers countered by encrypting their viruses so that the viruses were not so easily detected.
- Of course, antivirus researchers developed new detection techniques, actually targeting the part of the virus responsible for encrypting the viral code.
- In the next stage of development, virus writers created methods for changing the actual code of the virus without changing its function. These “mutating viruses,” as they are known, prompted the development of new detection techniques, called behavioral analysis.

Today, viruses and other forms of malware can still inflict damage; however, the focus of the most damaging attacks has shifted from vandalism to financial gain. Rather than just deleting files or spreading malicious code to other devices, malware is used to gain sufficient control of PCs to use them to distribute spam and for phishing attacks. Large networks of compromised computers, known as botnets, are responsible for much of the spam and phishing attacks spread on the Internet.

It is not just viruses that have changed to avoid detection or to become more virulent. Phishing, for example, is an all-too-common type of attack that takes advantage of people’s trust in businesses and other well-known organizations.

Phishing Attacks

Phishing is an attack that uses email or Web site content to trick victims into doing things that they would not normally do. Phishers succeed by establishing a sense of trust with the victim. The general class of such attacks is known as social engineering attacks. Examples of social engineering attacks include:

- Calling an employee posing as a service desk technician and asking for the employee's password to troubleshoot a problem with network logins.
- Sending a legitimate-looking email claiming your account with a well-known online retailer has been compromised and requesting you click an embedded link to go to a form that will allow you to update your password.
- Requesting that users take a brief survey about customer services in return for a cash payment. The link provided in the email links to a phishing site that downloads malicious software, such as a keylogger that captures usernames and passwords for banking and other financial services businesses.

As these examples demonstrate, the typical phishing attack includes a multi-step process:

1. Establish the victim's trust using a "lure," typically an email that appears legitimate.
2. Convince the user to take an action that will enable the capture of confidential information.
3. When the action in step 2 is taken, collect the confidential information and terminate the session.

Phishers have developed multiple techniques for each of these steps.

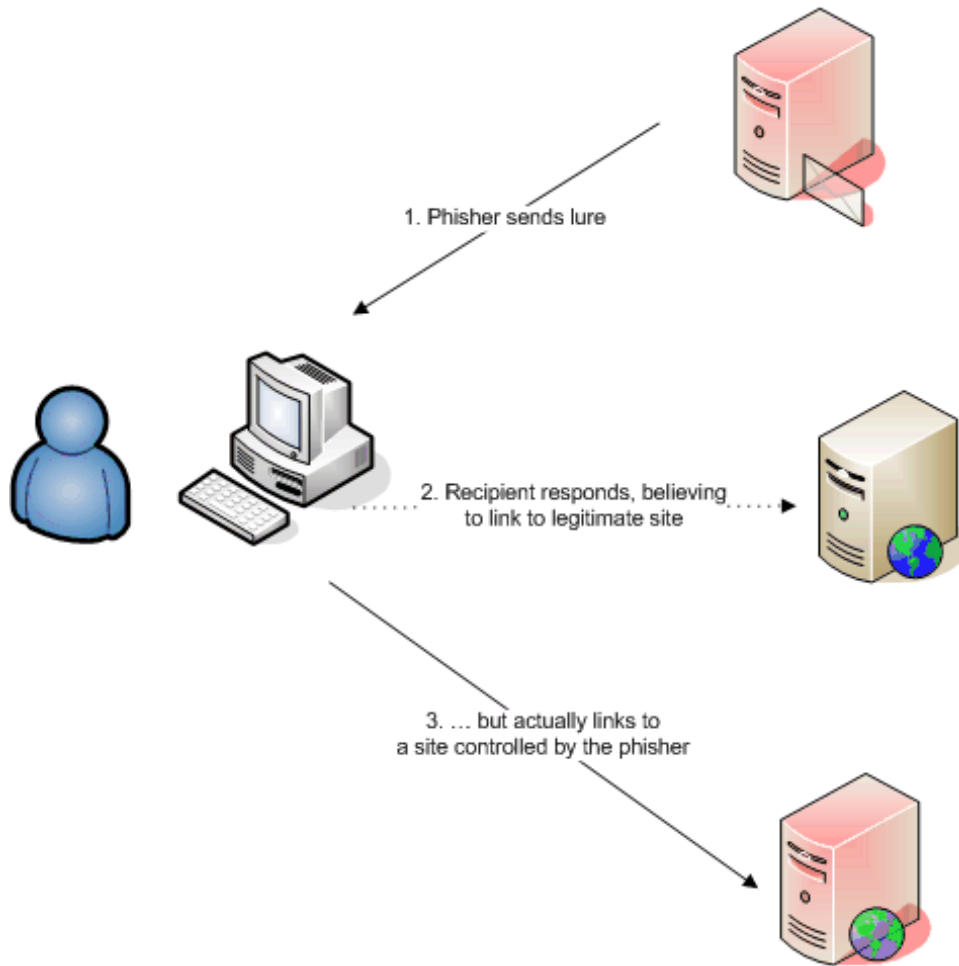


Figure 1.1: A typical phishing scam lures victims to a bogus Web site where confidential information is collected.

Establishing Trust

One of the quickest ways to establish trust is to use visual cues. Company logos, tag lines, and even entire Web pages are easily collected from legitimate sites. These can help to convince readers that the message is legitimate but it is rarely enough. The text within the message must be written in standard business English with no obvious grammatical errors. Links have to look like the domain of the target institution. In some cases, as Figure 1.2 shows, phishers even go so far as to advise users about anti-phishing practices.

Dear valued PayPal® Member

It has come to our attention that your

Congratulations! **Paypal®**

account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

You must **click the link below** and enter your password on the following page to Update your email address.

[Click here to Update your account](#)

However, failure to update your records will result in account suspension. Please update your records on or before:

- Buy from an online auction
- Pay on a merchant website
- Send money to anyone with an email address

Protect Your Account Info

Make sure you never provide your password to fraudulent websites.

To safely and securely access the PayPal website or your account, open a new web browser (e.g. Internet Explorer or Netscape) and type in the PayPal URL (<https://www.paypal.com/us/>) to be sure you are on the real PayPal site.

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at <https://www.paypal.com/us/securitytips>


Figure 1.2: A typical phishing lure can establish trust by including logos from legitimate businesses or, in this case, by recommending typing URLs instead of clicking on embedded links.

Some companies have responded to phishing attacks against their brands by implementing additional security measures, such as Bank of America's SiteKey. Customers choose an individual image that is displayed on a bank's site when a user logs in. Unless a phisher has access to information about customers' choice of images, the phisher cannot duplicate the functionality of the bank's site.

Convincing Users to Take Action

Like a good advertising campaign, a phishing attack includes a call to action. Getting a user to actually take the time to respond is a challenge even for legitimate advertisers, so phishers often use the well-known tactic: appealing to fear, uncertainty and doubt (FUD). Consider the subject line from some phishing lures archived at [MillersMiles.co.uk](http://www.millersmiles.co.uk), an anti-phishing service:

- Security Alert: Secure Your Online Banking Information.
- Wachovia Alerts: Unauthorized Access Into Your Wachovia Account
- eBay Bid Cancellation Notice - Item 300120654262
- Alert: A Thirdparty Access Into Your Online Banking Account.
- Your Account Is Blocked(Update Now)

 Details about these and other phishing lures are available at <http://www.millersmiles.co.uk/archives/>.

If a phisher can craft a well-written message with sufficient visual cues and no apparent tell-tale signs of a phishing scam, all that is left is to collect information once the reader has fallen for the lure.

Collecting Confidential Information

Once a phisher has drawn a victim to a website they control, it is a simple matter to display forms that look legitimate and collect basic information, such as usernames and passwords. Attacks may be more sophisticated and include the use of keyloggers, which are programs used to intercept and copy each keystroke as it is typed on a keyboard. The malicious program can then transfer the data in its entirety to the attacker or scan for patterns in the text that indicate the name of a bank or other financial service. When a target institution is found, the keystrokes near it are sent to the attacker with the assumption that users log in to their accounts shortly after accessing the institution's Web site. Phishing attacks typically require some action on the part of the victim but other attacks can occur without any participation of the victims.

Man-in-the-Middle Attacks

Man-in-the-middle attacks include a broad array of attacks that interfere with or observe the interactions between two parties. There are several forms of this attack:

- Simple eavesdropping
- Phishing by proxy
- Replay attacks

As with phishing attacks, there are a variety of practices that can reduce the risk of such attacks.


Double Vulnerability: Lack of Encryption and Poor Password Practices

Eavesdropping on wireless network communications is not difficult and in the right circumstances can easily yield confidential information. Let's consider a simple example. A person waiting for a plane has a few moments before boarding, so she decides to take care of a few online tasks. A coffee shop in the airport offers a free but unsecured wireless network, so she decides to use that. First, she checks her corporate email account, and then checks balances on her bank accounts, followed by browsing some online business journals.

A vulnerability of wireless communications is that anyone with reasonably inexpensive equipment can monitor network traffic. If someone were nearby with wireless equipment that allowed them to monitor all wireless traffic, they could pick communications of other users. Email and bank Web sites typically encrypt information but an eavesdropper could still pick up enough to know what email system or which banks are being used. Less security-conscious Web sites might pass usernames and passwords as plain text.

Unfortunately for this user, her business journal is one of those sites that do not bother to encrypt usernames and passwords. To make matters worse, this person has the habit of using the same password for multiple sites. In just a matter of minutes, an attacker could have collected enough information to begin to compromise the user's accounts, probably by exploiting other vulnerabilities as well.

The risk of this kind of attack can be mitigated by using only encrypted wireless networks. Furthermore, a well-known but too-often-overlooked best practice is to use different passwords for multiple sites.

 Until there is a secure, widely accepted standard for managing identities and credentials, we will be managing passwords for multiple sites and applications. Keeping track of all these usernames and passwords is so difficult that many users are prone to insecure practices, like writing down passwords or storing them in emails and other online repositories. A better option is to use tools such as Password Safe, available for free from <http://passwordsafe.sourceforge.net/>, that keep a secure database of all your account and password information.

As noted earlier, phishing is technically a man-in-the-middle attack, but I have distinguished most kinds of phishing from eavesdropping and tampering attacks. The next section will examine a technique known as phishing by proxy that combines elements both kinds of attacks.

Phishing by Proxy

In a phishing by proxy attack, a program intercepts communication between a user and a legitimate site. This kind of attack has the advantage (to the phisher) of displaying actual content from the real site while still collecting private information from a user. Here is how it works: A user responds to a phishing lure, for example, a purported email from the person's bank asking the user to verify information. When the user clicks the link, the browser loads content from a proxy server. The proxy server, in turn, gets legitimate content from the real business site and displays it for the user. There are no clues, such as poorly worded phrases or strange-looking URLs to visually indicate a phishing scam.

The user then continues to enter a username and password as well as respond to any security questions. All this information is passed to the phishing proxy, which stores the information and then passes it on to the legitimate site. The proxy has logged in on behalf of the user, so the proxy can return the same content the user would see from the legitimate site.

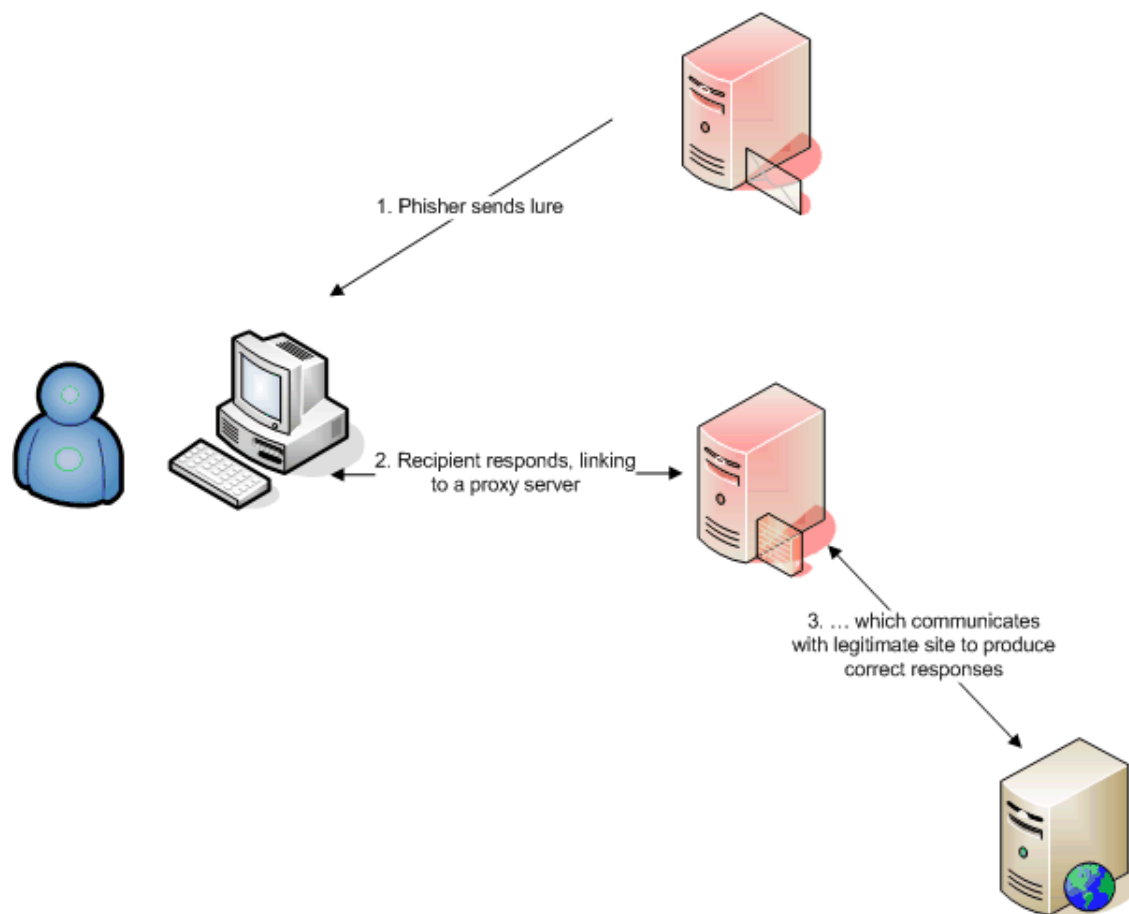


Figure 1.3: In a phishing by proxy attack, legitimate sites are used to generate responses on behalf of the phishing site.

This type of attack even works against newer two-factor authentication schemes. Even if a user has to enter an extra authentication code—for example, a number generated by a security token that changes every minute—the proxy server will have as long as 60 seconds to initiate another session with the legitimate site and execute a transaction. This reuse of a time-based code is also a type of replay attack.

Replay Attacks

In a replay attack, the attacker captures authentication information and uses it to establish another transaction. Replay attacks differ from man-in-the-middle attacks by collecting information and re-using it for a separate transaction rather than interfering with the original transaction. Several methods are available to prevent this type of attack, including the use of

- One-time passwords
- Session tokens
- Message authentication codes
- Time-stamping

Each of these techniques incorporates information that changes over time or with each session.

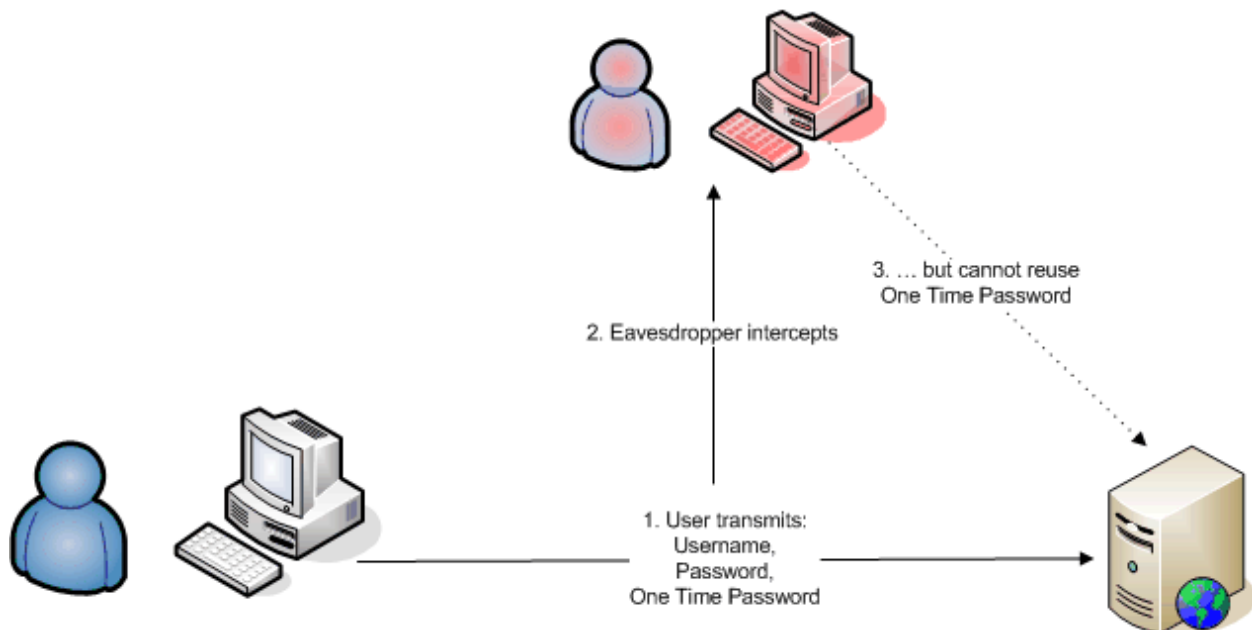


Figure 1.4: The use of varying information in transactions can thwart replay attacks.

The threat from man-in-the-middle attacks can be reduced in several ways, including the use of strong encryption and strong mutual authentication. In addition to these specific kinds of attacks on information, businesses must contend with the general problem of loss of privacy and confidentiality.

Loss of Privacy and Confidentiality

When Sun Microsystems CEO Scott McNealy said in 1999 that we have no privacy, “get over it,” he was saying more about how much information could be collected and harvested by business than about customers, patients, and the public in general’s demand for privacy. In addition to concerns about the ability of businesses and governments to analyze volumes of data from disparate sources, there is fear of unauthorized, malicious use of personal information. Consider some of the ways privacy and confidentiality can be compromised:

- Data mining across databases with information about banking, shopping, and Internet surfing
- Data breaches resulting in the large-scale theft of financial and personal information
- Inadvertent release of confidential information in violation of privacy protection directives, such as the private medical regulation known as the Health Insurance Portability and Accountability Act (HIPAA)
- Loss or theft of laptops and other mobile devices containing unencrypted private information
- Theft of customer credit card information by trusted database administrators for sale to the highest bidder

There is little these examples have in common except they are all ways in which private information can be mismanaged and disclosed. Collectively, these vulnerabilities can undermine consumer confidence and willingness to share information that in turn can hinder a business’ ability to fully utilize the benefits of information technology.

To effectively leverage the Web, organizations must cope with a wide array of security challenges:

- Fully develop, focused attacks on consumers, such as phishing, that seek immediate financial gain
- Information gathering attacks, such as man-in-the-middle attacks, that may be used in conjunction with other kinds of attacks to realize a larger goal
- The potential for a generalized fear of loss of privacy and confidentiality when information is shared online

These types of challenges can have a direct impact on business operations as the next section will explore.

Implications of Security Threats for Business

The variety of security threats businesses face online will vary and change over time. The consequences of those threats will largely remain the same:

- Reduced potential for online business due to lack of trust
- Fraud
- Identity theft
- Damage to brand reputation

Each can undermine both short-term sales and long-term objectives.

Reduced Potential for Online Business Due to Lack of Trust


Imagine you have a favorite restaurant that you have frequented for years. You learn one day that one of the wait staff has been copying customer's credit card information while processing their payments. The stolen information was then sold to others who committed credit card fraud. Would you still go to that restaurant? If you did, would you be willing to turn your credit card over to your waiter? Similar levels of uncertainty and lack of trust can limit willingness of people to conduct business online.

There is also the potential problem of security breaches in one business having an impact on other operations. If a customer frequently reads about phishing scams targeting their favorite online bookseller, the customer may become leery of trusting any online bookseller. The onus is now on the business to convince the wary customer that the business is indeed legitimate and trustworthy.

Fraud and Identity Theft

Fear of fraud and identity theft can also erode confidence in Web-based business transactions. Consumers generally face limited risk because of credit card company policies limiting liability of the cardholder in the case of fraud. Banks assume this risk but, not surprisingly, credit providers are demanding more of retailers to ensure credit card information is protected. The Payment Card Industry (PCI) Data Standards have established basic security and data handling standards for retailers; those not in compliance can expect to shoulder the cost of fraud if their security is compromised.

One of the largest data breaches in history occurred to TJX, a parent company of multiple retailers in the United States and United Kingdom. Credit card information of 47.5 million customers was stolen resulting in significant costs to banks, which had to cancel and replace compromised accounts. Lawsuits quickly followed as banks sought to recover those expenses arguing that TJX had not done enough to protect credit card data. As the TJX example shows, there can be readily quantifiable costs to businesses when fraud occurs as well as the more difficult-to-measure loss of business due to lack of confidence with a company's ability to protect customer information.

 For more information about the PCI Data Standard, see https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf. For details of the TJX data breach and its effect on the company, see several postings about TJX at the [Realtime Messaging and Web Security Community](#).

Damage to Brand and Reputation

When phishers displays a logo of a well-known bank or online auction site, they are leveraging that company's brand recognition and they are putting that brand at risk. Even if recipients are not lured into revealing information, there is still the potential for the reader to make associations between the malicious message and the brand.

The value of a brand is difficult to measure, so the damage done by cybercriminals playing on a company's reputation is equally unquantifiable. Nonetheless, anything that can leave a customer with unfounded, and even erroneous, concerns such as "how well is Company X protecting my information if they can't even prevent these malicious emails?" can damage one's brand.

Web security risks can adversely impact operations and revenues. Businesses can, however, mitigate these risks and the potential for lost trust and confidence on the part of their customers and partners.

Requirements for a Business-Grade Web

A successful environment for conducting business is built on trust between parties and confidence in the integrity of the business environment. The most basic protocols of the Web, and the Internet in general, implicitly trust the parties involved in a transaction. If an email message arrives claiming to be from JaneDoe@mycompany.com, the Simple Mail Transport Protocol (SMTP) "believes" it. If a low-level transmission control protocol (TCP) packet arrives at a router asserting that it is the third packet sent by the sender in a particular session, the router acts as if this is truly the case. Unfortunately, these kinds of transmissions are not always what they appear .

In the case of email, spammers often use other peoples' email addresses as the sender to help hide their identities. Low-level network packet transmissions can be spoofed; that is, information about the sender and other data about the transmission can be changed by an attacker. The fundamental problem is that the most basic Internet protocols use a layered abstraction (see Figure 1.5a) but business-grade services require a layered abstraction more like that shown in Figure 1.5b.

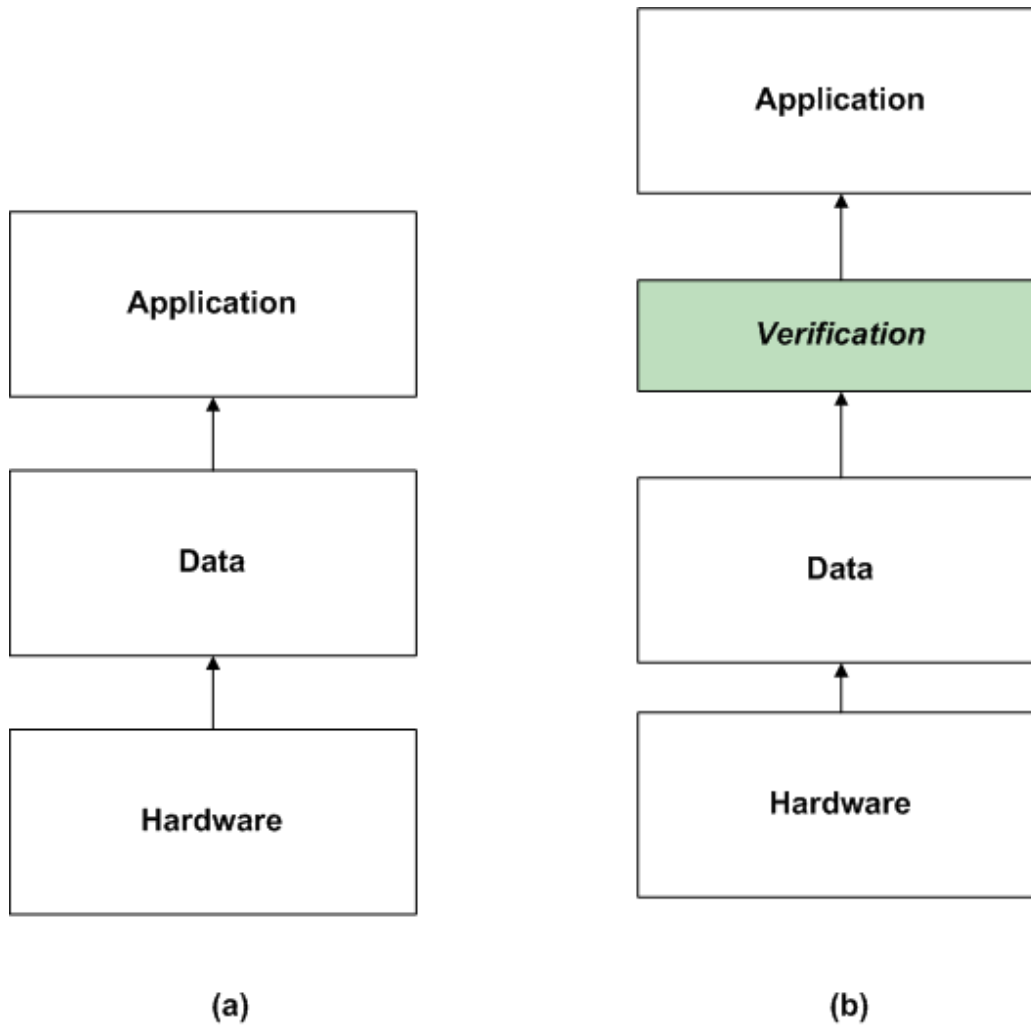


Figure 1.5: Two simplified network models (a) implicitly trusts parties in communication while (b) does not.

The verification element encompasses three components required for secure and trustworthy communication:

- Authenticated identities
- Confidential transmission
- Integrity of transactions

If any one of these is missing, communications may be compromised.

Authenticated Identities

Secure communications require that you know with whom you are communicating. Often we rely on usernames to identify a user and a password to authenticate or verify the person is who he or she claims to be.

As the earlier examples in phishing and man-in-the-middle attacks show, such attacks can circumvent simple log in schemes. Other approaches such as multi-factor authentication improve on passwords by using a combination of techniques, typically by requiring something the user knows and something the user has. A bank, for example, may require a customer to provide a password, then enter a randomly generated code provided by a security token synchronized with the bank's systems.

Although there are limitations to these techniques, they can reduce the risk of password-only authentication. A drawback of this approach is that it works well for the business trying to verify the identity of someone accessing their systems, but it is not a practical solution for customers who want to verify the identity of the online business they are visiting. Customers need another way to verify they are dealing with legitimate sites and not a phishing site. EV SSL certificates fill this need. Once the parties to a communication are confident they know who they are dealing with, the next step is to ensure that no one can eavesdrop on their session.


Confidential Transmission

Protecting information in motion is a challenge with a long history. Julius Caesar purportedly used a simple shift cipher, now known as a Caesar cipher, to communicate with his generals. The basic idea is that each letter in a message is changed to another letter a fixed distance in the alphabet. For example, if we use a distance of 2, an "A" would be changed to a "C," a "B" to a "D," and so on. Needless to say, these codes are easy to crack. The art and science of cryptography has come a long way since the days of the Roman Empire, but some basic characteristics remain unchanged.

Today, we still use algorithmic methods for changing messages, called plaintext, into a scrambled form, the cipher text. We still consider the strength of an encryption algorithm in terms of the time and effort required to decrypt a message when the key is unknown. Other characteristics, however, have changed:

- We have ways to conveniently and securely exchange keys over the same channel that will be used for the encrypted message
- Brute force, trial-and-error approaches to searching for keys are not practical with state-of-the-art algorithms and sufficiently long keys
- We now have the option to use both strong but computationally intensive algorithms and weaker but more efficiently computed algorithms, depending on the requirements of an application

Data encryption and key exchanges are fundamental to the use of both SSL and EV SSL certificates.

 Chapter 2 discusses the technical details of encryption as it relates to these certificates.

Integrity of Transactions

Secure communications are tamper-proof and non-reputable. If a customer submits a transaction ordering \$1000 worth of goods, it should not arrive at the server as an order for \$10,000.


Similarly, a customer who does place an order should not claim the order was never placed. A trusted business environment on the Web must provide this kind of integrity of transactions.

Algorithms, known as hash functions, are ideal for this task. They take a message as input and produce a fixed-length string as output. Sounds simple, except for the unique characteristics of hash functions. First, any change to the original message will yield a different output string. Even a minor change (for example, switching a comma for a period), will change the output string. The second useful feature of these functions is that it is extremely rare to have two different inputs that produce the same output. The chances of tampering with a message and somehow getting the same message digest are astronomically small. When you combine the ability to authenticate parties to a transaction, ensure that their communications are kept confidential, and provide assurances that their transactions are not tampered with and cannot be repudiated, then you have a business-grade service.

The Role of EV SSL Certificates

EV SSL certificates have been created to further enhance the level of trust and confidence in Web-based business. Threats such as phishing schemes are now so commonplace that additional measures are required to ensure current and potential customers that legitimate businesses are who they appear to be and EV certificates are one of those measures.

EV certificates are based on strong verification of a business or organization identity. The days of “no one knows you’re a dog” are over. Legitimate businesses now have the means to distinguish themselves online by using a standardized verification mechanism provided by a trusted third party.

 Chapter 3 describes in detail the steps an organization must go through before receiving an EV SSL certificate as well as the standards with which issuers must comply.

In addition, these certificates use strong encryption methods to protect the confidentiality of communications and integrity of transactions. Just as threats to information security have evolved to continue to be effective, so have the countermeasures that mitigate the risk from those threats.

Summary

The Internet has proven its importance to business, but security challenges threaten to hamper its full potential. Threats range from various forms of phishing scams and man-in-the middle attacks to the loss of confidential information and fraud. In spite of these challenges, a business environment can exist on the Web as long as three key attributes are ensured:

- Authenticated identities
- Confidentiality of information exchange
- Integrity of transactions

The Internet, however, was not designed to distrust other parts of the network or users of the system. Later additions to the family of Internet protocols, such as the SSL protocol, were added to improve security. In that same trend of identifying particular security needs and providing a means to address those needs, EV SSL certificates have been created to maintain a sufficiently secure business environment on the Web.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.