Computer Security

Ryan Hamel

Lowell Digisonde International, LLC

Outline

- Best Practices
- Data Computer Network Services
- Firewall Settings / Antivirus
- Routine Hard Drive Backup
- Windows XP

Computer Security Best Practices

- Place the system behind a hardware firewall or router
- Make use of Publisher computer
- Allow only limited remote access from select IP addresses and ports
- Do not use system as a workstation
- Install antivirus software (optional)

Data Computer Network Services

- DHCP (UDP 67, 68), and TFTP (UDP 69) for Control Computer PXE
- Windows Firewall disabled on “Internal” (Control Computer interface)
- Microsoft IIS FTP server (TCP 20, 21)
- SSH Server Not Installed by default (TCP 22)
- Apache (HTTP 80)
- Microsoft Remote Desktop (RDP 3389)
- Using Microsoft Firewall
- Windows Firewall Exceptions for “External” Interface
  - Necessary for 3389
  - Also include D:\Dispatch\FTPS.exe,

Firewall Settings

- Limit access to the system via firewall at the network edge.
- Only allow access to the system via
  - Port 80 (for access from anywhere)
  - Port 20,21 (for access from UMLCAR, LDI, you)
  - Port 22 (if SFTP / SSH services are installed)
  - Port 3389 (for access from UMLCAR, LDI, you)

A note on Antivirus Software

- No antivirus software is installed due to concerns regarding performance of data computer
- If antivirus software is installed, the Data Computer should be thoroughly tested. Stress the system with high cadence or “dense” schedules

Note Regarding Routine Backup of Spare Drive

- Important to routinely update the DPS-4D spare drive
- Use any hard drive imaging software: Acronis True Image, Norton Ghost, etc
- Usually requires removing operational drive from the DPS-4D

Windows Update

- Safe to update Data Computer via http://windowsupdate.microsoft.com
- Important to perform the windows update.
- Restore from DPS-4D spare hard drive if problems occur
- Contact us about certain vulnerabilities or patches if concerned

Microsoft Support Lifecycle

- Windows XP (Home, Media Center, Professional, Starter, Tablet Edition)
  - Extended Support End Date: April 8, 2014 (support and updates are no longer available)
- Windows XP Embedded
  - Extended Support End Date: January 12, 2016

Windows XP Embedded Support

- windowsupdate.microsoft.com can still be used to download updates up through the April 8, 2014
- Additional security fixes will be made available to OEMs when released
- Additional security fixes can be requested from LDI


Dalu
감사합니다
Gracias
Danke
Ευχαριστίες
THANK YOU
Obrigado
Köszönöm
Grazie
Спасибо
Dank
Tack
谢谢
Merci
ありがとう
IGF 2014
XIV INTERNATIONAL GIRO FORUM · 20-23 MAY

BACKUP

Overview of Windows Security Setup

- Windows XP Embedded service pack 3
- Default local security policy
- Default security template
- Makes use of standard Windows Firewall
- No Antivirus Software Installed when shipped

- Configuration of the operating system security is done via Microsoft Local Group Policy / Local Security Policy

Hard Drive Highlights

C:\	(Windows operating system)
D:\Apache	(Web server)
D:\Buffers	(Outgoing data directories)
D:\Dispatch	(Dispatcher, DCART, picture generating, ARTIST)
D:\DPSMAIN\Dps2Aux	(DCART data is delivered here)
D:\DPSMAIN\Aux2DPS	(Drift freq, progsched by dispatcher)
D:\Logfiles	(Apache, FTP, Firewall)
D:\Miscellaneous	
D:\NTP	(NTP Service for GPS communication)
D:\Secure\Diagnostics	(BIT, CEQ, DCART logs)
D:\Secure\Incoming	(Dispatcher remote commanding)
D:\Secure\IndividualFiles	(Temp location for all data)
D:\Public	(Short & long term storage)
D:\tftpboot	(Location of DESC os image)
D:\WWW\Docs	(Main Web server document root)
D:\WWW\IonoGIF.secure	(Ionogram pictures)
D:\WWW\SkyGIF.secure	(Skymap pictures)

Microsoft Security Policy

- Additional security settings can be adjusted via Microsoft operating system related policies.
- Local Security Policy
- User Rights
- Auditing, etc
- mmc (Microsoft Management Console)
- Please adjust security policy settings carefully and test system with new settings
- Should people upgrade their brow

Remote Access

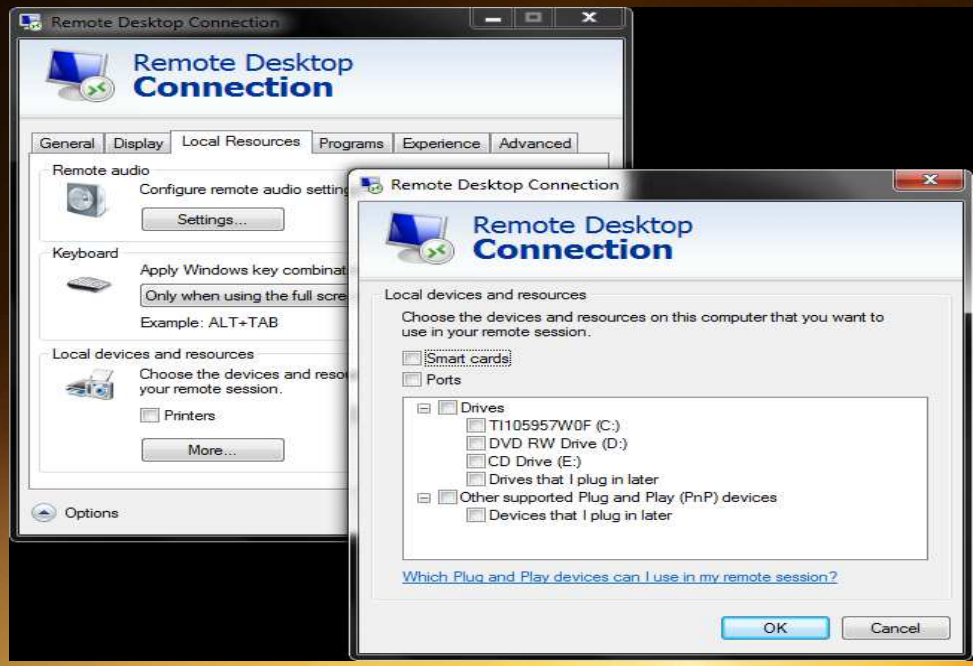
- Microsoft Remote Desktop
  - Direct control of the system
  - Complete control of DCART
    - Run / Create Programs, Run / Create Schedules
  - Hard drive access (configuration files, logs, Windows settings, etc)
- FTP Server (IIS)
  - Secondary control mechanism available if necessary
  - Allows upload and download of data and system configuration files.
- SFTP Server (not included)
  - More secure file transfer than FTP
  - Also provides shell (console) access
- Web Page (Apache)
  - Data Displays
  - Access to some system logs and reporting

Microsoft Remote Desktop

- Included on any version of Windows XP sp2, Vista, or Windows 7
- Provides client with full control over Windows
- Locks the local terminal, you cannot share the desktop with a local user
- Requires high speed connection
- Remote Desktop Connection Notes
  - Be wary of using local devices and resources
  - Adjust settings to make best use of available bandwidth
  - Care should be taken when “shutting down”

Microsoft RDP Client Settings

- Recommend to minimize “Experience” to improve client performance.
- Disable “Local devices and resources”.
- If local devices are not disabled the client will attempt to install device drivers on the Data Computer, and possibly cause extreme system slowdown.



FTP Access

- Low bandwidth connection
- Serves as an alternative to Remote Desktop regarding system access
- Provides access to D partition, UMLCAR software configuration, and system data
- Is provided on the Digisonde 4D via Microsoft IIS (Internet Information System)
- Inherently insecure
  - Passwords sent “in the clear”
- IIS can be disabled if desired
- Can be replaced by SFTP server (not included)

Web Page

- Provides quick browsing of recent data
  - Ionogram latest and history
  - Skymap latest and history
- DCART Screen Output
  - Communication errors with DESC
  - Bad data packets received
  - Report program run (and success)
  - Termination of program
  - Miscellaneous
- Dispatcher Screen Output
  - Report which data is being processed
  - ARTIST 5 scaling, other processing, and results
  - Picture generation
  - data delivery reports
  - Housecleaning (cleaning directories and drive space warnings)
- Latest System Status (BIT)
  - Latest BIT Report

Web Page Administration

- Apache Web Server does not use Windows Authentication
- D:\Apache\etc\users, groups are used for login
- D:\Apache\bin\htpasswd.exe for setting passwords and creating users
- D:\Apache\conf\httpd.conf for server configuration

Example D:\Apache\etc\users file

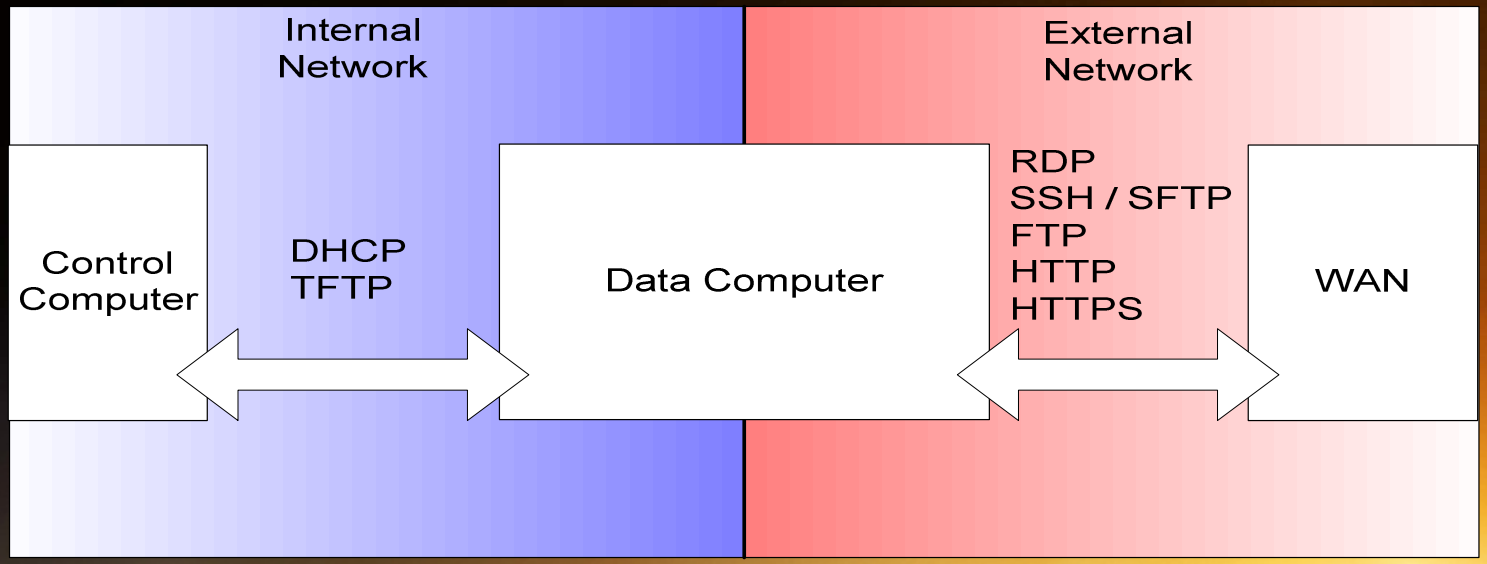
joint:$apr1$4n1MLIRD$I.zTmRUIGBD0tqggKXdkL/
umleng:$apr1$tuHt3RLN$iMTY8alJINl./KXsscBp4/
DPS4D-admin:$apr1$JQ3dazAQ$U4zpm12CsB0Ocv7FVG45A.

Control and Data Computer Boot Sequence

- Data & Control Computers POST
- Data Computer loads Windows and Starts Dispatcher, DCART, and Network Services (DHCP / TFTP)
- While Data Computer loads Windows the Control Computer DHCP process times out and resets.
- Control Computer requests IP via DHCP
- Control Computer requests os image via TFTP
- Control Computer loads DESC image
- Control Computer DESC listens for connections
- Data Computer DCART connects to Control Computer DESC
- Start Operations

Network Services Diagram

- Network Services by Interface



Routine Outgoing Network Traffic
Data Delivery

- FTP delivery
- D:\Dispatch\FTPS.exe
  - UMLCAR custom FTP client
- Dispatcher processes the raw data, generates a script file processed by the FTP client to deliver data
- Passwords for access in D:\Buffers\FTPx\System\account.ftp