

Realtime  
publishers

"Leading the Conversation"

*The Shortcut Guide™ To*



# Extended Validation SSL Certificates

*sponsored by*



*Dan Sullivan*

Chapter 5: Future of EV SSL Certificates .....	63
Historical Patterns and the Development of Information Security .....	63
Evolution of Malware .....	65
Early Viruses and Worms .....	65
Encrypted Malware .....	65
Polymorphic Malware .....	66
Changing Phishing Techniques .....	66
Spear Phishing .....	67
E-Commerce Phishing .....	67
Social Networking Phishing .....	67
Resilient Botnets .....	68
Common Patterns in the Development of Security Threats .....	70
Near-Term Emerging Requirements .....	70
Non-Phishing Threats and Attacks .....	71
Privacy Protections .....	72
Certified Security Measures .....	73
Other Integrity Certifications .....	75
Possible Improvements to Browser Interface .....	75
Search Result Filtering with EV SSL Certificates .....	76
Advertisement Filtering with EV SSL Certificates .....	76
Possible Additional Uses for EV SSL Certificates .....	77
Certifying Enterprise Web Applications .....	78
Certifying Standards Compliance .....	78
Certifying Online Services .....	79
Summary .....	80

---

## Copyright Statement

© 2007 Realtimerepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimerepublishers.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 Realtimerepublishers.com, Inc or its web site sponsors. In no event shall Realtimerepublishers.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.

Realtimerepublishers.com and the Realtimerepublishers 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 Realtimerepublishers.com, please contact us via e-mail at [info@realtimerepublishers.com](mailto:info@realtimerepublishers.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 5: Future of EV SSL Certificates

Extended Validation (EV) SSL certificates are the first significant advance in digital certification since the adoption of the X.509 standard certificates for SSL. The creation of EV SSL certificates came about in response to a pressing business need. It is likely that additional needs will emerge and the EV SSL standard will evolve in response. Of course, we cannot predict the future, but we can use our understanding of past experiences and current challenges in business to venture possible paths of EV SSL certificate evolution.

This chapter frames the discussion of the future of EV SSL certificates around:

- Historical patterns and the development of information security
- Near-term emerging requirements
- Improvements in browser interfaces and usability
- Extended applications of EV SSLs

It is often best to start with a look to the past to understand what might lie ahead.

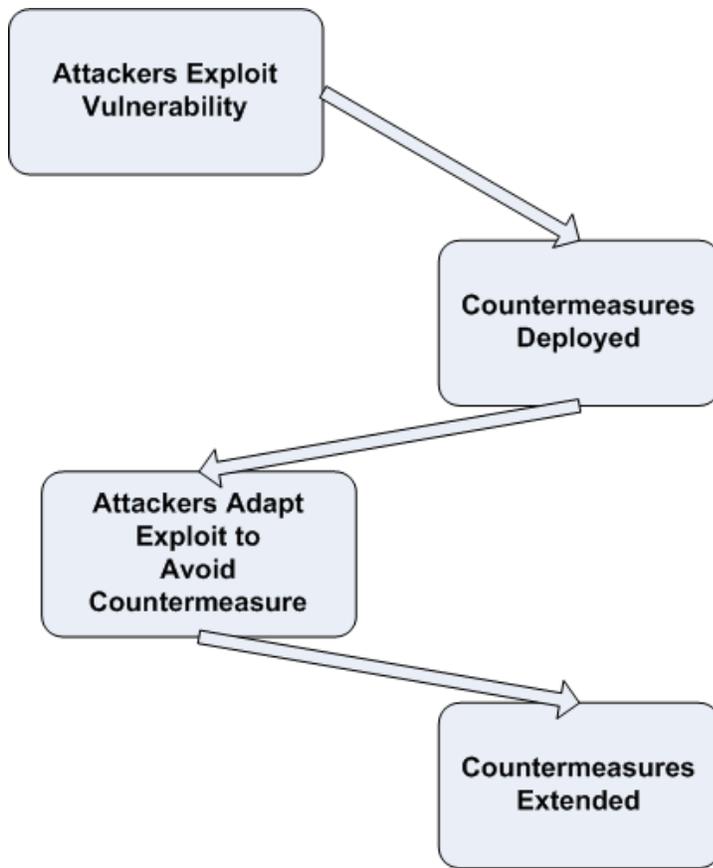
### Historical Patterns and the Development of Information Security

Information security, at least as we know it, has a relatively short history. We do not have the advantage of historians who study the rise and fall of empires or evolutionary paleontologist who study the fossil records for insight into past ages. They can examine facts and artifacts across generations and see recurring patterns that are not limited to a particular time and a particular place. Instead, we have a short and rapidly changing history.

Changes in the information security landscape occur in spans of months, weeks, days, and even hours. Take the recent Storm worm. This malware has changed to avoid detection, respond to threats, and find the right balance of spreading to as many devices as possible without becoming so exposed that it is likely to be taken down. The worm began spreading in January 2007 and quickly spread to account for up to 8% of all Windows-based malware. One of the reasons the malware is so resilient is that servers that distribute the code modify the application twice an hour to make detection more difficult.

 For more information about the Storm worm, see [http://en.wikipedia.org/wiki/Storm\\_Worm](http://en.wikipedia.org/wiki/Storm_Worm); and for the Storm botnet, see [http://en.wikipedia.org/wiki/Storm\\_botnet](http://en.wikipedia.org/wiki/Storm_botnet).

The Storm worm and botnets have managed to automate a common pattern in the history of information security: the cat and mouse game. Attackers find a way to compromise a system, systems administrators and security professionals close the vulnerability or create a countermeasure, and the attackers search for, and eventually find, another way to compromise the system. Needless to say, the systems administrators and security professionals respond as expected to mitigate the new threat and the process repeats.



**Figure 5.1:** *The evolution of information security has been a pattern of attacks begetting countermeasures which beget attacks and so on.*

As a prelude to examining emerging threats, it is useful to examine a few examples of how threats have changed; in particular, the changes in

- Malware
- Phishing
- Botnets

Each of these present distinct types of threats to information security, but their development paths exhibit common patterns.

## **Evolution of Malware**

The first malware appeared in the 1970s on the Arpanet, the precursor to the Internet. A program known as Creeper that infected the Tenex operating system (OS) would display the message 'I'M THE CREEPER : CATCH ME IF YOU CAN.' on infected systems. A clean up program, called Reaper, was deployed to eliminate Creeper, and so began the first iteration in the many cycles of malware attack and counterattack. For our purposes, the evolution of malware can be divided into three stages with subsequent stages representing more complex malicious code.

## **Early Viruses and Worms**

Early viruses and worms were relatively simple by today's standards, but as with their contemporary counterparts, early viruses and worms took advantage of vulnerabilities in OSs and applications to spread. Throughout the 1980s, viruses spread on Apple and IBM PC platforms taking advantage of the fact that OSs were stored on floppy disks with no logical access controls. Viruses spread when floppy disks were shared. Malicious code could copy itself to memory and then to other floppies, thus spreading the infection.

The first Internet worm also appeared in the 1980s. Known as the Morris Worm, it took advantage of vulnerabilities in email and network utility programs to spread. Unfortunately, the rapid spread of the worm created an unintended Denial of Service (DoS) attack on compromised servers.

Both early viruses and worms could be detected and eliminated relatively easily with basic pattern recognition techniques. As the motivation to create viruses and worms moved beyond pranks and experiments, malware writers, like bacteria in antibiotic-rich environments, had to adapt to survive. And just as some pathogens use a kind of chemical camouflage to disguise their presence in host organisms, programmers turned to obfuscation to avoid detection.

## **Encrypted Malware**

Attempts to mask viruses using encryption were a start at reducing the chance of detection, but they did not go far enough. It is true that a virus that replicated itself and then encrypted itself with a random key could not be detected using the signature-based antivirus programs. The problem for virus writers, though, is that they need to decrypt their program before it could be used. This meant that viruses would have to carry around a decryption module along with their payload and that was their Achilles Heal. Antivirus programs could use signatures to identify the unencrypted decryption module. Encrypting the payload was not enough; any data that spread by malware must be obscured and the patterns must change frequently and randomly enough to make signature-based detection impossible.

## Polymorphic Malware

Polymorphic viruses change patterns in executable code without changing the function of the code. When replicating a piece of malware, a polymorphic module injects nonsense instructions, for example  $A = A + 0$ , into the code. These extra instructions do not change the behavior of the program, so they can be injected anywhere, including into decryption modules and the polymorphic module itself. Signature-based detection was no longer sufficient.

Rather than examining the structure of viruses, which could now change, antivirus researchers turned to examining the one thing that did not change: the program's behavior. With behavior-based detection, suspected malware was run inside a sandbox environment and monitored for tell-tale signs of virus or worm activity.

The evolution of malware gives us our first indications of the efficiency of the cat-and-mouse game so often seen in information security. Antivirus researchers used signature-based detection, a low complexity solution, to combat malware as long as possible. Malware developers then tried a simple approach to avoiding detection, but encryption turned out to be too simple. Then, only when malware writers devised the means to circumvent structural detection, did antivirus researchers move on to the more complex behavior-based detection. A similar pattern of minimal changes to remain effective can be seen in phishing as well.

## Changing Phishing Techniques

Phishing has always been about tricking users into disclosing information. At first, well-known and popular companies and brands were targeted. This made sense and followed the pattern of minimal effort and maximum efficiency seen before.

Phishers may spam hundreds of thousands or more email addresses with lures. How can they be sure the lures will look sufficiently legitimate to maximize the number of people who are tricked? Initially, the answer was to use the names of large institutions such as Citibank, eBay, Paypal, and other businesses with large customer bases. Chances are many of the recipients will have an account with one of these organizations.

The problem for phishers, though, is that as the public learned of phishing schemes, it was more difficult to convince users that lures were legitimate. Phishers honed their lures and in some cases changed their methods. We can expect to see more adaptations, such as:

- Spear phishing
- E-commerce phishing
- Social networking phishing

## Spear Phishing

Spear phishing is a smaller, more targeted form of phishing. Spear phishing schemes often use smaller, regional businesses and target fewer victims than early, blanket-phishing schemes. Spear phishing has a number of advantages for phishers:

- They involve lower-profile phishing schemes that are less likely to draw attention to themselves.
- Victims may be less suspicious of messages that come from a regional business than one known to be commonly targeted in phishing scams.
- This method includes targeting new types of victims, especially businesses. For example, in early 2007, the Supervalu Inc. grocery chain fell victim to a business phishing scam and mistakenly deposited payments for suppliers into fraudulent accounts.

Many of the same anti-phishing techniques that are effective against blanket phishing, such as Web site reputation checks and EV SSL certificates, work with spear phishing schemes as well.

## E-Commerce Phishing

Phishing has traditionally depended on email to deliver a lure. As spam and phishing filters improve, phishers are looking for new ways to deliver lures. One such method is through e-commerce sites. A basic scheme is as follows: A phisher sets up a fraudulent e-commerce site and purports to sell products. The site uses application programming interfaces or other techniques to get product and pricing information from legitimate sites. When the site is queried for prices on a product, it returns a lower price than its competitors. Unsuspecting buyers attempt to purchase the item and in the process provide phishers with names, addresses, and credit card information. Again, EV SSL certificates can reduce the effectiveness of this kind of phishing scheme.

## Social Networking Phishing

The rise of social network phishing demonstrates another characteristic of information security—attackers follow the herd. As more potential victims adopt a technology, such as email, instant messaging, smartphones and social networking, the more attackers will be lured to try to exploit the platform.

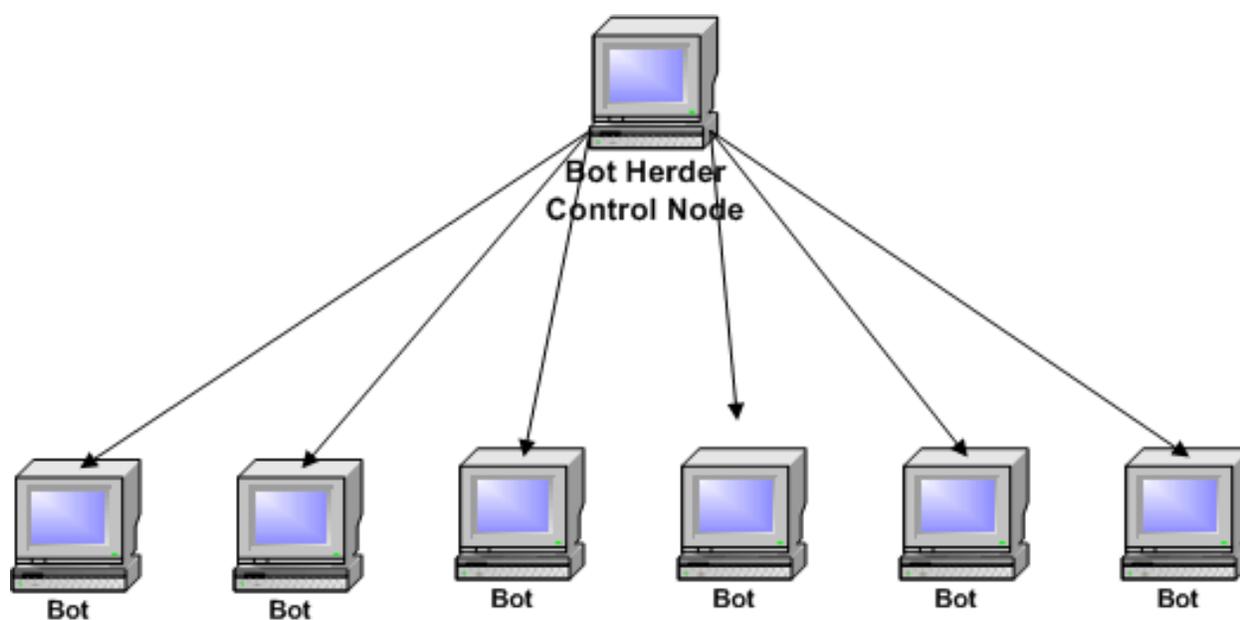
The wealth of personal information is an obvious reason for phishers to harvest data from social networking sites. Attackers have also used social networking sites to lure victims. A MySpace worm appeared in 2006 that exploited vulnerabilities in the social networking platform to change links in a victim's page that would lead visitors to a phishing site instead of the original site linked to by the victim.

Phishers are making small changes in their methods (for example, by targeting smaller pools of potential victims and using regional rather than national business) as well as adapting more varied distribution techniques (such as e-commerce and social network phishing). Similar to the pattern seen with the history of malware, phishing is a dynamic and adaptive phenomenon.

## Resilient Botnets

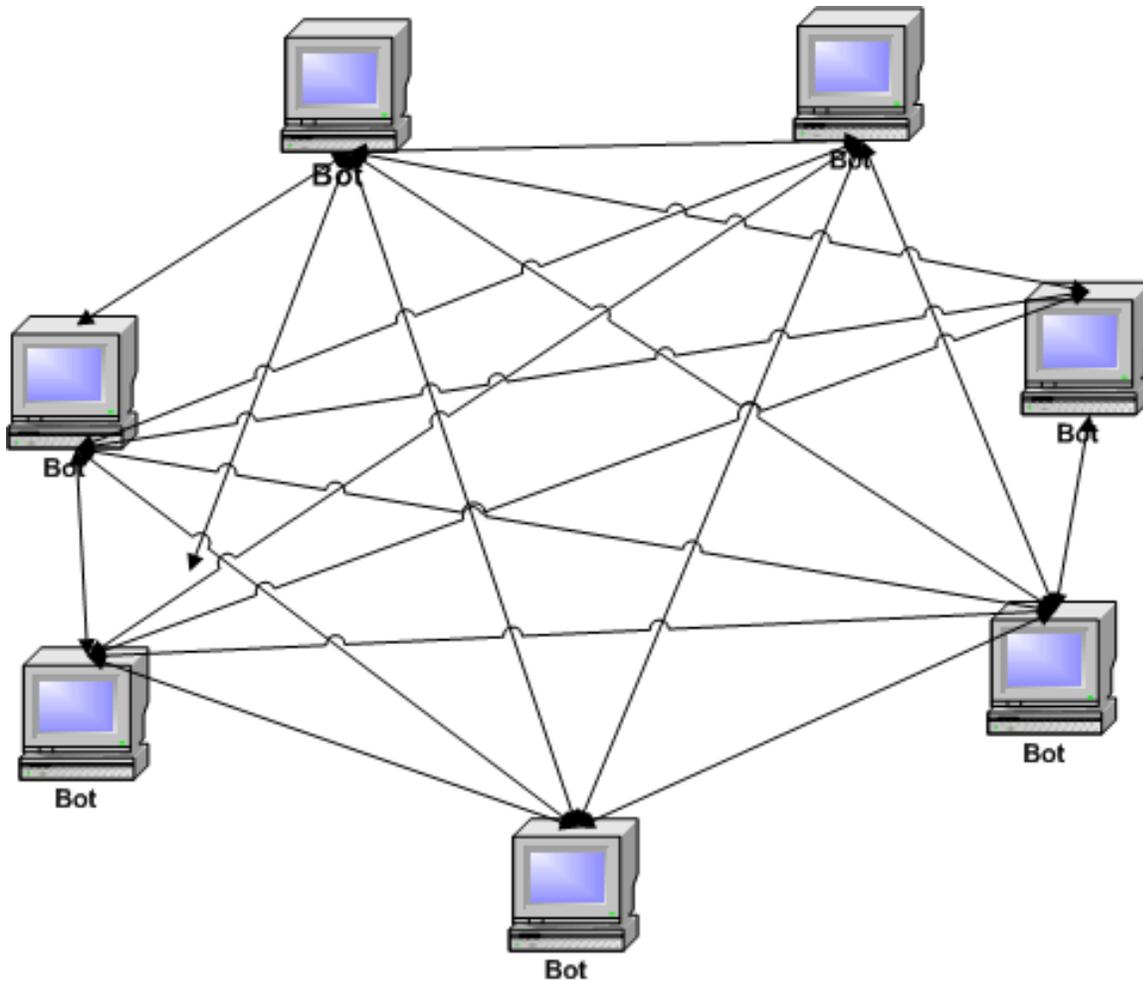
Botnets are networks of compromised computers that can be controlled by unauthorized users. Botnets are blamed for generating most of the spam that floods email systems, for launching distributed DoS (DDoS) attacks, and for providing compute resources for other malicious activities, such as password cracking.

The architectures and functions of botnets have changed, as those that create and control these networks strive to grow and maintain their ill-gotten resources. Early botnets used a hierarchical command and control structure (see Figure 5.2). This architecture had the advantage of being easy to implement yet effectively delivered needed functionality. A serious drawback, however, is that once the command and control node was identified and isolated, the botnet no longer functioned.



*Figure 5.2: Early botnets used a hierarchical command and control structure.*

A move to peer-to-peer architectures (see Figure 5.3) introduced more resilient botnets. No single command and control node managed the entire network, so it was no longer possible to disable the botnet by removing one node. If a management node was removed, another node could assume its role. Variations on the design, such as distributing partial lists of other bots in the network to nodes, are used to balance efficiency with resiliency.



**Figure 5.3:** Peer-to-peer botnets use a distributed command and control model that is more likely to withstand the loss of some nodes.

Recently, investigators have discovered that the Storm botnet is using defensive measures, including DoS attacks to prevent researchers from learning too much about the network.

### **Common Patterns in the Development of Security Threats**

As the history of malware, phishing, and botnets shows, there are common patterns discernable in the development of security threats:

- Threats emerging to exploit vulnerabilities in OSs, applications, and Internet services based on the popularity of those systems and services
- Countermeasures countering early versions of a threat only to trigger evolution of the threat
- The development of minimal changes to design and methods to avoid a countermeasure
- An occasional leap in complexity, such as the use of polymorphic viruses and peer-to-peer command and control structures, when incremental changes are insufficient to circumvent existing countermeasures

It is not unreasonable to assume that similar patterns will continue to appear. It is also safe to assume that EV SSL certificates will be used in new ways and the EV SSL standard itself will change to adapt to new threats.

At this point, it is time to shift our attention from the past and begin to examine ways in which the still-young EV SSL standard might adapt to meet needs just on the horizon.

### **Near-Term Emerging Requirements**

The CA/Browser Consortium developed EV SSL certificates to address the compelling need for better protections against phishing. By establishing a standard that is widely backed by certifying authorities (CAs) and browser developers, the group not only solved an immediate need but created a framework that can be used for additional needs as well.

There is no way to know for certain the next set of applications for EV SSL certificates, but some possibilities include:

- Use against non-phishing threats and attacks
- Establishment of privacy protections
- Certification of security measures
- Other integrity certifications

In each case, the ability to rely on a trusted third party to enforce well-defined standards of business practice enables these potential services.

## Non-Phishing Threats and Attacks

For many years, malware largely targeted desktop OSs and applications. The popularity of Windows and other Microsoft products, such as Word and Outlook, made them prime targets for attackers. Recently, malware targets and delivery mechanisms have shifted toward the browser.

Many kinds of browser- and Web server-based attacks are occurring:

- In September 2007, it was reported that the Bank of India Web site had been compromised and visitors were redirected to another Web site where malware was downloaded onto their devices.
- Malware developers have used Web sites to distribute Trojan horses that exploit vulnerabilities in popular plug-ins, such as RealPlayer and the Skype telephony client.
- Many browser-based attacks use HTML and JavaScript hacks but others have successfully used purely social engineering attacks to lure victims to click through and download malware to their computer. In one case, *PC World* reported an purported patch to Adobe RealPlayer was served from a Web page that did not even try to hide the non-Adobe source of the file (Source: “Security Alert: Browser Plug-Ins May Be Malware,” *PC World*, June 22, 2007).

EV SSL certificates are immediately useful today in the case of the victims being redirected from legitimate Web sites to malware delivery sites. Had a victim been to a financial site displaying a green bar and then automatically redirected to a non-green bar site, the victim would have an obvious visual cue that something was wrong.

As for attacks that lure people to other sites but do not make significant attempts to hide obvious clues, the lack of a green bar in the address line might help, but that is debatable. It could help because users would not have to read an actual URL to notice that a patch for a product from Company A is coming from a site named something completely different. There is also the fact that some consolidated download sites offer drivers and patches for many products. Users could easily confuse a rogue site for one of these legitimate service sites. Today’s EV SSL certification is not a guarantee that a site is free from malware, however, certifying a site or a business that follows security management best practices is a possible future extension of EV SSL certificates.

 For more information about security certifications and other potential applications for EV SSL certificates and related certificates, see the section Possible Extensions for EV SSL Certificates later in this chapter.

## Privacy Protections

Privacy concerns are a long-standing issue in information management. State, national, and transnational governments have enacted legislation to protect the privacy of individuals in a range of circumstances:

- In the United States, the federal HIPAA legislation defines requirements for protecting the confidentiality of protected health information of individuals.
- In the European Union (EU), privacy directives establish broad protections for personal information and rights related to correcting mistakes in erroneous data.
- Individual states within the United States have passed laws to establish rights of individuals to protect their personal financial information and to be notified if such information is lost, stolen, or otherwise disclosed in unauthorized ways.

 The Federal Trade Commission (FTC) in the United States has also undertaken a number of privacy initiatives; see <http://www.ftc.gov/privacy/index.html> for details.

In addition to the privacy protections established in legislation, individuals may enter into agreements with businesses. For example, companies often define privacy policies related to data they collect on Web sites. Today, users would have to read through sometimes legalistic policies to know what their rights and responsibilities are. They would also have to understand the implication of clauses indicating the rights of the site owners to change the policy at any time. Following the EV SSL certificate model, companies might want to distinguish themselves by the level of privacy they guarantee to protect.

Consider the case of the emerging business of personalized genome sequencing. Companies are now offering customers the chance to sequence their own DNA and search for indications of genetic predispositions to diseases or to better understand one's ancestry. Although there may be many individuals who would like to have this kind of information, there are privacy concerns:

- Will insurance companies have access to the information and potentially deny coverage to individuals with particular genetic characteristics?
- Will employers be able to subscribe to a genetic scoring service, akin to a credit rating score, for potential employees?
- Will the data be disclosed to third parties for marketing purposes so that, for example, people with a predisposition to Type II diabetes could be targeted by pharmaceutical companies?
- Will the data be completely deleted from company records if the customer requests it?

Right now, customers can ask these questions but have no guarantees other than the claims of the business providing those services. Potential customers might be more willing to engage in such a service if the policy statements were not only clear and agreeable but also recognized as enforced by a trusted third party.

A possible extension to EV SSL certificates is a certified privacy practice. In such a model, CAs would follow an established standard to review companies' privacy policies, audit the companies' data management practices, and verify that privacy policies are adhered to. This kind of new service would require a new standard or standards, but much of the service infrastructure in place for EV SSL, such as registering authorities (RAs), CAs, and browser developers, could be reused for privacy protections.

 See Amy Harmon's *New York Times* article "[My Genome, Myself: Seeking Clues in DNA](#)" for one person's account of with personalized genome sequencing and some of the privacy questions that arise with patrons of these services.

### **Certified Security Measures**

We have seen examples in this chapter of malware threats from compromised Web sites. News stories bring to the public's attention the problem of information lost due to a range of causes:

- Corrupt database administrators who sell customer information to unscrupulous data brokers
- Weak network security at a major retailer that is cracked by attackers who may have accessed 96 million customer records
- An employee with an online customer relationship management (CRM) service became victim of a social engineering attack that led to phishing attacks on customers whose data was accessed

Customers may begin to wonder, if they don't already, how secure are the companies they do business with? We expect governments and large financial institutions to have the resources to maintain sound security practices, but what about other businesses? How are consumers to decide which businesses to trust with their information?

Ideally, businesses would have a security equivalent to the electrical device industry's Underwriters Laboratory (UL). Such a trusted third party would test and verify that the security practices of an organization meet an established standard. If this could be done, and it is not at all clear that it could be, here are some possible criteria for evaluation:

- Access control policies for both logical and physical access to IT resources and data
- Network architecture and defenses in place on the network, including vulnerability scanning
- Device defenses, such as antivirus, anti-spyware, firewalls, and host intrusion prevention systems (IPS)
- Security policies and procedures
- Incident response plans and forensic capabilities
- Application development methodologies, code reviews, and application vulnerability scanning

Perhaps security management standards, such as ISO 27002, could be used as a foundation for such an evaluation. Security management is, however, a complex area. Even relatively narrow standards, such as the Payment Card Industry (PCI) Data Security Standard (DSS), have met with mixed reactions. Some businesses find the standards leave too much room for interoperation and others find the implementation cost prohibitive.

 For a summary of the ISO 27002 standard, see <http://www.27000.org/>. Details about the PCI DSS is available at [https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf).

Assuming for the moment that the difficulties with establishing a standard could be overcome, the EV SSL certification infrastructure could be readily applied here. Digital certificates could be issued to companies that meet established standards. Those certificates could then trigger a visual cue in a browser when a customer visits the company's site and people would know that a trusted third party is vouching for the security practices of the business.

### **Other Integrity Certifications**

EV SSL certification was developed to have a trustworthy way of demonstrating businesses are legitimate operations and are actually who they claim to be. This is only possible with the combined resources and commitment of CAs and browser developers. As we have seen with privacy and security considerations, the business and technical infrastructure in place for EV SSL certificates is amenable for use for other certification services.

Expanding the types of certifications will likely be driven by market need but could include diverse interests such as:

- Environmental concerns and green business practices
- Fair trade and fair labor practices
- Manufacturing quality controls
- Customer service quality standards

Basically, when a business wants to make a claim about its operations, practices, and products and wants a trusted third-party verification that cannot be forged by frauds, it could use the same business and technology resources created for EV SSL certificates. In the future, we will likely see emergence of business certifications that go beyond the scope of the current EV SSL certificates. We will also likely see additional uses of EV SSL certificates to improve browsing.

### **Possible Improvements to Browser Interface**

The browser plays a central role in the use of EV SSL certificates. Through the browser, users are made aware of the EV status of a business. There is no need to find certificate options in browser menus or try to make sense of public key cryptography details stored there. Instead, users have a pronounced visual cue with the green bar. They also have simple access to additional data about the business by clicking on the vendor name at the end of the green bar. There may be additional visual cues embedded in browsers in the future; it is also likely that independent developers may extend browser functionality with add-ons that make use of EV SSL certificates.

### **Search Result Filtering with EV SSL Certificates**

One possible improvement to browser interfaces is the use of EV SSL certificates to filter search results. Currently, when a user searches for a particular item, say “camping equipment,” search engines return results based on how well the search terms match with the content of the site. This process is site-centric in that the sites control, to some degree, how well they match particular terms. The well-established industry of search engine optimization (SEO) is a testament to how much effort goes into designing sites to improve the chance of high ranking in search results.

EV SSL certificates offer a chance to turn more control over to users. If, that is, a browser plug-in could be designed to allow users to filter results based on the existence of EV SSL certificates. The plug-in could work like this:

1. The browser user downloads and installs an EV SSL certificate detection plug-in.
2. The user configures the plug-in to filter results from the user’s favorite search engine.
3. The user enters search terms into an input box on the toolbar.
4. The search is performed by the search engine and the results returned to the browser.
5. The plug-in intercepts the results and parses URLs.
6. The URLs are checked for the existence of a valid EV SSL certificate.
7. If an EV SSL certificate exists, the site’s listing is passed through to the user; otherwise it is discarded.

The speed of this process could be improved if the search engine cached EV SSL certificate data; if that were the case, there would be no need to visit the Web site before listing the entry. This would require the search engine to check the status of the EV SSL certificate fairly frequently and a reasonable balance would have to be struck between frequently checking the status and maintaining adequate search performance.

### **Advertisement Filtering with EV SSL Certificates**

Advertisements are commonplace on the Internet. We see them in search results, in online email services, on social networking sites, on blogs, and on many of our favorite Web sites. Today, we depend on a variety of methods to ensure that we shop with reputable businesses. For example, users might:

- Depend on advertising services, such as Google and Double Click, to screen legitimate businesses.
- Install browser add-ons that verify the integrity of Web sites by checking sites for malicious software or logging complaints about sites.
- Click through on ads only from trusted sites, assuming that trust among sites is transitive.

These solutions are a start but they have serious limitations. Advertising services are largely automated. As long as one can pay the bills, one can generate key word-based ads and have them served up in related contexts. Online advertising companies sell ads; they are not necessarily security screeners.

Add-on integrity checkers are an improvement over blind faith in advertising firms, but their data is limited to what can be determined by crawling the site or registering as users and tracing spam back to those sites. These services are definitely useful and worth employing, but they are not as comprehensive as an EV SSL certificate-based approach.

Web sites can subscribe to the advertising services that provide ads tied to the content of the site. The site designers in such cases do not screen advertisers; thus, assuming that vendors advertising at a favorite Web site are as trustworthy as the site creators is a mistake. A better solution is to use ad filtering software that allows advertisements only from EV SSL certificate sites. Such an add-on could work like the search result filtering process described in the previous section.

 It should be noted that some Web site creators who earn revenue through ads frown upon blanket ad blocking. A Firefox add-on called Adblock Plus (<http://adblockplus.org/en/>) prompted a wholesale effort to keep all Firefox users from accessing ad supported sites, regardless of whether the user had installed an ad blocking component. The Why Firefox Is Blocked campaign (<http://whyfirefoxisblocked.com/index1.php>) provides arguments why ad blocking is unfair. Similar arguments could probably be made for ad filtering.

The green bar is an effective way to quickly convey information with a visual cue, but there may be additional ways to leverage EV SSL certificates to provide an improved and more secure browsing experience for users.

## Possible Additional Uses for EV SSL Certificates

As noted earlier, EV SSL certificates and the business processes that support their creation and distribution, are well suited to other areas in which a trusted third party can vouch for the integrity of a business or system. We will consider three such potential applications:

- Certifying enterprise Web applications
- Certifying standards compliance
- Certifying online hosting and services

### **Certifying Enterprise Web Applications**

As the efficiencies of delivering software as a service grows, there will be a growing need to certify aspects of Web applications. This is especially true of services that will either store sensitive data or have access to intellectual property and trade secrets. These include:

- Hosted ERP solutions that include accounting, budgeting, forecasting, and inventory management
- Desktop replacement applications that will be used to create, store and share documents with confidential and proprietary information
- Vulnerability assessment services that analyze code for potential security weaknesses
- Shared storage services that allow business partners to establish virtual disks on line for sharing files over the Internet

There are probably many other examples one can think of that involve trusting an application or service that runs in a browser.

Today's EV SSL can address some of these needs. For example, an accountant logging into an online ERP service would notice the EV SSL-specific green bar. Other systems, such as code analysis programs, may be used as part of an automated workflow process.

For example, at the end of the day programmers may check in code to a repository. An automated process then collects modules, compiles them and builds an application that is run through a series of regression tests and code analysis applications. Before sending proprietary code to an outsourced service, one had better be sure it is going to the right place. An automated method for verifying the information contained in an EV SSL certificate used by a code analysis service would meet that need. In some cases, it is not just a particular service that must be verified, but the quality of business processes as well.

### **Certifying Standards Compliance**

Professional organizations and standards bodies have established best practices and sometimes have ways to recognize adherence to these best practices. Compliance with stringent standards is one way to distinguish oneself in a crowded market. For example, a company that earns ISO 9000 quality certification would understandably want to make their achievements known to customers. The ISO 9000 family of standards addresses a wide array of quality controls including:

- Operational processes
- Monitoring activities
- Recordkeeping
- Defect detection and correction
- Reviews of quality control procedures

How can a business that achieves and maintains the quality business processes required to earn ISO 9000 and similar certifications convey this to customers? Displaying logos from certifying organizations is one option, but visitors can reasonably question whether such displays are legitimate. Bogus sites used in phishing scams routinely steal the entire look and feel of a legitimate business' Web sites. A digitally signed EV SSL certificate from a trusted third party used along with a certification logo can provide assurances that a company has legitimately earned recognition.

### ***Certifying Online Services***

Let us consider a hypothetical business situation: An entrepreneur has an idea for a new business that provides services online. The entrepreneur is an expert in a particular business domain but not information technology (IT). She already outsources accounting and legal services, so she decides to outsource some IT services as well. She would like to:

- Host a Web site with a hosting service
- Add computing resources as the business grows
- Add redundant data storage to minimize the risk of data loss

There are companies offering these services, but how is the entrepreneur to know which businesses are sound and follow IT management best practices? How is she to know—if some of the providers in the market are resellers—that their providers follow sound practices? Online businesses depend on the quality of their providers just as brick and mortar businesses do. Can small and midsized businesses send inspectors into providers' sites to inspect the quality of the way services are delivered? Would they know what to look for?

Following the model of EV SSL certificates to use trusted CAs, one can easily envision a model for certifying online services. It would be especially useful, for example, when visiting a service provider to be able to access the full chain of service providers that are used to deliver a service. For example, when visiting a service, it would be useful to know whether that provider uses other services and, if so, whether the additional services have also been certified as following industry best practices.



*Figure 5.4: A hypothetical example of the type of information that could be displayed to describe a chain of certifications indicating the quality of services provided.*

## Summary

EV certificates are a major step forward in helping establish the trustworthiness of Web-based services. Phishing has been, and almost certainly will continue to be, a problem that plagues businesses and their customers for the foreseeable future. EV SSL certificates provide the best method yet for distinguishing legitimate business from fraudulent sites. Earlier chapters have examined the business case for EV SSL certificates and provided some details on the new certificate's standards. In this chapter, we have turned our attention to the future.

IT and security is as dynamic as the free market itself. New opportunities and demands are cropping up constantly. The EV SSL certificate has established a model for using a combination of trusted third parties and secure digital certificates to attest to the integrity of a Web site. If the conjectures of this chapter withstand the test of time, we will see a wide array of extensions to EV SSLs that address the needs of as-yet-unmet requirements of business.

## 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>.