Principled Technologies®

WHITE PAPER
February 2007

Rich clients with thin client data security: a hybrid approach

Contents 2
Executive summary 2
Key data security concerns and remedies 3
Summary 5
Appendix A: Additional common security issues ...6
Appendix B: Sample test description 7

Executive summary

Intel Corporation commissioned Principled Technologies, Inc. (PT) to examine how to deliver some of the data security characteristics traditionally associated with thin clients on rich clients (PCs).

Full security of a computing environment involves more than just data security. Full security includes dealing with viruses, Trojan horses, worms, and other types of attacks on system. It also involves physical security. This white paper concentrates on data security, the prevention of theft of data from computers. In particular, it looks at the data-security differences between thin and rich clients and how IT departments can overcome those differences.

Thin clients often receive praise for being one of the most secure approaches to computing for one simple reason: Because they hold no actual data locally, extracting any sensitive information from them is quite difficult. This characteristic has an immediate and obvious appeal to organizations that, such as those in health care, finance, and government, that are particularly concerned about losing sensitive information. The lack of any local storage means that users cannot extract confidential information by employing any of the most common methods: copying files using CDs, diskettes, or USB drives; copying and pasting information from one file to another; and taking screenshots. (Though many thin client devices possess USB ports, disabling those ports for data transfer is typically a fairly straightforward process.)

Rich clients, by contrast, often receive criticism as possessing many inherent data security problems. Those problems center on the fact that rich clients typically provide multiple mechanisms, including the ones we mentioned above, for removing confidential data. At the same time, rich clients provide a wide variety of attractive features that have made them far and away the desktop computing standard. Key advantages over thin clients include performance (for example, see our test report http://www.principledtechnologies.com/clients/reports/intel/ThinvsPCperf.pdf), flexibility, ability to prepare for future technologies, and so on.

Organizations that use rich clients can, of course, mitigate or address these issues through the use of proper security procedures and policies that govern data storage on servers, application development, and use of client and server operating system security capabilities.

For some organizations, however, the fact that rich clients possess the many ways of removing information remains a major concern.

Fortunately, a hybrid solution exists that can make it as difficult to remove certain sensitive information from rich clients as from thin ones.

This solution uses software to let a rich client essentially act as a thin client while running security-sensitive applications. Administrators set up the servers and clients so that users have access to sensitive information only while computing in this controlled environment. The users can still, of course, run other, less sensitive applications in the usual way, locally on their PCs.

Thus, this hybrid technique lets users enjoy both the security controls of a thin client and the performance and other benefits of the underlying rich client.

Several possible software options exist, but in this white paper we examine the most popular one, which involves using software from Citrix Systems. (Other computing models, such as application streaming, that have positive implications for data security are beyond the scope of this paper.)

The Citrix Access Essentials software includes a program (Access Client 4.1.0) that runs on a PC. That software communicates over a network to additional Citrix software on a server. This server software (MetaFrame Presentation Server 4.0) lets multiple users run sessions on the server and send the screen images from the server back to the program on the PC. Administrators then permit access to secure information only from applications running in the Citrix client environment.

Put differently, the PC would contain a window that was acting as a thin client and running programs on the server. Other windows could simultaneously be running other applications locally on the PC.

Simply running this Citrix software does not by itself address the security issues. The Citrix client

software provides many features, such as access to USB devices from the host, cutting and pasting from host applications into ones running locally on the PC, and so on, that are extremely useful in many environments. These same abilities, however, can also open security issues.

Fortunately, most versions of the Citrix Presentation Server software allow you to disable those features for specific applications or services. (Buyers should, of course, check with their vendors to determine which version of Citrix Presentation Server will best meet their needs.)

So, by running the Citrix software and disabling the appropriate applications and services, organizations can have the security features of thin clients on their PCs, while at the same time preserving all the other advantages of the PC and the ability to run less sensitive applications locally.

In the next section, we provide the details necessary for customizing the Citrix software to provide these features. We also discuss how to address another potential rich client security issue, screen shots.

We verified that all of these techniques work by actually implementing them. In Appendix B, we provide a brief description of our sample test setup.

Finally, we must note that both thin and rich clients share certain security vulnerabilities. Some of these vulnerabilities involve common computing technologies, while others stem from issues outside the client computing device. We examine some of these issues in Appendix A.

As these sample issues illustrate, any organization that considers security to be a key concern will have to employ not only technological security solutions but also a solid set of security policies governing human behavior.

Key data security concerns and remedies

Rich clients offer three main avenues for removing data that thin client devices typically do not:

- Copying files
- Copying and pasting
- Taking screenshots

A combination of the Citrix-based hybrid solution we described and some additional work with the operating system of the rich clients can let them act as thin clients in each of these areas. The following subsections detail the solutions to each of these areas.

Copying files

One of the most obvious security threats to sensitive data is the use of a CD drive, diskette drive, or USB drive to copy files straight from a server to a mobile device or storage medium on the PC. Such data movement is very easy to do and can be difficult to detect in many computing environments.

Fortunately, addressing it with the hybrid approach is straightforward.

The Citrix software includes the ability to let users who are running programs on the server copy files directly onto their PCs' USB, diskette, or CD drives. The software does this by using a technique called drive mapping, in which a PC's local drives appear as if they were drives in the user's session on the server. This ability is useful and even vital in many computing environments.

To prevent that ability in situations where security is a paramount concern, however, the Citrix software includes security options the administrator can set. The connection configuration options for the Citrix server software include a capability for disabling client drive mapping. Disabling drive mapping will prevent a user from copying server files to a local device during his Citrix server session.

The basic process an administrator would follow to disable drive mapping from Citrix to the desktop involves the following simple steps:

1. Open Citrix Connection Configuration.
2. Double-click ICA-TCP connection type.
3. Click Client Settings.
4. Check Disable Client Drive Mapping.
5. Click OK.

This change affects only applications that are running on the server and that users are accessing via Citrix software. Applications that are running locally on the PC would still have their normal ability to save and copy files.

Copying and pasting

Another potential way to move sensitive data from the server to a PC is by using copy and paste. While moving the contents of a file via copy and paste is more labor-intensive than simply copying

the file, it still represents a potential security vulnerability.

Of course, in many environments this same ability can be very useful. A user might, for example, need to copy the results of a database query he executed during a Citrix session and paste them into a local PowerPoint presentation he was preparing for management.

As with file copying, Citrix's software provides an option, Disable Client Clipboard Mapping, for preventing users from being able to copy server data to the PC's local clipboard.

The process an administrator would follow to invoke this option is basically the same as the one we described above. This option and the Disable Client Drive Mapping option appear on the same settings dialog box. Local PC applications would still be able to use the Clipboard for copying and pasting.

Taking screenshots

The final potential vulnerability of the hybrid PC solution stems from the ability of the PC user to take a screenshot of a Citrix session and store that image locally. The user would first get the data of interest in the Citrix window and then save it to a file on the PC by using the print-screen (PrtScn) key.

This approach to data theft is obviously both inefficient and labor-intensive, but it does represent a potential security liability.

This issue is trickier to address than the other two we discussed because it is not a feature of the Citrix software. Instead, it is a Microsoft Windows capability. The way most users take screenshots is built into Windows and is simple to activate: Press the PrtScn key on the computer's keyboard.

Neither Windows nor Citrix offers an obvious way to disable this capability. Fortunately, workarounds to this problem exist.

The simplest and most effective strategy we found to eliminate the Windows PC's ability to take screenshots is to remap the PrtScn key so that pressing it no longer executes the print-screen function. (An IT administrator, rather than a user, would typically make this change.) You can do this by using a Registry editor, such as Windows' RegEdit, to edit the Windows Registry as follows:

1. Find the Registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout
2. Create a new Binary Value, and name it Scancode Map
3. Set 00, 00, 00, 00, 00, 00, 00, 00, 02, 00, 00, 00, 00, 00, 37, E0, 00, 00, 00, 00 as the value in ScanCode map. (In this example, we include commas to separate the values for ease of reading. The Registry entry would not show them. We also use red to show the remapped key value (do nothing) and blue to represent the original key value (print screen)).
4. Reboot the computer.

Most users will not know how to restore this functionality. Organizations that want to make sure users cannot restore it can remove most end-user rights to the complete registry. (By default, users who belong only to the Windows built-in Users group do not have the necessary rights to edit this area of the registry.) Administrators can also make global group policy changes or discrete registry security changes that can disable any Citrix user's ability to modify this setting.

This technique stops all PC applications, both those running on the server via Citrix software and those executing locally, from being able to use the PrtScn key.

This approach does not, however, stop applications designed to capture screen images from doing so. The only way to stop those applications is to not allow users to install them. IT departments that want to stop this potential security issue, as well as issues that malicious software might cause, is to enforce strict policies governing the software the organization allows on its PCs.

Finally, the problem of stopping the determined and skilled data thief is beyond the scope of this white paper. See Appendix A for a brief discussion of some of the issues such people pose.

Summary

The fact that many thin clients possess no ability to store data locally makes them appear to some users to be more secure than typical rich clients. By properly configuring rich-client computing environments with Citrix software and making a Windows Registry change, organizations can give rich clients the same security features for certain security-sensitive applications and data. Disabling the most common data security loopholes will typically not affect local PC applications. Some of the steps, such as disabling print screen and preventing applications from installing on the PC, can affect local PC applications.

This hybrid approach lets the PC users continue to run appropriate applications locally and enjoy the many other advantages of the rich client.

Appendix A: Additional common data security issues

During testing, we noted several potential security issues that are present on both thin clients and rich clients (PCs). Most of these security issues arise when a system has access to the Internet. Two potential issues have nothing to do with the client technology per se.

All of these issues are equally problematic for thin-client, rich-client, and hybrid rich-client environments. The only way to avoid all of them is to implement the appropriate human security procedures. That said, organizations can help control the Internet-based issues by using service-based applications running Citrix software rather than general server-based sessions in which the user can run any application.

We mention these issues only to point out that any complete security system must include and enforce a set of controls on the actions of its users.

Internet-related potential issues

For environments in which users can access email or a Web browser, they may be able to use email—either their corporate e-mail system or a browser-based email offering such as Hotmail or Gmail--to break security by sending files or information outside the enterprise. This problem can affect server-based applications even if you have disabled local copying and pasting, because it offers another way, even on thin clients, to remove corporate data.

Even without access to email, simple access to a Web browser may allow users to upload files or copy and paste to them to sites designed to receive information.

IT departments must resolve these issues on the server side for both thin and rich clients. They may need to change some server-based applications and even disable some application capabilities to make those applications appropriately data secure.

Hardware or software client spoofing

One way around most of the protections of thin or rich clients is to use a hardware device (or software on a PC) to spoof the server--basically, to pretend to be a thin client. By doing this, the device or software could record what the server sends to the thin client or thin-client session.

IT organizations can prevent this type of attack by using the proper client-server authentication protocols and techniques.

Hardware device

A malicious user could also connect a recording device to the connector to which the monitor of either a PC or thin client would attach. The only way to prevent this from happening is by creating and enforcing policies against it.

Issues related to digital cameras

Users can employ digital cameras, both dedicated cameras and those present in such other devices as phones and PDAs, to photograph on-screen data and take that data outside the enterprise. This approach is obviously quite labor-intensive for all but the smallest data thefts, but the combination of such photos and optical character recognition technology represent another path for taking large quantities of data from an enterprise and reproducing it in computer-readable form.

The low-tech approach

Anyone who really wants to steal sensitive information from a computer can, of course, do so without any electronic device. Simply writing a set of account numbers or other private information on a sheet of paper is an easy way to copy confidential information.

Appendix B: Sample test description

We began the setup by linking a server, a PC, and a Wyse thin client on a network that had Internet access. After our initial testing with Internet access, we placed the three systems onto a closed network to help identify vulnerabilities that did not involve Internet capabilities.

Server setup

We used a server running Windows 2003 Server. We set up the server according to the methodology in our previous thin client test report: http://www.principledtechnologies.com/clients/reports/Intel/ThinvsPCperf.pdf.

We also installed Citrix Access Essentials on the server and gave the system a static IP address.

We then worked with the Citrix security settings available in its Connection settings dialog. We used such settings as Disable Client Drive Mapping and Disable Client Clipboard Mapping.

PC client setup

We installed Windows XP Service Pack 2 with the default settings on the client PC. We then installed the client portion of Citrix Access Essentials. We set up that software so the system would properly connect to the server. We created two connections: one with a full desktop connection to the server, and one that allowed only Microsoft Word.

Thin client setup

For the Wyse thin client, we added the Citrix ICA connection and set up a static IP address.

About Principled Technologies

We provide industry-leading technology assessment services. We bring to every assignment extensive experience with and expertise in all aspects of technology testing and analysis, from research into new technologies, to the development of new methodologies, to testing with existing and new tools.

When the assessment is complete, we know how to present the results to a broad range of target audiences. We provide our clients with the materials they need, from market-focused data to use in their own collateral to custom sales aids, such as test reports, performance assessments, and white papers. Every document reflects the results of our trusted independent analysis.

We provide customized services that focus on our clients' individual needs. Whether the technology involves hardware, software, Web sites, or services, we offer the experience, expertise, and tools to help you assess how it will fare against its competition, its performance, whether it's ready to go to market, and its quality and reliability.

Our founders, Mark Van Name and Bill Catchings, have worked together in technology assessment for over 20 years. As journalists they published over a thousand articles on a wide array of technology subjects. They created and led the Ziff-Davis Benchmark Operation, which developed such industry-standard benchmarks as Ziff Davis Media's Winstone and WebBench. They founded and led eTesting Labs, and after the acquisition of that company by Lionbridge Technologies were the head and CTO, respectively, of VeriTest.

Principled Technologies, Inc.
1007 Slater Road, Suite 250
Durham, NC 27703
www.principledtechnologies.com
info@principledtechnologies.com