Net Admin Weekly

59,000 Subscribers Worldwide

September 18, 2002
Issue #9

CramSession StudyGuides InfoCenter Discussions SkillDrill Newsletters

CramSession

Feature

Q & A

Security Advisories

News Headlines & Resources

Download of the Week

PrepLogic
Pass the First Time.
Prepare for your MCSE, MCSA, and A+.
...And pass. Guaranteed!
Practice Tests Practice Tests Practice
Click Here

Feature

Building a Public Key Infrastructure

to top

One of the most popular security buzzwords (or more accurately, buzz acronyms) these days is PKI. Every organization is scrambling to get one, even if management isn't exactly sure what one is. What is a PKI? Does every network need one? And if yours does, how do you go about building one? In this week's feature article, we'll address these questions, and more.

The PKI is based on (who would have guessed?) public key cryptography.

Encryption is the process of "scrambling" data to make it unreadable to anyone who doesn't have the key to decrypt it. A key is a variable used in conjunction with an encryption algorithm (a formula or calculation). You probably already know that encryption comes in two flavors: symmetric (also called secret key encryption) and asymmetric (public key encryption). Secret key encryption uses the same key to encrypt and decrypt data, while public key encryption uses a pair of mathematically related keys, a private key and a public key. One is used to encrypt and the other to decrypt. This eliminates the need to share a single key (with the risk of compromise that entails).

Public key encryption depends on the public key being made available freely to everyone, and the private key being kept absolutely secret from everyone except the owner of the key pair. To send data confidentially, the sender obtains the public key of the intended recipient and encrypts the data with it. Only the private key that is associated with that public key can decrypt the data, so it can only be read by the holder of that key pair.

The keys can be used in the opposite way to provide authentication of the identity of the sender of a message. In this case, the sender uses his/her own private key to encrypt the message. Now anyone can decrypt and read it, because the associated public key is available to everyone–-but they can be assured that if the sender's public key will decrypt it, only the sender could have sent it, because only the sender has the private key that encrypted it.

Sounds great. So what's the problem?

Public key encryption is more secure than secret key encryption because there is no need to ever share the private key with anyone. However, with this system you need a way to ensure that a public key really belongs to the person to whom it is purported to belong. Otherwise an unscrupulous person could publish a public key and say it belongs to someone else, then intercept messages sent to that other person and decrypt them with the associated private key.

To overcome this problem, we have to introduce the concept of a trusted third party. In the world outside computers, we rely on this type of system to verify identities all the time. If you want to give a check to a merchant, the merchant will probably require that you show a driver's license, state ID card, or other “official” document to prove that you're really the person to whom the bank account on which the check is drawn belongs. This document is issued by a third party--usually the government. The merchant trusts that the third party verified your identity before issuing you the license or card.

In the computer world, the document that you present to prove your identity is called a digital certificate. The certificate is a guarantee that a particular public key really belongs to the user who claims it. It contains the public key itself along with information about the user, the purpose for which the certificate can be used, and the expiration date. The certificate is signed by the trusted third party that issued it.

The trusted third party that issues certificates is called a certification authority (CA). Just as ID cards can be issued by public (government) entities or within an organization (employee ID cards), certification authorities can be public entities, which provide certificates across the Internet, or private entities set up within an organization to issue certificates only on an internal network.

So what does all this have to do with the PKI?

The public key infrastructure refers to the components-–keys, certificates, certification authorities-–that make up a system for securely requesting, issuing, managing, and revoking digital certificates. A CA is a computer, on which the certificate services software has been installed, which is used to perform these tasks.

An organization can have one CA or several, and CAs can operate in a hierarchical structure, so that there is a root CA at the top of the hierarchy that is implicitly trusted and issues a certificate to itself. Under it are subordinate CAs that issue certificates to users. Their own certificates are issued by the root CA.

A CA keeps a database of certificates it issues, and another important duty it has is to maintain and make available to users a list of all certificates that have been revoked. For example, if the private key associated with a certificate is compromised, that certificate will be revoked. The CA publishes a Certificate Revocation List (CRL) so other users will know that these revoked certificates are invalid and therefore not to rely on them.

How do I set up a PKI on my network?

If you're running Windows 2000 or .NET Server (the latter has not yet been released), building a PKI is relatively easy. The operating system includes the Certificate Services component, which can be installed on a Windows Server computer to make it a certification authority (the CA can also perform other server functions). It is not installed by default, but can be selected from the optional Windows components during installation.

CAs can be set up as Enterprise CAs (in a Windows 2000/.NET domain) or standalone CAs (which do not require Active Directory and do not have to be domain members-–although they can be). Either type (enterprise or standalone) can be installed as a root or subordinate CA. Microsoft recommends that Certificate Services always be installed on an NTFS partition.

If Active Directory is present on the network, it is used for storing and publishing certificates and CRLs. Once a CA is set up, users can request certificates from it using one of two methods:

- The certificate Services web page: When a server is operating as a CA, by default it hosts a web page at http://servername/certsrv. Users can use a web browser (MSIE 4.0 or above or Netscape 3.01 or above) to request certificates or check the status of pending certificates.
- The Certificates MMC snap-in: if the CA is an Enterprise CA, users can use the Certificates snap-in added to a custom management console to request, view, and manage their certificates (the user must have the proper permissions to do so).

Certificates can also be exported to a different location to create a backup or to move a user's certificate to another computer (for example, if the user gets a new workstation). An Export Wizard guides you through the process. To restore a certificate that has been exported to a file, you can use the Import Wizard.

Summary

A public key infrastructure provides a secure way to handle digital certificates, which are used to verify the identities of users, computers, and other entities. In a medium or large organization, it may be impossible to ensure that all users are who they claim to be without a formal system in place. For more information about public key infrastructures, see the many excellent resources available on the web. You'll find many links at the **PKI Page web site**.

This week's feature article by
Deb Shinder
Net Admin Weekly Author

Q & A

Internet Explorer Bug or Network Design Problems?

to top

Question:

Hey Dr. Tom,
I want to report a very annoying bug of Internet Explorer 6 that I and most of my friends with Windows XP have and doesn't seem to have a logical explanation. In many sites IE6 freezes for about 30 seconds, becomes unresponsive, like it is doing something else, and after that 30 second period comes back like nothing happened. I believe that this is a very serious bug because i see about 60% of users affected and no official response by MS. I run Windows XP SP1 and IE6 with the latest cumulative patch plus IE6 SP1 and the bug's still there! I really would

like to hear your opinion on this. Thank you in advance. --DisMan

Answer:

Hey DisMan, you've got some problems over there. I haven't heard of this problem with IE, and I've had the pleasure of running thousands of desktops with Windows XP and IE 6.0 without any problems like those you describe. I would look at a couple of things first. Are you using an authenticating Web Proxy server? That can cause similar problems like what you're having. How's your name resolution infrastructure put together? Are the clients resolving names, or do you have a Web Proxy performing DNS proxy for your clients? Problems with name resolution can cause long delays and failed Web pages. Does this issue affect just certain sites, or are all sites equally affected? It could be that some sites having coding issues and this causes IE to lock up. Check out your network infrastructure and the sites, and if you still have a problem, start running it up the Microsoft flagpole.

Active Directory and DNS Subdomains

to top

Question:

Hey Dr. Tom,
Can I create a DNS subdomain even though I don't have a AD child domain? For example, can I be host.subdomain.domain.com in DNS, but just be a member of the domain.com AD domain? Am I totally confused???? --labattsblue

Answer:

Dear labattsblue,
Sometimes I wish Microsoft continued with a flat name space for their Active Directory domains. That would have made life easier on everybody. The fact is you can name your machine whatever you like, but I have to ask what you would want to do such a thing? If your machine belongs to the domain.com and has the hostname host.domain.com, why would you want to create a subdomain and give yourself the hostname host.subdomain.domain.com? You can create the subdomain and put in a Host (A) entry for your computer, and it would then resolve to host.subdomain.domain.com. But you should make sure that your machine's primary DNS appendix belongs to the domain that it belongs to, or else you may run into authentication issues.

Security Advisories

New Slapper Worm Moving through the Internet

to top

This worm has affected 6700+ Apache servers in the last few days. This exploit opens a shell on a client machine and uses this to upload the exploit code to other victims. Its peer-to-peer capabilities allow it to participate in a coordinated DDoS attacks. The code listens on UDP port 2002. For more information, check out the link to the Symantec Antivirus Center.

Read more...

Unchecked Buffer in Network Share Provider Can Lead to Denial of Service

to top

There is a weakness in the Windows SMB protocol that a hacker, by sending a specially crafted request, can mount a denial of service attack on a target server machine and crash the system. The attacker could use both a user account and anonymous access to a ccomplish this. Though not confirmed, it may be possible to execute arbitrary code on the victim server.

Read more...

Security Issue with NetInfo Manager Opens Up Mac OS X 10.2 to Attack

to top

There is a severe security issue with Mac OS X 10.2 that allows any user to move through the file system and change or delete any file he wishes. The problem is with the NetInfo Manager, which is run as Root. A malicious user could compromise a server based on this application's default access privileges.

Read more...

News Headlines and Resources

CISSP Study Guide now at Cramsession

to top

Are you getting ready for your CISSP exam? If so, you need to study up, because the exam is definitely not a no-brainer! One of the best things you can do is check out the Cramsession CISSP Study Guide. What's really cool is that they have a version with no ad's and no pop ups!

Check it out here.

Office Subscription Trial Dumped

to top

Microsoft consumers get a short reprieve. We were expecting Office 2002 (10.0) to be the last version of Office anyone would ever use, but it look like Office 11.0 might have a chance. That's right! No self-imploding subscription based software for the next Office. This is good news, but we'll wait and see how long it lasts.

Read more...

Protect Your Wireless Networks from Drive-by Spammers

to top

I thought I had my bases covered. I don't allow my SMTP relays to relay mail except to my own mail domains. I don't allow the Exchange SMTP Service to accept mail for relay unless they're from one of my network IDs. What I didn't think about was the drive-by spammers! Watch those WLANs, you could end up sending spam for the local scumbag.

Read more...

The Darker Side of Spam Whacking

to top

Have you noticed you're getting less email these days? Have you noticed that you're not getting your newsletters like you used to? Might be spam filtering software choking off your connection to the outside world. Spam whacking is a good thing–-RBLs can be bad! Not all of them, but you need to avoid any RBL that depends on user reports. Also make sure to read the second link, as the article beats down one of the sleaziest spam whackers out there-- SpamCop.

Read more...
Read more...

Windows XP Media Center: Who Needs It?

to top

Wouldn't it be great to have a computer that allows you to listen to music, view your photos and camcorder movies, and even record your favorite television shows? What? You also have a Sony Vaio? OK-–you'll be able to do the same things (almost) with the upcoming Windows XP Media Center! Well, almost. Your personal video recorder TV and movie recordings will be copy protected. Can you say "Windows XP Media Center = Microsoft Bob?"

Read more...

Uplddrvinfo.htm Contains JScript Code That Might Permit a Malicious User to Delete Files

to top

There's a real bad security flaw in the Windows XP Help Center that you must fix. If you install Windows XP Service Pack 1 you'll get the fix. But if you want to bypass Windows XP Service Pack 1 and still patch this baddie, you can get a tool from Steve Gibson to do this for you.

Microsoft KB article on the problem
Steve Gibson's fix

Windows XP Service Pack 1 Clearing House

to top

What flavor of Windows XP Server Pack 1 would you like? Express? Network Install? Slipstreamed? Would you like an order of hotfixes with that? Check out the answers to these questions and more at the Microsoft Windows XP Service Pack 1 Clearing House.

Read more...

Download of the Week

Microsoft Web Application Stress Tool

to top

Are your Web servers up to snuff? Have you rolled out a new Web, let the word out, and then seen it crumble under the weight of the traffic? If so, then you failed to perform proper stress testing! Web server stress testing isn't something you can do by calling ten friends and telling them to visit your server. You need a tool that automates the process. If you're running an IIS 5 site, you're in luck! Microsoft has the Web

Application Stress tool that you can download for free and it'll do the heavy lifting for you. Download it and get the basic configuration docs here.

Read more...

Free Cramsession IT Newsletters - **Choose Your Topics!**

H = HTML Format **T** = Text Format

H	T		H	T		H	T	
□	□	A+ Weekly	•	□	Exam Tips 'N Tricks	□	•	.NET Insider
□	•	ByteBack!	□	•	IT Career Tips	•	□	Script Shots
□	□	Cisco Insider	•	□	Linux News	□	□	Security Insider
□	□	Developers Digest	□	•	Must Know News	•	□	Trainers News

Enter your Email

Subscribe Now!

CramSession
Prepare for Success!

Your subscribed e-mail address is:steven.thode@toadworld.net
To unsubscribe, simply **click here** and hit "send" in your e-mail reader.