Remote Access Options to University Resources

Samuel Petreski
IT Security Office
Introduction

- What is Remote Access?
- Why use Remote Access?
- How many of you use Remote Access to Campus resources?
- Goal of today’s presentation
Agenda

- Statistics of current applications used
- Remote access considerations
- Remote access options and best practice configuration
  - FTP
  - MyFiles
  - VNC
  - Remote Desktop
  - SSH/SFTP
  - WebDAV SSL
  - X Server
  - VirtualDesktop
- Recommendations
- Q & A
Statistics

April 2007 Statistics

- Remote Desktop - 6584
- SSH Servers - 2400
- FTP Servers - 1499
- VNC Servers - 814
- X Servers - 241

November 2007 Statistics

- Remote Desktop - 7450
- SSH Servers - 2438
- FTP Servers - 1432
- VNC Servers - 861
- X Servers - 209
Remote access considerations

- Remote access creates vulnerability
- Extends University data beyond campus boundaries
- Strong user and computer authentication
- Data communication encryption
- Simple, flexible, and secure
Remote access options - FTP

- **Access type**
  - Remote access to files

- **Pros**
  - Simple to configure and use
  - Faster than http
  - FTP client available with most OSs

- **Cons**
  - Unsecure – plain text authentication & communication

- **Best practice configuration**
  - Don’t use it for private communication!
  - Use SFTP
Remote access options – SSH/SFTP

- **Access type**
  - Remote access to the system and files

- **Pros**
  - Simple to use
  - Secure (encrypted) authentication and communication
  - SSH and SFTP server configuration is the same

- **Cons**
  - Special client required (included with most *nix systems)
  - Some applications don’t support the protocol

- **Best practice configuration**
  - Allow access only to the users that needed
Remote access options – SSH/SFTP
Remote access options – SSH/SFTP

- **Best practice configuration**
  - **sshd.config – configuration examples**
    - Protocol 2
    - PermitRootLogin no
    - AllowedUsers spetresk <userid>
    - MaxAuthTries 3

- **Inetd, iptables**

- **The Auto Blacklist Module: pam_abl**
  (http://www.hexten.net/assets/pam_abl_doc/index.html)

```bash
# /usr/local/etc/pam_abl.conf
# debug
host_db=/var/db/pam_abl/hosts.db
host_purge=2d
host_rule=*:10/1h,30/1d
user_db=/var/db/pam_abl/users.db
user_purge=1d
user_rule=!spetresk|!<user>:/sshd:5/10m,30/1d
```
Remote access options – SSH/SFTP

- **University Resources**
  - H: drive – Personal file space, Departmental Drive, DFS

```
Host: sftp.iowa.uiowa.edu
```

- **Available Applications**
  - SSH Secure Shell
  - WS_FTP Pro
  - OpenSSH
  - Windows SFTP server
    - CopSSH
    - SSH Tectia
Remote access options – MyFiles

- **Access type**
  - Remote access to files stored on ITS’ file cluster

- **Pros**
  - Accessible through a web browser
  - Simple to upload and download files
  - Secure (encrypted) authentication and communication
  - Hawk ID authentication

- **Cons**
  - Not accessible through applications

- **Access**
  - [https://myfiles.uiowa.edu/](https://myfiles.uiowa.edu/)

- **Demo**
Remote access options – WebDAV SSL

- Access type
  - Remote access to files

- Pros
  - Simple to use
  - Secure (encrypted) authentication and communication
  - Many web edit applications support the protocol

- Cons
  - Web server add-on for WebDAV support
  - Default configuration without SSL
  - Vista default configuration doesn’t work

- Best practice configuration
  - Make sure only WebDAV over SSL is enabled
Remote access options – VNC

- **Access type**
  - Remote access to the desktop

- **Pros**
  - Full access to desktop applications and files
  - Freeware server/client applications available
  - Cross-platform support

- **Cons**
  - Special client required for access
  - Easy to mis-configure
  - Not all VNC applications support encrypted communication

- **Best practice configuration**
  - Allow access only to specific hosts
  - Use an application that supports encrypted communication
Remote access options – VNC

- **Best practice configuration**
  - Always use a strong password
  - If encryption is not supported, use SSH tunneling

- **Available applications**
  - RealVNC ([http://www.realvnc.org](http://www.realvnc.org))
  - UltraVNC ([http://www.uvnc.com](http://www.uvnc.com))
  - Vine Server Mac OS X
  - Many other flavors of VNC

- **Demo**
Remote access options – X Server

- **Access type**
  - Remote access to *nix systems

- **Pros**
  - Full access to desktop applications and files

- **Cons**
  - Special server/client required
  - Easy to mis-configure
  - Communication is not encrypted

- **Best practice configuration**
  - Allow access only to specific hosts (xhost)
  - SSH tunnel your connection
Remote access options – Remote Desktop

- **Access type**
  - Remote access to Windows host desktop

- **Pros**
  - Full access to desktop applications and files
  - Secure file transfer between client and remote host
  - Part of the Windows XP/2003/Vista Operating System
  - Encrypted authentication and communication

- **Cons**
  - Easy to mis-configure
  - Man-in-the-middle attacks
Remote access options – Remote Desktop

- **Best practice configuration**
  - Allow access only to specific hosts
  - Allow only specific users to have access
  - Install SSL Certificate on MS Terminal Server
Remote access options – VirtualDesktop

- **Access type**
  - Remote access to published applications

- **Pros**
  - Accessible through a Web browser
  - Encrypted authentication and communication
  - Secure access to H: drive, and flexible file transfer

- **Cons**
  - Thin client installation or Java required
  - Only certain application available

- **University Resources**
  - [https://virtualdesktop.uiowa.edu/](https://virtualdesktop.uiowa.edu/)
  - [https://desktop.healthcare.uiowa.edu/](https://desktop.healthcare.uiowa.edu/)
Remote access options – VirtualDesktop

- Demo

![Citrix Web Interface](image1)
![Client File Security](image2)
![Citrix Web Interface](image3)
Recommendations

- Use a strong password
- Limit the range of hosts that can connect
- Use a server/client that supports encryption
- Keep your solution simple

- Use VirtualDesktop
Q & A
Thank You!