GeoTrust®

Best Practices for Securing Your Enterprise:

10 Things You Need to Know

white paper

In today's global economy, businesses depend on the Internet like never before -- enterprises are increasingly conducting e-commerce transactions and opening up access to their network resources to vendors, business partners, customers and remote employees. Yet, while it has become more convenient to do business online, it has also become more difficult to ensure reliable and secure data exchange and communications. Continually evolving security threats and changing regulatory standards can make maintaining a trusted online environment a challenge for any size enterprise.

In this White Paper, we'll prioritize our "Top 10" recommended security practices for building online trust both inside and outside your enterprise. While these guidelines are not comprehensive, they are focused on the most critical areas every enterprise needs to adopt -- from running SSL on servers to supplying client side SSL certificates to employees, to establishing solid policies and procedures for security and embracing paperless transactions.

1 Without SSL encryption, the integrity of data is compromised

Deploy SSL Server Certificates throughout your enterprise. SSL is the most widely deployed security protocol in the world. It should be deployed on any and all servers to protect any confidential and personal information that is passing from browser to server.

Secure Sockets Layer (SSL) encryption is one of the leading technologies used today to secure web sites, intranets, extranets and other server-based applications. Without it, the integrity of data exchanged over public and private networks can be compromised, ultimately affecting business continuity and your bottom line. SSL safeguards network access, online communications and digital transactions by enabling a secure channel between your servers and your users.

Awareness and understanding of the benefits of SSL technology has expanded considerably over the past several years. More and more users are looking for the lock symbol indicating that a session is encrypted with SSL.

Millions of sites have installed the X.509 special server digital certificate that activates SSL between browsers and servers. The support for SSL is already built into all modern web browsers and servers so all that is needed from the enterprise perspective is the simple installation of the certificate on the server. Once the browser and server perform their handshake, all data transmitted from one to the other is encrypted, preventing any eavesdropping that might jeopardize the security or integrity of the data transmission.

2 Without robust physical and network security, sensitive corporate data is at risk of intrusion

The use of firewalls, intrusion detection, client PC virus software, server-based virus checking and keeping all systems up to date with security patches will prevent most types of threats from impacting operations, compromising sensitive data or threatening your business continuity.

Network security is about computer systems and network access control, as well as detection and response to unwanted incursions. The risks from poor security are tremendous: theft, interruptions of service, physical damage, compromised system integrity and unauthorized disclosure of proprietary corporate information.

To secure network access paths, start with the basics, such as locking computers that are not in use. Beyond the basics, more robust solutions include key card access, hardware tokens or biometric access to especially sensitive areas.

Firewalls are an essential part of network security. Firewalls restrict access from one network to another and inspect and restrict all traffic flowing through the network. Firewalls should restrict access from the Internet and from one internal network (e.g. application servers) to another network (e.g. database). It is necessary to carefully construct the IP address ranges and the ports to which the firewall will open access. In addition, it's recommended to use multiple layers of firewalls for distinctly different functional portions of the network – one for the demilitarized zone (DMZ), a second for the web server, a third for the application server and perhaps a fourth for the database layers.

Intrusion detection systems watch for attacks, parse audit logs, alert administrators as attacks are happening, protect system files, expose a hacker's techniques, illustrate which vulnerabilities need to be addressed and help to track down perpetrators of attacks.

Another must-have is up-to-date virus and trojan checking software on all client machines. There are thousands of viruses and each new one is more sophisticated and more damaging than its predecessor. A tremendous and costly amount of damage has been done by the last few worldwide email-based viruses. A particularly robust solution is the server-based virus software that runs on email transfer machines (such as Microsoft Exchange) to prevent infected messages from moving on to users or from leaving one client to infect others.

Finally, the simplest but most powerful thing of all – ensure every security patch for all operating systems and applications is applied on all systems as soon as they come out. Hackers know well the vulnerabilities of Microsoft's Internet Information System Web Servers and seek sites running them as easy targets. Patches that make IIS not vulnerable have been freely available for years and yet over 30 percent of IIS systems on the public web are not up to date. This one is worth repeating: apply all security patches immediately.

3 Building an effective in-house PKI system will take considerable time and expense. Opt for managed PKI services.

Having security services fully managed will allow you to focus on applications needed to drive your business while a trusted third-party builds out the complex, secure and expensive public key infrastructure and manages it for you.

Public Key Infrastructure (PKI) is a tool to enable online applications to be used in ways otherwise not possible. Without an efficient method for issuing, revoking and managing credentials, businesses would not be able to deploy a benefits system on an intranet and expect employees to use it exclusively for their benefits information, especially if a large percentage of employees are remote. Similarly, a sales force would not be able to fully utilize a CRM system – the crown jewel of the company – if access was not safe and secure. Businesses are clamping down on the uses of e-mail and many are banning instant messenger usage – all because these systems are not yet secure.

Early generation PKI was great in theory, but in practice it required a complex install of software and hardware, it required specialized IT talent and it required special security to protect systems. Needless to say, all of this also translated to tremendous financial cost. But, PKI has matured and sufficient innovation has occurred to the point where it can be an outsourced component of applications. A trusted third party – a certificate authority (CA) – can build, maintain, manage and keep secure the public key infrastructure an enterprise needs. The CA behind a fully managed service has expertise in authentication techniques and methodologies. The enterprise knows the business rules it wants to implement and the applications it needs to deploy to automate its business processes. The integration point is how the certificates are used in the applications to implement security. Many applications are already certificate-ready like browsers, email and VPNs and the trend is to do this more and more.

The key components of a fully managed security service are flexible authentication models (how do we know individuals are who they say they are?), an administration interface (who from the organization is authorized to make changes and control the process?) and an operational interface (where do the individual constituents of the organization come to get their credentials?).

Most organizations have needs in one or more of the following application areas that can be outsourced to a trusted third-party: secure access, secure messaging and paperless transactions. Secure access to corporate networks like the intranet and access to critical applications like CRM systems for employees is a critical need for all large organizations. Secure messaging for email or instant messenger provides a mechanism to securely identify the message sender and to protect the contents from eavesdropping. While a paperless transaction takes a paper-based process that requires intent to be demonstrated today with a “wet” signature and makes it totally digital to save time and cost of paper-based processes.

4 Free software will crack your password in 30 minutes

Passwords are weak and getting weaker, making your secure systems vulnerable. Dramatically decrease that vulnerability by enforcing strict password usage rules.

Passwords are weak and getting weaker as computers get faster and stakes of cracking passwords get higher and more enticing to those "bad guys". Cracking passwords is getting more fruitful as more mission-critical systems are networked. With free downloadable software anyone can crack a 6-character password in 30 minutes and an 8-character password in six hours.

You need to immediately set rules about how people construct passwords (use upper and lower case, always include at least one number and punctuation character, do not use names from your personal profile, make them at least 8 characters), and how often they change them. Most importantly, where you need to continue to use passwords, make sure all passwords disable after five failed attempts to thwart brute force cracking attempts. Get and run password crackers internally to root out weak passwords. Then, begin to shift over to low-cost, outsourced authentication and digital SSL certificate services to replace these passwords.

5 Email is leaking your business secrets

Issue all employees digital client certificates for signed/encrypted email to protect corporate data and to increase confidence in the origination, authenticity and confidentiality of all corporate communications.

Secure messaging (think e-mail for now but later, instant messaging, voice over IP and so on) is about making sure only the intended recipients of a message can read it. The more that email is used, the more important it becomes for company confidential information. This is especially true for email going outside the enterprise. Email moves across the public network from server to server in plain text. Servers along the way can and do save all messages they touch and have the right to do so. In most email systems, a sender has no control over who gets a forwarded email message and no audit trail showing this has happened.

With a simple exchange of client certificates, any two employees can now sign and encrypt messages to each other. It can be proven that these messages have not been altered; their origin can be verified and no eavesdropper on any system in between can read the message. This should be required on company confidential email. Furthermore, organizations should also deploy a secure instant messaging product quickly and disallow use of non-secure IM. Instant messaging has become a common part of business and serves a very useful function; however, critical company information is being transmitted over IM systems and could be archived by uncredentialed parties. With a secure IM, that would no longer be an issue.

6 Traditional access control solutions are either ineffective or costly

Replace weak password entry-points and expensive time-synchronized tokens to secure systems with digital certificates which are much more secure than passwords, lower cost than secure tokens and yet, when fully managed, are easy to deploy.

SSL supports authenticated identity on BOTH sides: server and client. When the server presents a certificate to the client it means that the server has been authenticated (the organization that has domain control acquired the certificate and has been validated) and the client (browser) verifies that the certificate domain and the server domain match. When the client presents a certificate to the server it means that the client has been authenticated. Client authentication involves verifying the identity of the human and that this human and the certificate are bound to the machine communicating with the server. These client SSL certificates reside in the browser and in this way replace password access to secure web sites.

Certificates are much more secure than passwords because one cannot socially engineer away another person's certificate. Stealing their computer with the certificate on it doesn't work because it still requires a password to activate the certificate. Because certificates are much more secure, more important applications can be made accessible like CRM systems and corporate intranets.

Many companies are or will soon be installing virtual private networks (VPNs) to allow secure access to critical systems for remote users. This is a great move but do not weaken this by allowing identification via password; instead require client certificates installed in the VPN for entry.

Time-synchronized tokens are small devices that generate a number that the user needs to enter into a web page for secure access to a network or application. Unfortunately, they are expensive, people lose them, batteries fail and you can "loan" them to others easily. Implement a managed security service that issues and manages the lifecycle of client-side certificates.

7 Your web site can be spoofed with a point and a click

Project and protect your business identity through your web site using a trust mark establishes both identity and trust with site visitors.

SSL is vital for encryption when dealing with sensitive data. But SSL does not provide identity about the web site being visited – this is the "dirty little secret of Internet security." To protect your business identity on your web site, use a trust mark or site seal which can not be copied. For organizations, this will eliminate the possibility of their site being spoofed and for a customer it provides the confidence that they are on a legitimate web site. Unfortunately, many existing "identity" products (seals) do not provide protection – they can be click-copied. Visit any web page with a graphic icon or seal on it and right click to see the menu.

Instead, use a dynamically generated site seal that can not be copied. For example, GeoTrust site seals are placed on web pages to identify that the site is legitimate, authentic and validated via an active call to a trusted third party. First, they consider the confirmation of site identity of the owner of highest importance. Second, it is designed to combat fraudulent usage. Third, it provides a "self-policing" capability that is unique to the web. If it determines that it cannot confirm the identity of the site owner from which it is launched, it causes the image to completely disappear. Finally, it links to a rich repository of validated information about the site and its owner to assist the user – and ultimately the site itself. This establishes trust with the merchant that will hopefully lead to numerous transactions.

8 Testing in production is tempting fate

Create a demilitarized zone (DMZ) to cordon off risky network activities from your business-critical production network segments for all modem access, for simulating production or for allowing customers to do any kind of acceptance testing.

Allowing modem access into the heart of secure networks is one of the most common sources of intrusion. There are hundreds of people with what are called war dialers who try to access corporate or government systems via modem banks. They are frequently successful.

Create a DMZ that has access to the Internet but limited access to internal networks. This is accomplished through careful setup of firewalls that cordon off the DMZ from the rest of the network while still allowing full Internet access. The firewalls protect the critical portions of the network from this DMZ.

If customer acceptance testing is part of your business, only allow this kind of testing through the DMZ.

9 The weakest link in your security is your people

Define your security protocol. This is perhaps the most overlooked, and the most dreaded of the 10 guidelines, yet it is the easiest and arguably the biggest impact item of all: write it down, communicate it and enforce it.

Security is only as strong as your organization's weakest link. Security is never entirely automatic, it involves people. People have the biggest impact on how successful an organization's security strategy will be. The "bad guys" have found that social engineering is the easiest way to breach an organization's security. Organizations can combat social engineering and simple errors best by having clearly written, clearly explained security policies that are enforced.

Clearly document the appropriate processes and rules for accessing the facilities, accessing the networks, acceptable use of company systems and networks and acceptable use of company email and browsers.

List standards that are supported and those that are not. Include operating systems that are allowed on the network and explain why others are not. Allowing a visitor to come in to your conference room where there is a network tap and plug in, is a very common way networks are penetrated as quickly as you can say "Trojan Horse".

10 "Nobody knows if you're a dog on the web"

Start using well-tested, mature authentication technologies to establish identity of anonymous web-based individuals. Streamline your business through paperless transactions.

"Nobody knows you are a dog on the web" is a famous New Yorker cartoon that graces many web sites, presentations and even T-shirts. This points to the single biggest threat in using the web for critical transactions. The standard procedure to authenticate an individual is to query them about a set of shared secrets only you and the other person could know. The challenge with conducting business over the web is that the individuals are unknown to the business and therefore there are no shared secrets.

Many organizations that require their customers to sign up, register or fill out applications are looking to eliminate manual paper processes and the manual approval process. In order to conduct online applications, organizations must be able to authenticate the consumer is who they say they are and have the ability to generate e-signatures.

Conclusion
The Internet represents an opportunity for enterprises to extend their reach, integrate their community of employees, business partners and customers and to reduce costs by using inexpensive public networks. Inside and outside the enterprise, business is moving online, which means there's an important need to establish secure communications and practices in both extranet and intranet applications. Every enterprise network needs protection of confidentiality of data, integrity of data and secure access to data for appropriate users. There are, of course, many different aspects of security in enterprise networks, and our "Top 10" recommendations represent just a few best practices in the areas of physical security, data security and network security.

GeoTrust Solutions for Enterprise Security
GeoTrust is committed to aggressively developing solutions that are progressive and innovative to help you secure your enterprise systems and maintain secure e-commerce transactions, trusted identities and fully managed trusted e-business environments. GeoTrust offers a comprehensive array of enterprise security solutions to secure online identities for people, devices and applications, including:

Enterprise SSL.™ Enterprise SSL is an ideal solution for any enterprise that needs to deploy and manage five or more SSL certificates. It includes powerful 1024-bit signed certificates and a centralized, web-based administrative portal for complete control over certificate lifecycle management.

Client Certificates. True Credentials® is a fully-managed, web-based client certificate service that safeguards communication and data exchange between your enterprise and your employees, vendors, business partners and customers. It provides secure network access to credentialed users, enables secure messaging and S/MIME and supports digital signature applications.

Subordinate Certificate Authority. GeoRoot™ is a root signing service that allows global recognition of self-signed certificates by being chained to GeoTrust's trusted root. This solution is ideal for those organizations that recognize the requirements and responsibilities involved in establishing their own Certificate Authority and have significant in-house PKI expertise.

Identity Verification Services. True Identity® is an ideal solution for any enterprise where identity validation is critical to conducting business online, including financial services, insurance companies, banks, mortgage companies, online brokerages and e-commerce sites with high-volume, high-value transactions. True Identity leverages GeoTrust's unique partnership with Equifax to compare user provided information against three powerful verification databases to provide back a level of "identity certainty." The entire verification process can be completed online in minutes.

Certified Document Services for Adobe® Acrobat®. Certified Document Services (CDS) for Adobe Acrobat allows authors to create Adobe Portable Document Format (PDF) files that clearly certify to recipients that the author's identity has been verified by a trusted organization and that the document has not been altered. CDS for Adobe Acrobat provides a centralized, web-based management system for issuing digital certificates and is ideal for organizations that need either desktop-based or server-based certified document services.

SSL Security for Mobile Environments. The Power Server ID™ SSL certificate provides the highest level of browser compatibility and web security for mobile and networked environments. An ideal solution for hosting companies and enterprises with a global e-business base, Power Server ID ensures that any customer can connect from any device, anywhere, anytime.

Code Signing Certificates. Code Signing certificates are available for developers to ensure that code that is passed to platforms, particularly wireless platforms, is not tampered with in any way. Code Signing certificates assure developers of the code integrity, protects handheld users from viruses and enables enterprises to roll out secure applications faster.

TrustWatch® web site verification service. TrustWatch (www.trustwatch.com) is a free toolbar and search site that helps consumers recognize whether a site has been verified and is safe for the exchange of confidential information.

ABOUT GEOTRUST, INC.

GeoTrust is a leader in identity verification and trust services for e-business. Its products include web security services for secure e-commerce transactions, identity verification, managed security services and TrustWatch (www.trustwatch.com), a free toolbar and search site that helps consumers recognize whether a site has been verified and is safe for the exchange of confidential information. With more than 70,000 companies in over 140 countries using its technology for online security, GeoTrust has rapidly become the second largest digital certificate provider in the world.

GeoTrust®

117 Kendrick Street
Suite 350
Needham, MA 02494
Toll Free: (800) 944-0492
Phone: (781) 292-4100
Fax: (781) 444-3961
E-mail: info@geotrust.com
www.geotrust.com