Global Information Assurance Certification Paper

Thomas D. Reece

Citrix ICA Perimeter Security Issues

One of the popular buzzwords over the last few years has been thin client computing. For a Windows environment, this usually means Citrix Winframe or MetaFrame. Citrix Winframe is a licensed version of NT Server 3.51, with changes made by Citrix to NT to allow multiple user sessions. It is a single product, and does not require any software from Microsoft. MetaFrame is an add-on product from Citrix to Microsoft's Windows NT 4 Terminal Server Edition. These are separate products, with the MetaFrame product providing additional functionality to Terminal Server. Both Winframe and Terminal Server with MetaFrame use special components developed by Citrix to allow multiple user sessions to a Windows server, and a proprietary protocol known as ICA for transmitting information. ICA can run over TCP/IP across the Internet, with definite security implications for perimeter defenses.

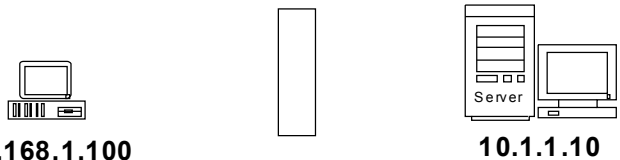
This discussion will focus on perimeter security issues with using the ICA protocol. There are certainly other steps that should be taken to secure a server running Winframe or Terminal Services and MetaFrame, with more information available at www.citrix.com and www.microsoft.com/ntserver/terminalserver. I will assume that those steps have been or will be taken. Additionally, the common precautions for NT Server, such as removing all unnecessary services, should also be taken.

Establishing an ICA Session

The ICA protocol was developed by Citrix and optimized for transferring information to and from Citrix servers from Citrix clients. The information transferred is related to the user interface, including screen images and user input. The actual data and applications are running on the server rather than the client, and therefore are not transferred. This provides a minimal level of inherent security, as the data is not clear text. The session data is encoded by ICA for optimal data throughput, although actual encryption of the session is discussed later. Any sniffed information would have to be decoded into screen information and keyboard input.

It should be noted that in order to use ICA, you must use either a Winframe Server or Terminal Server with the MetaFrame add-on. Terminal Server alone does not use ICA, but Microsoft's RDP protocol. Because of the extra functionality provided from MetaFrame, RDP is not commonly used.

The client always initiates ICA sessions. Under no circumstances will a Citrix server initiate a Citrix session to a client. Clients can be configured to either connect to a specific server's hostname or IP address. Clients can also browse for Citrix servers using Citrix ICA Browsing. Clients can also connect to a Citrix "server farm" for load balancing, which is also based on browsing. To connect to a specific server, the client connects to TCP port 1494 with a request for connection. This port can be changed if necessary, but requires editing the configuration files for all clients and changing the server configuration. ICA uses dynamic port allocation, so the server responds on a random port above 1023. A simplified example of the ICA handshake for the following diagram appears below.



Source IP Address	Destination IP Address	Source Port	Destination Port
192.168.1.100	10.1.1.10	3624	1494
10.1.1.10	192.168.1.100	1494	3624

This table illustrates how the ports are used to establish an ICA session. The client, 192.168.1.100, connects to the server TCP port 1494. The client specifies a random port above 1023 for the server to respond to, in this case TCP port 3624.

For ICA Server Browsing (not to be confused with Microsoft browsing), the client will use UDP port 1604, again with a dynamic response on a port above 1023. If you specify a specific server address in the client configuration, the client does not use UDP to broadcast for a Citrix Master Browser, and those ports can remain closed. With dynamic ports, a proprietary protocol, and potential UDP packets, ICA can definitely pose challenges for your network perimeter defenses.

Firewall Considerations

Configuring a firewall depends on two things. First, are the ICA connections outbound to another network's Citrix server, or inbound to your server? Second, what type of firewall are you running? Each of these questions is significant.

For static packet filtering firewalls, port 1494 must be opened for connections from the client to the server. Then, ports above 1023 must be opened for packets from the server back to the client. So, if the client is on your network, you would need to allow outbound traffic on port 1494, and inbound on ports above 1023. This ideally would be done only for the specific IP addresses of the client(s) and server, if possible. If you are using ICA Browsing, you will need to do a similar configuration for UDP port 1604. This is not a particularly strong solution, but unfortunately it is the best available for static packet filters.

Dynamic packet filters, or Stateful Inspection firewalls, can be configured to allow the connection on port 1494, with rules to allow appropriate users to connect through the firewall. The exact way this is done will be firewall-dependent. This is a significant improvement over static packet filtering, as the entire port range above 1023 does not have to be opened.

Application Proxy firewalls generally must recognize ICA in order to pass it natively. Unfortunately, most proxies do not handle ICA, and therefore cannot natively allow ICA sessions. Recently ICA has been upgraded to include SOCKS support, and therefore SOCKS firewalls can be configured to handle ICA sessions. Note that only the more recent documentation from Citrix describes this. For older clients, you must look for third-party add-ons to support ICA through SOCKS.

NAT Considerations

ICA can work with Network Address Translation (NAT), but requires some additional setup. The problem is that when the client tries to browse the Citrix server, the address returned from the server is the server's internal address. Meanwhile, the client is only aware of what it sees as the server address, which is really the NAT translator. This problem is solved by using the *altaddr /set* command, which assigns an alternate IP address to the server. The address specified by the altaddr command is an external

address. You must also change the client configuration to use the alternate address. Depending on the version, you must edit the Appserve.ini file for the Winframe client or add the address to the Address List option in the MetaFrame client. Additional information is available in the Citrix Solution Knowledgebase, by searching for the article titled "ICA Browsing with Firewall Address Translation (NAT)".

Dial-up ICA

One of the popular features of MetaFrame is its ability to run applications over a dial-up connection. This can be done either through a standard RAS connection and connecting a session as if it were a LAN, or by creating special asynchronous sessions that are MetaFrame-specific, and use ICA instead of RAS. This asynchronous, or async, connection is one of the key advantages to running MetaFrame in addition to Terminal Server. If you choose to use RAS connections, you face the standard RAS threats and vulnerabilities in addition to the potential for an attacker to establish a MetaFrame Session. These connections should be secured in the same way as other RAS connections for your organization. If you use Async connections, the attacker must know that it is a MetaFrame server and either have the Citrix client installed or be able to mimic the client. Async sessions are pure ICA sessions, and TCP/IP and RAS are not involved. Also, other measures, such as restricting access to sessions to specific accounts and call back options can help enhance dial-up security.

SecureICA Services

To further protect sessions, both as they are initiated and as they are used, Citrix provides SecureICA Services as an option for MetaFrame. SecureICA encrypts sessions between Citrix clients and servers using Diffie-Hellman for key agreement. The 1024-bit key is then used to create keys for RSA Security's RC5 algorithm, which is used for actual session data. Encryption can be 40-bit, 56-bit, or 128-bit, except where 40-bit is mandated by Federal export regulations. Encryption levels can be controlled on a per-user or per-connection basis, with client connection attempts not using the minimum encryption levels being rejected. SecureICA can also be used over async connections.

Conclusion

The most secure ICA implementation would include a properly configured dynamic packet-filtering firewall, ICA browsing disabled, and SecureICA services. Configuring the firewall, regardless of type, can be tricky, and for some firewalls, impossible. However, with careful planning, configuration, and testing, using Citrix technology doesn't have to mean an open door for attackers.

References:

"Using Firewalls with Winframe", Citrix Solution Guide. URL: http://www.citrix.com/support/solution/sol00053.htm

Carrol, David. "Published ICA Applications, Minimize the Dangers." Windows 2000 Magazine, February 2000. URL: http://www.win2000mag.com/Articles/Index.cfm?ArticleID=7880

"SecureICA Technical Overview". URL: http://www.citrix.com/products/sica/sicawp/start.htm

"ICA Browsing with Firewall Address Translation (NAT)". Citrix SolutionsKnowledgebase. March 24, 1999. URL: http://ctxex10.citrix.com/texpert.nsf/2e89dc7305e02e12852566650069ba69/e9e622dbbaf8b2b985256688005be477?OpenDocument

Last Updated: July 24th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor