Internet Security Overview 101

Kathleen Bies

Follow this and additional works at: http://commons.pacificu.edu/inter02

Recommended Citation

This Article is brought to you for free and open access by the Interface: The Journal of Education, Community and Values at CommonKnowledge. It has been accepted for inclusion in Volume 2 (2002) by an authorized administrator of CommonKnowledge. For more information, please contact CommonKnowledge@pacificu.edu.
Internet Security Overview 101

Rights
Terms of use for work posted in CommonKnowledge.
Internet Security Overview 101

Posted on March 1, 2002 by Editor

By Kathleen Bies <KBEIS@mn.rr.com>
Associate Editor, Interface

Security issues as related to the Internet are significant. Which issues you need to address are based on how you plan to use the Internet. Are you using the Internet for e-mail and nothing else? Are you using the Internet to launch your company’s web presence and provide opportunities for on-line shopping? Or, do you want to use Virtual private networks (VPNs) to provide secure communications for your extranet?

Depending on how you use the Internet, you can use:

- **A Firewall**: Provides a fully functional firewall to serve as a logical barrier between your internal network and an external network, such as the Internet. The firewall runs on a separate processor.
- **Virtual private networking (VPN)**: A virtual private network (VPN) is an extension of an enterprise’s private Intranet across a public network, such as the Internet. You can use a VPN to create a secure private connection, essentially by creating a private “tunnel” over a public network.
- **IP packet security**: An integrated feature of OS/400, IP packet security provides basic firewall separation and protection for your system. IP packet security allows you to create packet filter and network address translation (NAT) rules to control TCP/IP traffic in your network.
- **Digital Certificates**: Certificates allow you to create, manage, and apply digital certificates to your applications so that you can use SSL for secure communications and stronger authentication.

**Internet security defined**

What do we mean by “security”? Internet system security has these basic components:

- **A security policy**: Defines what you want to protect and what you expect of your system
users. It provides a basis for security planning when you design new applications or expand your current network. It describes user responsibilities, such as protecting confidential information and creating nontrivial passwords. You need to create and enact a security policy for your organization that minimizes the risks to your internal network. The inherent security features of your software or hardware, when properly configured, provide you with the ability to minimize many risks. When you connect your system to the Internet; however, you will need to provide additional security measures to ensure the safety of your internal network.

- **User authentication:** Ensures that only authorized individuals (or jobs) can enter your system. When you link your system to a public network like the Internet, user authentication takes on new dimensions. An important difference between the Internet and your Intranet is your ability to trust the identity of a user who signs on. Consequently, you should consider seriously the idea of using stronger authentication methods than traditional user name and password logon procedures provide. Digital certificates provide a stronger alternative while providing other security benefits as well.

- **Resource protection:** Ensures that only authorized users can access objects on the system. The ability to secure all types of system resources is a system’s strength. You should carefully define the different categories of users that can access your system. Also, you should define what access you want to give these groups of users as part of creating your security policy.

Some Internet services are more vulnerable to certain types of attacks than others. Therefore, it is critical that you understand the risks that are imposed by each service you intend to use or provide. In addition, understanding possible security risks helps you to determine a clear set of security objectives. Once you understand the risks, you must ensure that your security policy provides a means of minimizing those risks.

**About your security policy**

Each Internet service that you use or provide poses risks to your system and the network to which it is connected. A security policy is a set of rules that apply to activities for the computer and communications resources that belong to an organization. These rules cover areas such as physical security, personnel security, administrative security, and network security.

To develop your security policy, you must clearly define your security objectives. Once you create a security policy, you must take steps to put into effect the rules it contains. These steps include training employees and adding necessary software and hardware to enforce the rules. Also, when you make changes in your computing environment, you should update your security policy to ensure that you address any new risks that your changes impose.

**About your security objectives**

When you create and carry out a security policy, you must have clear objectives. Security
objectives fall into one or more of the following categories:

- **Authentication**: Assurance or verification that the resource (human or machine) at the other end of the session really is what it claims to be. Authentication proves that a resource or user is what or who it claims to be. Solid authentication defends a system against the security risk of impersonation, in which a sender or receiver uses a false identity to access a system. Traditionally, systems have used passwords and user names for authentication; digital certificates can provide a more secure method of authentication. Authenticated users may have different types of permissions based on their authorization levels.

- **Authorization**: Assurance that the person or computer at the other end of the session has permission to carry out the request. Authorization is the process of determining who or what can access system resources or perform certain activities on a system. Usually, authorization is performed in the context of authentication. Authenticated users may have different types of permissions based on their authorization levels. Consequently, the user’s authorizations on a system are determined when the user presents the certificate to the server for authentication.

- **Integrity**: Assurance that arriving information is the same as that sent. Understanding integrity requires you to understand the concepts of data integrity and system integrity.

- **Data integrity**: means that data is protected from unauthorized changes or tampering. Data integrity defends against the security risk of manipulation, in which someone intercepts and changes information to which he or she is not authorized. In addition to protecting data stored within your network, you may need additional security to ensure data integrity when data enters your system from untrusted sources. When data that enters your system comes from a public network, you may need security methods so that you can:
  - Protect the data from being “sniffed” and interpreted, usually by encrypting it.
  - Ensure that the transmission has not been altered (data integrity).
  - Prove that a transmission occurred (non-repudiation). In the future, you might need the electronic equivalent of registered or certified mail.

- **System integrity**: System integrity is your system’s ability to provide consistent, expected results with expected performance. System integrity is the most commonly overlooked component of security because system integrity is a fundamental part of most architecture. For example, some systems make it extremely difficult for a mischief-maker to imitate or modify an operating system program when you use higher security levels. When you think about connecting to the Internet, you need to think about your system’s availability and how a hacker might try to assault it. A hacker can launch a DDoS attack without ever signing on to your system. A hacker can, for example, compromise your system’s ability to service user requests by flooding your system. Your disk storage can be flooded, for example, with unwanted mail or with printed output. Processing unauthorized requests can overwhelm your processor, for example, by error recovery or simply. Your legitimate users either cannot log on or they receive poor performance because your system is spending resources dealing with unauthorized requests.
• **Non-repudiation:** Assurance (accountability) that any transaction that takes place can subsequently be proven to have taken place. Both the sender and the receiver agree that the exchange took place. Non-repudiation is proof that a transaction occurred, or that you sent or received a message. The use of digital certificates and public key cryptography to “sign” transactions, messages, and documents supports non-repudiation.

• **Confidentiality:** Assurance that sensitive information remains private and is not visible to an eavesdropper. Confidentiality means keeping information protected from unauthorized viewers. Confidentiality is critical to total data security. Encrypting data by using digital certificates and the secure socket layer (SSL) helps ensure confidentiality when transmitting data across untrusted networks. Your security policy should address how you will provide confidentiality for information within your network as well as providing it when information leaves your network.

• **Security auditing:** Monitoring security-relevant events to provide a log of both successful and unsuccessful (denied) access. Successful access records tell you who is doing what on your systems. Unsuccessful (denied) access records tell you either that someone is attempting to break your security or that someone is having difficulty accessing your system.

Understanding your security objectives helps you create a security policy that covers all your system and network security needs. Next, you should understand what is involved in setting your system security for Internet readiness.

*This is the first of a series of articles I have developed. The information contained is a condensed version of a complete book I co-wrote for IBM and placed on their AS/400 Information web site. These articles are not system specific, rather point out basic security information a business owner should know and be aware of if they operate a network or are moving activities to the Internet.*

This entry was posted in Uncategorized by Editor. Bookmark the permalink [http://bcis.pacificu.edu/interface/?p=2373].

5 THOUGHTS ON “INTERNET SECURITY OVERVIEW 101”

Marylin Kroll
on January 30, 2014 at 6:15 PM said:

Helpful information. Lucky me I discovered your site by chance, and I am stunned why this coincidence did not took place in advance! I bookmarked it.
dashboard camera reviews  on January 31, 2014 at 3:25 PM said:

Howdy! I’m at work browsing your blog from my new apple iphone!
Just wanted to say I love reading through your blog and look forward to all your posts!
Keep up the excellent work!

africa  on February 4, 2014 at 10:19 AM said:

Hi! That is my 1st comment right here so I just wanted to give a quick shout out and tell you I truly appreciate reading your articles. Can you suggest any other blogs/websites/forums that go more than the exact same subjects? Enjoy it!

nigeria entertainment news  on February 4, 2014 at 10:30 AM said:

Hey, thank you for the feedback! I would suggest that saying “God died over a cross” is not specific sufficient theological terminology to accurately describe what happened there. Vague terminology like that will cause deviant considering on the trinity. Of course I do not think it’s the cardinal sin to use vague phrases, but I think it can reveal our confusion when it comes to the trinity.

nigeria entertainment news  on February 4, 2014 at 10:40 AM said:

I and also my buddies came looking at the great tips located on a site and just before long I had a terrible feeling I in no way thanked the internet web site owner for people tips. All the men and women are really warmed to learn them and have now really been creating probably the most of these things. Many thanks for genuinely getting extremely type as well as for figuring out specific extremely beneficial themes most individuals are incredibly needing being aware of. My trustworthy apologies for not expressing appreciation to earlier.