Georgia Library Quarterly

Volume 47 | Issue 1 Article 4

January 2010

Save Gas Using your Office Computer from Home

Steve Duckworth
Augusta State University, sduckworth@aug.edu

Damon Armour
Augusta State University, darmour@aug.edu

Jeff Heck
Augusta State University, jheck@gru.edu

GOMO WHITE PAPER

Save gas using your office computer from home

by Steve Duckworth, Damon Armour and Jeff Heck

Introduction

Improvements in technology in the past decade have improved options for working from home. Increased bandwidth, more secure connections and faster computers allow employees to connect productively with their office computer[1]. Cost efficiencies in business in the past decade, and particularly the current economy, serve as a stimulus for employees to work from home as possible, given the costs of transportation, parking, traffic, the need to be able to connect at any time[2] and concerns about personal safety when visiting an office at night.

How does this play out in the higher education environment in Georgia? What options are available for connection from home, how secure are they and how easy are they to implement? What are the underlying technologies, and how does the establishment of such connections affect the information technology (IT) departments in colleges and universities?

This paper will review current literature available in library databases, provide background on the protocols used to establish remote connections, discuss changes in the Remote Desktop Protocol (RDP) currently in use in Windows products, illustrate making a connection from home, provide information on security and mention a method currently in use for users at Augusta State University for providing a secure connection. The hope of this paper is that it will provide options for some users and open discussion on how best to provide this service for employees. It is aimed at users with a moderate ability and interest in how computer systems work. Users with little background should consult their IT unit to determine an effective method of connection.

Literature Review

Searches of library databases produced few articles on the subject of remote connection to office computers[3, 4]. While there were articles concerning working from home, the one article located on the use of RDP in libraries focused on its use within a network[5] rather than connection from a computer outside the work network, which is a different security situation. Computers in the same network do not have to pass across the public Internet or travel through a firewall.

Underlying Protocols

Terminal emulation is a long-established process in the Unix world for connecting one computer to another. Products such as Hummingbird have provided an ability to connect from one computer to another device, even from Windows to Unix, since at least the 1970s. In the Microsoft Windows environment, Terminal Services comes in two flavors. One is a Remote Assistance client, for connecting to a server to run applications there; for individual PC users to connect to other PCs, Remote Desktop Protocol is used, providing an established set of instructions both computers use to establish the transfer of data, including moving files. With RDP, all the processing is done on the computer to which you connect, then transferred by "channels" to the computer where you are for display. Mouse activity is one channel, keyboard activity is another channel, etc.

RDP was first introduced as part of Windows NT 4.0 Server, Terminal Server Edition as version 4.0 (August 1996). New versions have been released since including version 5.0 with Windows 2000 Server (February 2000), version 5.1 with Windows XP (October 2001), version 5.2 with Windows Server 2003 (April 2003), Version 6.0 with Windows Vista (November 2006) and version 6.1 with Windows 2008 Server (February 2008). By default, the protocol uses 128-bit encryption, using the RC4 encryption algorithm, and it listens for incoming

connections on TCP port 3389. RDP clients exist for most versions of Windows (including handheld versions), Linux/Unix and Mac OSX.

Secure Shell (SSH) is a protocol that allows data exchange using a secure channel. It was designed as a replacement for Telnet and other insecure remote shells that would send information in clear text (no encryption). The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet. The first version of the SSH protocol, known as SSH-1, was first introduced in 1995. It has been revised over the years, and the latest version of the protocol, which provides both security and feature improvements, is known as SSH-2.

RDP Features

RDP currently is in version 6.1, and that version will continue in Windows 7.[6] Earlier versions of remote desktop caused some problems with matching screen resolutions and number of colors, printing, file transfer, etc., but ease of use and functionality have steadily improved in the versions. One consideration for institution networks traditionally has been that if many users are connected remotely, it can overconsume available bandwidth and input/output. In Windows 7, connecting to a Windows 2008 server, the compression and design are improved; users will even be able to play high-definition video using Media Player.[7] Video was unavailable in earlier versions of RDP.

Version 6.0 improvements[8]

- Server authentication (keeps you from connecting to the wrong server; can be set to refuse the connection if authentication fails)
- Resource Redirection (supports Plug and Play devices)
- Terminal Server Gateway Servers (combines RDP with secure HTTP to allow connection over a corporate firewall using a Secure Sockets Layer tunnel; removes a need for a Virtual Private Networks (VPNs))
- Terminal Services RemoteApp (allows you to run a specific application on a remote computer without having to view the complete desktop; the program opens on a window on the local computer.)
- Monitor Spanning (allows the use of two high-resolution monitors
- Supports 32-bit color and font smoothing

Version 6.1 features

- Network Level Authentication (verifies user before a full connection to the remote computer is established; can be used with XP Service Pack 3)
- Terminal Services Web Access (reach your PC through any computer with a Web browser)
- RDP Signing (allows administrators to restrict your access to specific resources)
- Terminal Services EasyPrint (removes the need to set up the local printer (only for connections to Windows 2008 servers)

Security Concerns

In a system of providing remote access to campus resources, the confidentiality, integrity and authentication of all data and systems are crucial. RDP offers a relatively easy method for users to connect to remote computers on or off campus. Earlier versions of RDP (versions prior to 6.0) were very susceptible to man-in-the-middle attacks where — even though the traffic was encrypted — the potential was there to decrypt the data if it was weak or no certificate system was in place. Version 6 of RDP introduced the use of TLS (Transport Layer Security), the antecedent protocol to Secure Socket Layer (SSL). Wikipedia explains TLS as a "protocol allowing client/server applications to communicate across a network in a way designed to prevent eavesdropping, tampering and message forgery. TLS provides endpoint authentication and communications confidentiality over the Internet using cryptography."[9] Version 6 has reduced the risks associated with man-in-the-middle attacks.

Other methods for implementing RDP sessions include utilizing other security protocols for connectivity and transport of data. These options can include RDP over SSL, RDP over SSH, and RDP over VPN. Utilizing these secure protocols better insures that the data between the two endpoints is transferred securely, including reducing the risk of man-in-the-middle attacks. Utilizing the above protocols also eliminates issues related to RDP version conflicts. The sessions are contained within the secure tunnels created by SSL, SSH, and VPN.

In any secure transaction, security at each endpoint is as important as the security of the transfer of information between the endpoints, With a successful connection to a campus computer, the remote endpoint (if allowed by your institution's policies, this could be your home computer) is now connected and interacting with the campus computer in a trusted fashion, so the security of the remote endpoint is key. The home institution loses control of the security infrastructure of these endpoints. Maintaining proper training and assistance to remote users on security tools to protect their systems on and off campus is therefore vital. The home user must remain up to date with their virus protection, anti-spyware software, critical operating system patches and appropriate wireless network encryption and remember to avoid weak password practices (such as using the same password for all accounts) and social engineering threats (don't allow others to use your computer account).[10] For these and other recommendations, see the National Institute of Standards and Technology User's Guide to Securing External Devices for Telework and Remote Access, http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf.

For our school, these concerns are addressed in our Remote Access Agreement. *(See sample on page 10.)* The agreement covers: All requests for accounts must be approved by the employee's supervisor, accounts may be disconnected from remote access at any time, and no other remote networks may be connected to at the same time as the ASU remote access.

A security concern with commercial products is that they may bypass the campus firewall or similar security infrastructure and connect directly to a desktop; these connections can be set without the immediate awareness of the local IT group. Such connections may pose a security risk because of the possible insecurity of the home computer.

An Example of How To Start RDP

To establish an RDP connection, either a Virtual Private Network (VPN – to connect you to a group of computers where you can identify one computer by its name) or the specific IP of the computer on the Internet will be needed. VPNs are more often used in the corporate world. If your institution provides VPN connections, contact them for access.

If you have a specific IP address for the computer to which you wish to connect, follow these steps. (The same approach with screen shots is available at: http://www.microsoft.com/windowsxp/using/mobility/getstarted/remoteintro.mspx)[11]

For XP:

On your office computer (must run XP Professional or server):

1. Click on Start, then Control Panel, then Performance and Maintenance
2. Click System
3. Click the Remote tab; check the box for Allow users to connect remotely to this computer

Office of Information Technology Services
Augusta State University

Remote Access Agreement

Last Name: _____

First Name: _____

Department: _____

Timeframe Needed:
- ☐ Annual
- ☐ Semester
- ☐ Other_____

By signing on the line below, I agree to and understand the following criteria:

- Ensure the confidentiality of the records I have been given access
- Safeguard the security of my password and other credentials involved in connecting with ASU resources
- Maintain current anti-virus definitions, all Operating System patches and hot fixes on all computers or other devices used to connect to the ASU network (http://www.aug.edu/its/pc_mgt_home.html)
- Ensure that the ASU or privately owned computer that is remotely connected to the ASU network is also not remotely connected to another network at the same time. Example: Establish only one remote connection at a time
- I agree to abide by and follow the policies and procedures established by the University for the use of the network and information systems (http://www.aug.edu/its/policies)
- If network problems are detected, your remote access may be disconnected at any time
- Accounts will be monitored for inactivity, and disabled after 90 days if unused. Accounts can be reactivated by contacting the ITS Help Desk.

My signature indicates that I have read, understand, and agree to abide by the terms and conditions of this agreement

_____ Date: _____
Signature of the requestor

Department Head Authorization:

_____ Date: _____
Name / signature of the requestor's department head

ITS Use Only

_____ Date: _____
Remedy Ticket Number

Version 1.2 3/2/2009

4. Set Windows Firewall to allow RDP connections; return to the Control Panel and select Security Center
5. Click Manage security settings for Windows Firewall
6. Uncheck the Don't Allow Exceptions box
7. Click the Exceptions tab
8. Check the Remote Assistance box; click OK
9. Return to Control Panel; click Performance and Mantenance, click System, then click Computer Name tab. Write down computer name (if using a VPN); click OK. Or, if not using a VPN, go to Control Panel, Network and Internet Connections, Network Connections, Local Area Connection, Properties; click on Internet Protocol(TCP/IP) and Properties. Write down the IP address. If there isn't one there, check with IT. It's likely your computer is randomly assigned an IP number, and you'll need to work with them.

On your home computer:

1. Click on Start, choose All Programs, then Accessories
2. Choose Communications, then Remote Desktop Connection
3. In the Computer box, type in the name of your host computer (if using a VPN) or the IP address of the computer if not.

Note: Your campus may restrict use of RDP for security reasons by limiting remote connections on the network, by blocking access to the port RDP normally uses or by other means. Contact your IT unit if you have questions.

Example of Use

Augusta State University currently provides remote access capabilities for faculty and staff using RDP tunneled over the SSH protocol. Using freely available terminal software (Bitvise Tunnelier, PuTTY, etc.), the Microsoft RDP client and an SSH server, the remote session can make use of the 256-bit AES (Advanced Encryption Standard) encryption provided by SSH to further secure the connection to the office computer over the Internet. Once connected, the experience is identical to the user sitting at their office computer. This method provides the users with easy access to their work data in a visually familiar environment, which keeps productivity high — even while sitting at home. Now instead of taking data home on a flash drive or other removable media, data is protected from being lost or stolen since it never leaves campus.

The librarian author of this paper uses a MacBook Pro at home, with VMWare Fusion (to run a different operating system virtually) and Windows 7 release candidate to connect to campus. (There is a Mac RDP client that can be run directly in the Mac operating system, but the terminal services client to provide the SSH tunnel is a Windows-environment software.)

Use at Other USG Sites

In an informal review of four other universities in the system, two schools reported that remote desktop connections are not allowed by the campus IT unit, based on security concerns. One school reported that they point interested users to PCAnywhere. The last school provides access through SSH (as we do) but does not provide support. While security is crucial, and RDP in earlier versions ran unencrypted or with weak encryption, it is now possible to run the protocol with higher levels of encryption. One author promotes such connections in the Linux environment.[12] A belief in the adequacy of the level of security is an issue that must be settled at the local institution.

Other Considerations

Another consideration is that, according to state law, any device you use at home for business purposes may legally be searched by state enforcement agencies. The Secretary of State's Department of Archives and History notes that under the Open Records Act, it would be possible for government agencies to subpoena access to your personal computer and cell phone in order to see public records.[13]

Conclusion

While there are security issues to be considered, and which must remain a primary concern, there are options for securely connecting to an office computer. The option offers meaningful time savings and ease of productivity for employees. The remote desktop may provide access to software that cannot be purchased for home use, access to stored e-mail and access to resolve problems when remote services go down. ⏭

Steve Duckworth is assistant director for network services and Damon Armour is IT security officer in the Information Technology Services at Augusta State University (ASU). Jeff Heck is automation librarian at ASU's Reese Library.

Software Options:

Some commercial software options that make use of RDP to connect to your office computer:

GotoMyPC – 30-day trial; $20/month, discount for annual subscription. https://www.gotomypc.com

LogMeIn – free version; provides strong encryption. https://secure.logmein.com

PCAnywhere – Symantec product. $199.95 download. Supports more complex setups. http://www.symantec.com/norton/symantec-pcanywhere

GBridge – establishes a VPN. Extends Google GTalk but not supported by Google; supports XP, Vista, Windows 7 among others. http://www.gbridge.com/

Note: Use of these packages is likely to require logging in through and transferring information through third-party servers, a practice that security-conscious IT personnel may consider a risk in itself.

Recommended Sites:

For plain English information about RDP, specifically aimed at Windows XP but useful for learning about the software for any version, see the Microsoft TechNet paper at http://technet.microsoft.com/en-us/library/bb457106.aspx

Microsoft TechNet article on configuring Remote Desktop in XP: http://technet.microsoft.com/en-us/library/bb457106.aspx

RDP FAQ from Microsoft: http://windowshelp.microsoft.com/Windows/en-US/Help/f55326fa-e629-423b-abba-b30f76cc61e61033.mspx

Wikipedia article on RDP: http://en.wikipedia.org/wiki/Remote_Desktop_Services

To see a comparison chart that shows many of the software packages allowing remote connection, including Linux and Mac, see: http://en.wikipedia.org/wiki/Comparison_of_remote_desktop_software

For a site offering reviews of and downloads for Remote Desktop software: http://download.cnet.com/windows/remote-access/?tag=mncol;pop

Troubleshooting RDP connections (focused on Vista, but may help): http://windowshelp.microsoft.com/Windows/en-US/Help/5c4f7ad8-40b3-452d-81ec-3a63453f0ada1033.mspx

Tips for securing RDP: http://www.mobydisk.com/techres/securing_remote_desktop.html

Advanced Microsoft site for security with RDP 6: http://msdn.microsoft.com/en-us/library/aa912575.aspx

2005 advisory about Man in the Middle attacks with RDP: http://www.oxid.it/downloads/rdp-gbu.pdf

64-minute detailed video from a developer's conference on RDP in Windows 7: http://channel9.msdn.com/pdc2008/ES21/

Bibliography:

1. Smith, Dawn, and Teresa B. Van Dyke. A Telecommuting Interlibrary Loan Librarian's Experience; the views of Both the Telecommuter and the On-Site Supervisor. Journal of Interlibrary Loan, Document Delivery & Information Supply. 18, no 4, 2008, pp. 449-55.

2. http://en.wikipedia.org/wiki/Terminal_Services

3. Working from Afar: a new trend for librarianship. Duncan, Jennifer. College & Library Research News. 69, no. 4, April, 2008. pp. 216-18.

4. Lookin' Good: for the next frontier in displays and virtualization, look to the GPU. Morejon, Mario. Computer Reseller News. December 3, 2007, p. 35. Retrieved from Lexis-Nexis in GALILEO, July 25, 2009.

5. Using Remote Desktop® with Pro® and Vista Business®. Norman, Dan. Nebraska Library Association Quarterly. 38, no. 3, Fall 2007, pp 25-7.

6. ibid.

7. http://channel9.msdn.com/pdc2008/ES21/

8. http://support.microsoft.com/kb/925876

9. http://en.wikipedia.org/wiki/Transport_Layer_Security

10. User's Guide to Securing External Devices for Telework and Remote access (DRAFT). Scarfone, Karen, and Murugiah Souppaya. National Institute of Standards and Technology. Special Publication 800-46, version 2. Nov. 2007. http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf

11. http://www.microsoft.com/windowsxp/using/mobility/getstarted/remoteintro.mspx

12. Paranoid Penguin: Secured Remote Desktop/Application Sessions. Bauer, Mick. Linux Journal. September, 2008, no. 173, pp 34-38.

13. http://www.sos.ga.gov/archives/who_are_we/rims/publications/legal_duties_and_liabilities.htm