



MOOSE VIEWS

What's
Inside

**We've Finished
our Move:
See Back Page
for our new
Mailing
Address**

**The Citrix
Corner—The
Citrix Secure
Gateway**

Story on Page 2...

**Warning!
Be careful of
what you say
in an Instant
Message!**

Story on Page 3...

Moose Views

is a monthly newsletter prepared by Moose Logic to bring you information and tips on maintaining a trouble free network.

Vol. 2, Issue 1

January, 2007

View past issues at:

www.mooselogic.com/news

Top Mistakes That Make You A Prime Target For Identity Theft

The numbers are staggering: according to the 2006 Identity Fraud Report, identity theft cost consumers *and* businesses a whopping \$56.6 billion dollars. Identity theft occurs when someone steals your name, Social Security number (SSN), bank account number, or credit card to open accounts, make purchases, or commit other fraudulent crimes.

The Methods They Use To Steal Your Identity

The methods identity thieves use range from low tech strategies (like going through your trash can, also known as “dumpster diving”) to highly sophisticated phishing scams that include cloned PayPal or bank websites that trick you into giving your username, password, or account number. Other ways include:

- ♦ Stealing records from an employer or bribing an employee who has access to the records.
- ♦ Hacking into the company’s employee records.
- ♦ Stealing mail, such as bank account or credit card statements, tax documents, pre-approved credit cards, or new checks.
- ♦ Abusing their employer's authorized access to credit reports.
- ♦ Stealing laptop computers that contain confidential information (one reason for the “BitLocker” drive encryption feature in Windows Vista).

How Identity Theft Affects You

Once someone has stolen your identity, they can use your credit cards or bank account to purchase expensive consumer goods like computers and electronics that can easily be resold for cash. They can also open and charge up new credit cards, which can be a real mess to straighten out with vendors and credit reporting agencies. Other criminal activities include taking out auto loans in your name, opening a new phone or wireless service in your name, or writing counterfeit checks to drain your bank account. Some have even used it to file for bankruptcy to avoid paying debts they've incurred, or to avoid eviction.



How To Protect Yourself and Your Employees

Never give your personal information, Social Security number, credit card number, or bank account numbers over the phone or online unless you know for certain you are dealing with a legitimate company. Make sure your employees are given an AUP (acceptable use policy) that educates them on the dangers of phishing scams and spam e-mails designed to either trick you into revealing your information or install a virus that secretly

Continued on back page...

The Citrix Corner—The Citrix Secure Gateway

When you purchase Citrix Presentation Server, you also get the rights to deploy the Citrix Web Interface (“WI”) and the Citrix Secure Gateway (“CSG”). Although, in many cases, the Citrix Access Gateway appliance is a better and more flexible way to provide your users with secure access over the Internet, it’s important to understand the differences in functionality between the CSG and the Access Gateway appliance. In this issue of The Citrix Corner, we’ll talk about the CSG. Next month, we’ll talk about the Access Gateway appliance.

Ever since the days of WinFrame (the NT v3.51 version of the product that evolved into the Citrix Presentation Server), we’ve had the ability to do what was then called “Application Launching and Embedding.” Briefly, what that meant was that I could construct a Web page, and on that page I could create a hyperlink to a text file with a .ICA extension. In that .ICA file, I could put information about the name and IP address of a target Citrix server, the application I wanted to launch, and even the credentials I wanted to use to log on and launch the application. When someone clicked the hyperlink, the underlying Windows file associations called the Citrix client software to read the contents of the .ICA file. The Citrix client software would then dutifully do whatever the .ICA file said to do, i.e., contact the target server and launch the desired application.

There were, however, some big problems with this approach, and some of you may have already spotted them. First, the links were *static*. If I wanted Fred and Mary to see different sets of application links, I would have to construct a unique Web page for each of them. Second, there was no way of preventing someone from right-clicking on the hyperlink, choosing “Save Target As,” saving the .ICA file to a local drive, then opening it with a text editor and reading the contents—which included information that you probably don’t want floating around the Internet, like server names and IP addresses, that could be used later to launch an attack on the network. Moreover, if you wanted users to connect from the public Internet (as opposed to the corporate Intranet), you had to configure your firewall to allow ICA traffic (port 1494 by default) from the Internet into your protected network – an obvious security risk. Finally, if the *client* PC was on the far side of a firewall or router that blocked port 1494, the Citrix client software would never be able to reach the target server to launch the application.

The first problem was addressed by the Web Interface technology, which some of you old-timers will recall was

developed as “Project Charlotte” (as in *Charlotte’s Web*—get it?) and introduced to the market under the “Nfuse” name. This technology placed enough intelligence on the Web Interface server that it could (1) consume your login credentials, (2) communicate with AD to validate those credentials, (3) communicate with the Citrix server farm to determine what published applications you had the rights to run, and (4) dynamically build and present you with a Web page containing only the icons corresponding to the applications you had the rights to run. Then, when you actually clicked on an application icon, the WI server would have another dialog with the Citrix farm to determine which server was the “least busy” according to the load-balancing rules for that application, and then dynamically build and send to the client a file called “LAUNCH.ICA” that contained the information the Citrix client software needed to contact that server and launch the application. This was some very cool technology, but it didn’t solve the security issues.

The security issues were finally addressed by the introduction of the CSG, in combination with a secure ticketing process. The CSG software typically runs on a Windows/IIS server in the DMZ. (For anyone not familiar with the term, most firewalls support the creation of a DMZ, which gets its name from the military concept of a “Demilitarized Zone,” and which is a network segment that is isolated from both the public Internet and from the protected network. The firewall then allows you to implement a different set of access rules for traffic between the Internet and the DMZ vs. traffic between the DMZ and the protected network.)

The CSG has two primary functions. First, it serves as an *ICA-specific* SSL/VPN. By that, I mean that the CSG server acts as a *proxy* to pass the ICA traffic back and forth between the public Internet and the protected network, and that all communication between the Citrix client software and the CSG server, including the initial submission of login credentials, is encrypted via SSL. Second, the CSG server is an integral part of the secure ticketing process that eliminates the need to imbed sensitive information in the LAUNCH.ICA file.

The details of the secure ticketing process are beyond the scope of this article, but in broad terms, it works like this: somewhere in the protected network, you have one or more servers running the Secure Ticketing Authority service. When you (the client) click on an application icon in your browser window, and the determination is made of which Presentation Server to direct you to, an encrypted ticket is requested from the STA that specifically authorizes *you* to

run *that application on that specific server*, and which has a specific *time-to-live* built into it. That encrypted ticket gets incorporated in the LAUNCH.ICA file that is sent to the client instead of sending explicit information about server names and IP addresses. Now, if the LAUNCH.ICA file is saved and opened with a text editor, all you will see is a bunch of gibberish. Moreover, if you don't successfully launch the specified application on the specified server within the specified time-to-live interval, the ticket expires and is no good anyway!

The client-side firewall concerns tend to go away simply because we're using SSL between the client and the CSG server. Because SSL is such a widely-used standard for securing Web content (chances are you use it every time you do online banking or shop for something on the Internet), the standard SSL port (443) is almost never blocked.

So it's all good, right? Why wouldn't everybody want to deploy this technology? Well, thousands of organizations have. However, remember that the CSG is only going to support ICA traffic between Citrix clients and Citrix Presentation Servers – it won't give you VPN access to any other kinds of resources on the protected network. You can't synchronize Outlook through it, or get to file shares, or access other kinds of Web applications that may be running in the protected network.

Also, it's not totally without cost: even though you don't have to pay for the CSG software, you still have to have a piece of server hardware to run it on, and a Windows server license on that piece of server hardware.

Finally, I'm very much aware that there are organizations that are philosophically opposed to having a Windows server in the DMZ under any circumstances, and it's my experience that you're better off talking religion and politics than trying to change someone's mind on that issue!

So stay tuned for the next issue of The Citrix Corner, when we will discuss the Citrix Access Gateway—a hardened Linux-based appliance that does everything the CSG can do and more besides.

Be Careful Of What You Say In An Instant Message

If you think your words disappear forever when an instant messaging session is closed, think again.

Your IM is not a safe refuge for private chatter. Companies and government agencies can monitor and log instant-messaging conversations conducted on company computers. Google saves chat sessions automatically and they can be searched later. Users of Google Talk must disable the setting or choose "off the record" for sessions they don't want saved.

Instant-messaging services such as AOL's AIM, Yahoo's Yahoo Messenger, and Microsoft's Windows Live Messenger don't store conversations on their servers automatically, but they offer various tools for companies and individuals to log conversations.

Recent scandals demonstrate that instant messaging is not private. Government-monitored IMs found inappropriate messages by a member of Congress, who then resigned. And IMs have figured in



corporate scandals, as well. Instant-messaging services are offering a host of new products and tools for tracking IMs. AIM Pro, a free version for individuals and businesses, automatically archives conversations and saves them for 14 days. The feature can be extended or turned off.

Microsoft's Live Communications server, allows a company's information technology department to log and search employee conversations, including those on IM services like Yahoo and AOL.

A study by the American Management Association and The ePolicy Institute shows that only 13 percent of companies now track and log instant messages. The crackdown, however, is starting to take effect. Two percent of employers have fired someone because of what they said, and about 26 percent of companies have fired someone for misuse of email. And some companies who are subject to regulations that govern the retention and archiving of email messages are finding that those same regulations may apply to instant messages!

Courts have repeatedly held that employees do *not* have a reasonable expectation of privacy when they are using the employer's computers, software, and bandwidth to communicate. However, your organization should have a *written* "Acceptable Use Policy" that is given to all employees, and which reinforces the point that any email or IM communications that take place using company resources are the property of the company and are subject to inspection...and all employees should be required to sign an acknowledgement stating that they have received, have read, and understand the Acceptable Use Policy.

If you don't have an Acceptable Use Policy, we'd be glad to help you write one. (But you already guessed that, didn't you?)



MOOSE LOGIC

1415 Western Ave.

Suite 488

Seattle, WA 98101

Phone: (206) 774-0619

Email: info@mooselogic.com

www.mooselogic.com

Moose Views © 2007 by Moose Logic, all rights reserved

Services We Offer:

- MooseGuard™ Support Services
- General Network Repair and Troubleshooting
- Network Design & Implementation
- Disaster Recovery
- Virus Protection & Removal
- Network Security
- E-mail & Internet Solutions
- Wireless Networking
- Access Infrastructure Solutions
- Spam Filtering
- Storage Solutions
- Voice over IP Phone Systems

Microsoft
CERTIFIED
Partner

Networking Infrastructure Solutions



GOLD
Solution Advisor



Top Mistakes That Make You A Prime Target, Continued from page 1

steals the information stored on your PC.

You can recognize a secure website, as it has an <https://> at the beginning of the web address (regular web sites only have <http://> and no "s") at the top of the page on which you are submitting your information. It also must have a picture of a lock in the bottom right corner of the page. (If you're running IE 7, the lock is at the top of the page, next to the refresh button.) If you don't see both of these measures in place, do not submit your information.

And even if you DO see this, use a credit card instead of a debit card or pay-by-check option because you'll get security protection from your card's issuer. Visa, MasterCard and American Express all have a zero liability policy. If you notify the bank of unauthorized transactions, you pay little or nothing. And some credit card companies offer one-time use numbers to prevent someone from stealing your account number and using it for unauthorized charges.

Shred all medical bills, financial statements, credit card applications, tax statements, or any other mail that contains confidential information about you before you throw them into the trash. Most shredders these days will even shred an old credit card.

Never open e-mails or attachments from e-mail addresses you are unfamiliar with, and NEVER respond to e-mails that ask you to verify your account information because your account is being closed, suspended, or charged. If you want to verify this, call the bank or

the company to see if it was a legitimate e-mail.

Signs That You've Fallen Victim To Identity Theft

If you see any unexplained charges or withdrawals from your bank accounts, if you receive credit cards that you did not apply for, or if you start receiving bills or collection letters for items you have not purchased, someone may have stolen your identity.

Always follow up with the business or institution to find out exactly what is causing the situation as quickly as possible. The faster you act on identity theft, the easier it will be for you to clear your name.



"Book 'em, Pete, they're being charged as accessories."