Deploying Director's Station Part II Jumping Through Firewalls

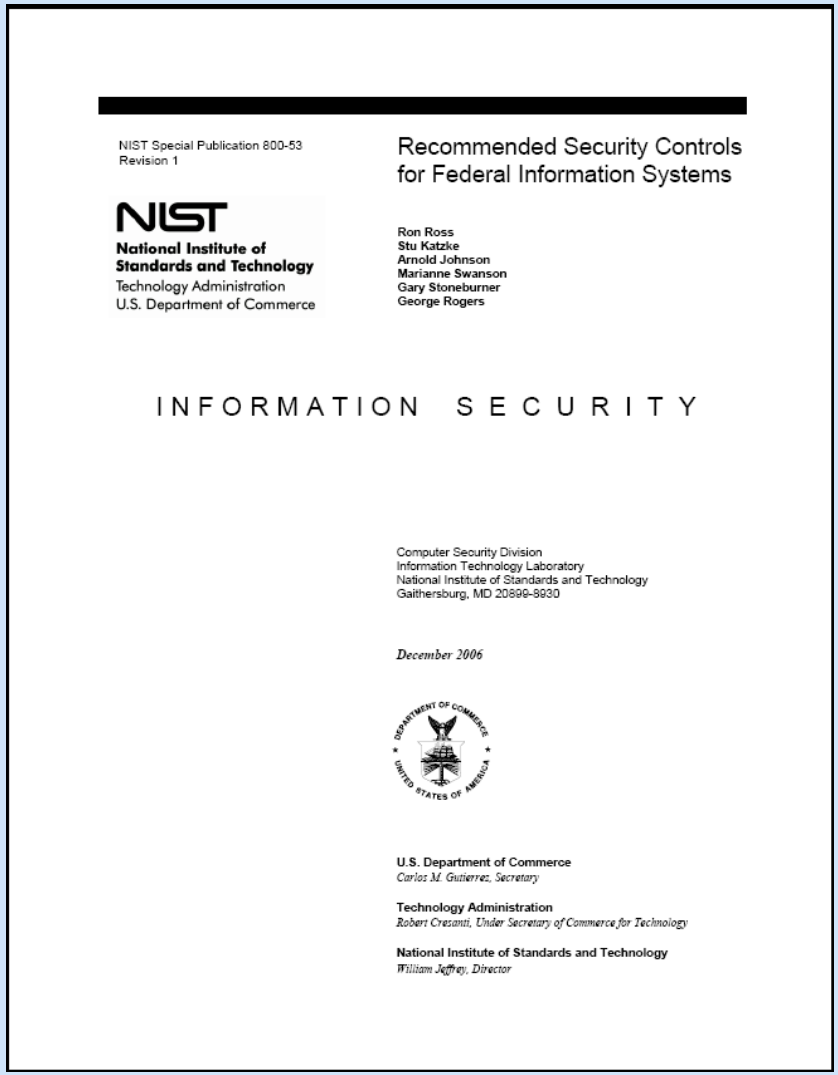
Paula Deutsch

February 20, 2006

Or…

How We Resolved The Security Issues Inherent In The Delivered Method For Supplying Director's Station With Unicorn Data

NIST has a few thoughts about cybersecurity



NIST Special Publication 800-53
Revision 1

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Recommended Security Controls for Federal Information Systems

Ron Ross
Stu Katzke
Arnold Johnson
Marianne Swanson
Gary Stoneburner
George Rogers

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

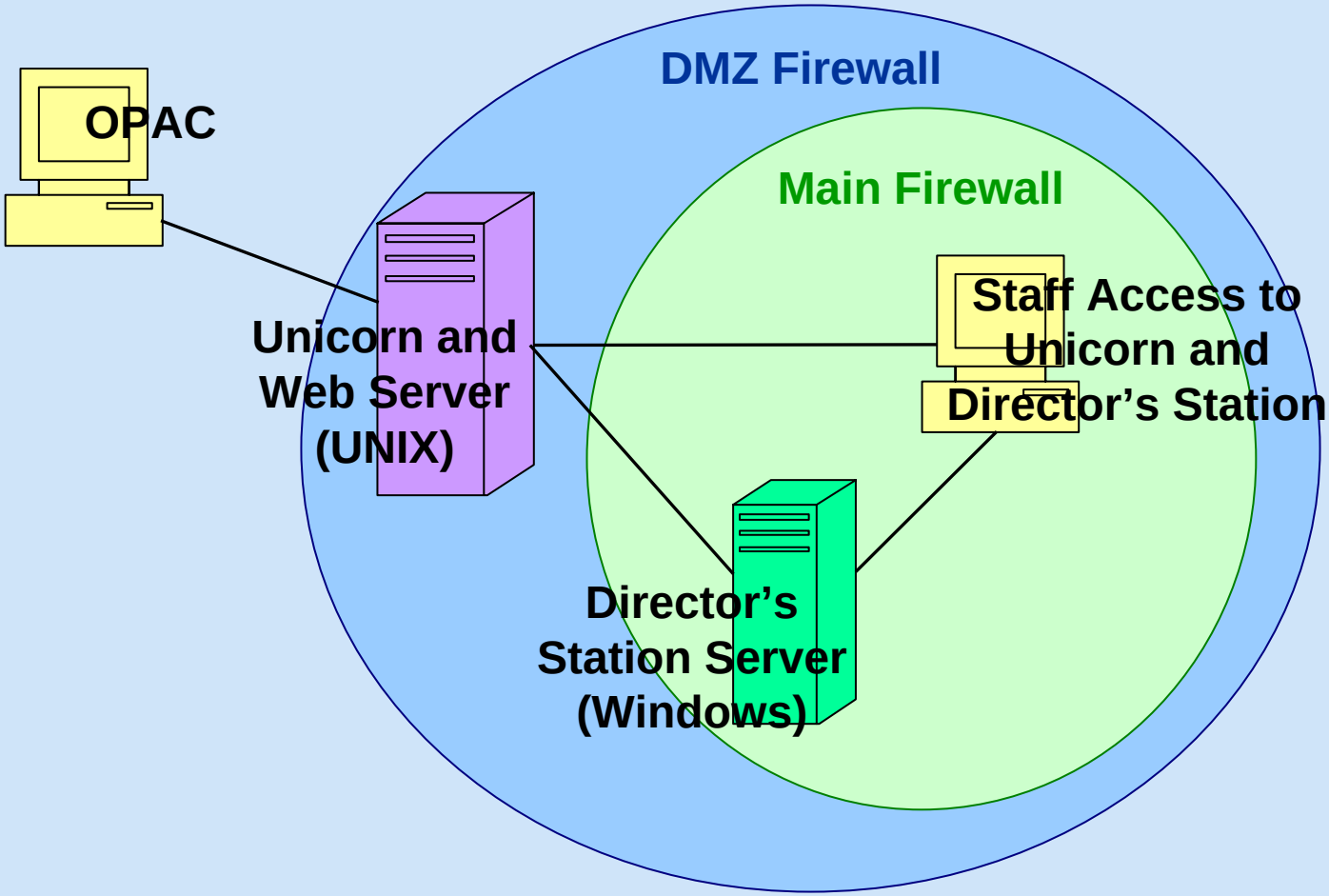
December 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

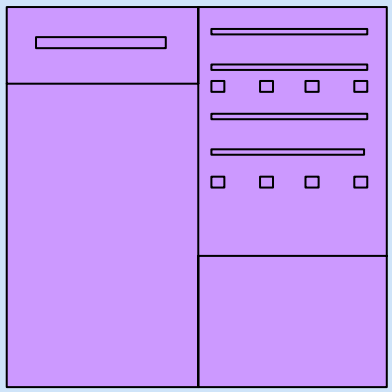
Technology Administration
Robert Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
William Jeffrey, Director

Our Set Up

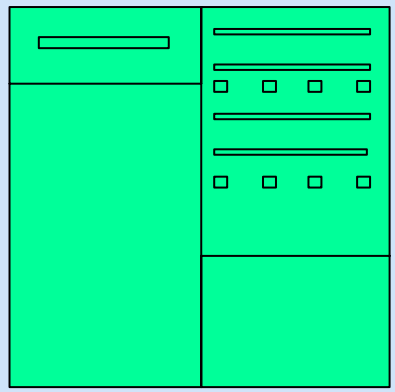

DMZ Firewall
Main Firewall
OPAC
Unicorn and Web Server (UNIX)
Staff Access to Unicorn and Director's Station
Director's Station Server (Windows)

Delivered Procedure For Data Exchange



Unicorn server runs Data Interchange reports nightly

Unicorn server pushes data out to Director's Station Server (using ftp)



Director's Station server crunches the data

The Problem: Unacceptable Security Risks

- NIST CIO does not allow an open ftp port on systems in the DMZ (ftp sends unencrypted passwords across the network).
- NIST CIO does not allow systems in the DMZ to push data through the firewall.

The Solution

Recipe for: Secure Data Transfer

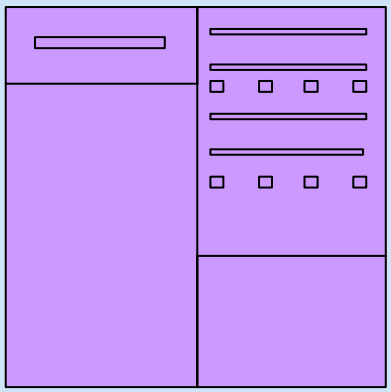
Ingredients:

UNIX cron job utility
PuTTY Utilities (open source)
WinSCP (open source)
Windows Scheduled Tasks utility

Directions:

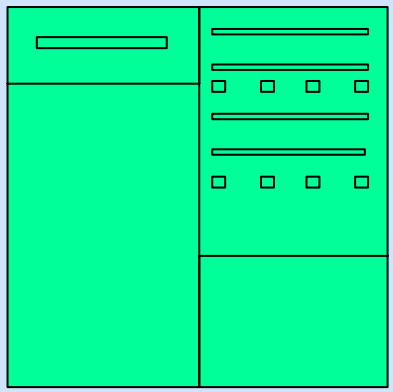
Combine all ingredients and add scripts to taste.

Modified Procedure For Data Exchange



Unicorn server runs “data interchange” reports nightly

Director’s Station server **pulls** data from Unicorn Server (using scp)



Director’s Station server crunches the data

The Process

Data Interchange report runs on Unicorn server and delivers data to a directory on Unicorn	Cron job changes permissions on files	Director's Station logs onto Unicorn server and picks up files	Director's Station server runs DTS for data crunching
1:15 am	2:15 am	2:45 am	8:00 pm

TIME LINE

Changes Made To Delivered Data Interchange Report

- Modified by SirsiDynix Director's Station implementation team.
- Files are placed in Director's Station directory on Unicorn server (/s/sirsi/DirStation) instead of being sent to Director's Station server by ftp.

Establish Connectivity Between Unicorn and Director's Station Servers

1. Create Director's Station account on Unicorn server.
2. Create UNIX cron job to change permissions on data files to allow Director's Station user to download them.
3. Set up matching keys that will allow Director's Station to log in to Unicorn server automatically.

1. Create New User Account on Unicorn

Create Director's Station account on Unicorn server:

Belongs to "staff" group which owns no files on Unicorn server. Therefore only has "other" permissions to all files.

2. Create Cron Job on Unicorn Server

In order for the Director's Station user to copy some of the files generated by the Data Interchange report, permissions on those files must be changed.

-rw------- sirsi staff

Needs to be changed to:

-rw-r--r-- sirsi staff

Creating the Cron Job

A. Write a script that will change file permissions.

B. Schedule the script to run automatically.

A. Script To Change File Permissions

/a/sirsi/DirStation/allow_data_transfer

```
#! /bin/bash

# allow_data_transfer created by Paula Deutsch 8/20/2006
# This script changes permissions on the data files so that
# Director's Station's user can copy them.

cd /s/sirsi/DirStation
chmod -R g+r,o+r Data
chmod -R g+r,o+r Histlog
chmod -R g+r,o+r Ved
chmod -R g+r,o+r WLS
```

B. Use Cron Job Utility to Automate

- %>crontab
- 15 2 * * 1-5 /a/sirsi/DirStation/allow_data_transfer > /dev/null 2>&1
- CONTROL D

Syntax: *minute hour day-of-month month-of-year day-of-week-(Sunday = 0) script redirect-output-(to "bit bucket")*

3. Generate Public and Private Keys

- PuTTYgen can be used to create matching public and private keys.
- Open source software.
- Available from:

  http://www.chiark.greenend.org.uk/~sgtatham/putty/
- Demo

Download Data Files From Unicorn To Director's Station

1. Install a secure copy (scp) utility to pull files from Unicorn and place them in the appropriate directories on Director's Station.
2. Create script for automated downloading.
3. Use Windows Scheduled Task utility to run script nightly.

1. Secure Copy Utility: WinSCP

- WinSCP can be used to automatically download files.
- Open source software.
- Available from:

  http://winscp.net/eng/index.php

2. Script Automated Downloads

Set up environment and connection:

library.txt connects to Unicorn as Director's Station user and #copies data files

Automatically answer all prompts negatively to avoid stalling #the script on errors

option batch on

Disable overwrite confirmations

option confirm off

Connect

open *Director's Station user name@Unicorn server address*

Download text files:

```
# Set to ascii mode
option transfer ascii
# Download files from DirStation/Data into d:\sirsi\ExpData
get /a/sirsi/DirStation/Data/*.txt d:\sirsi\ExpData\
# Download files from DirStation/Ved into d:\sirsi\DSVed
get /a/sirsi/DirStation/Ved/catalog d:\sirsi\DSVed\
get /a/sirsi/DirStation/Ved/desc d:\sirsi\DSVed\
get /a/sirsi/DirStation/Ved/zipcode d:\sirsi\DSVed\
get /a/sirsi/DirStation/Ved/policies d:\sirsi\Policies\
get /a/sirsi/DirStation/Ved/strings.pol d:\sirsi\Policies\
```

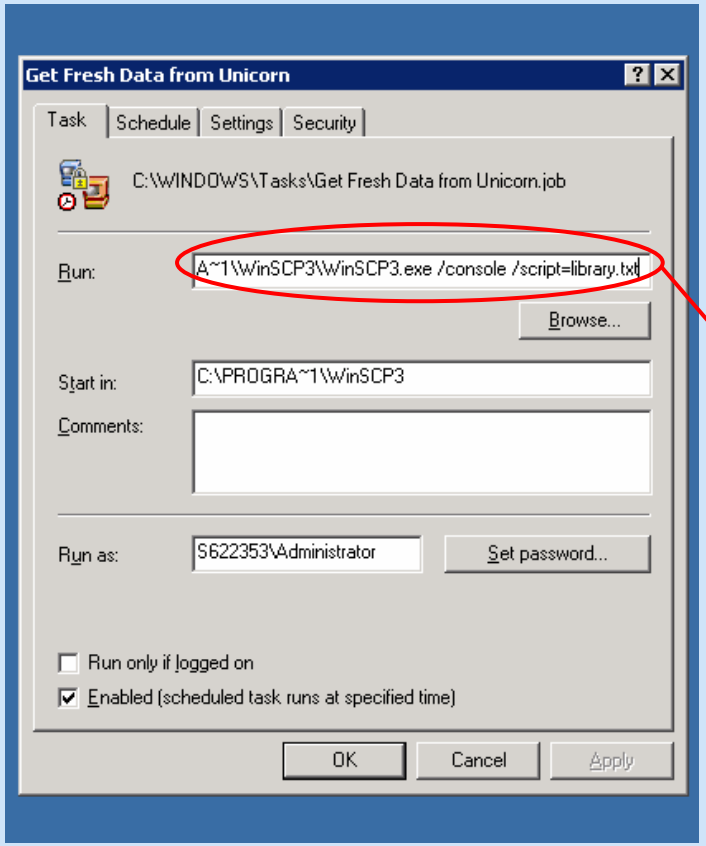
Download compressed files:

```
# Set to binary mode
option transfer binary
# Download files from /a/sirsi/DirStation/Histlog/ to
# d:\sirsi\Histlog
get /a/sirsi/DirStation/Histlog/*.Z d:\sirsi\Histlog\
# Download files from /a/sirsi/DirStation/WLS/ to
# d:\sirsi\Weblog\WLS
get /a/sirsi/DirStation/WLS/*.weblog.Z
d:\sirsi\Weblog\WLS\
```

End session:

```
# Disconnect
close
# Exit WinSCP
exit
```

3. Create Scheduled Task on Director's Station



C:\PROGRA~1\WinSCP3\WinSCP3.exe /console /script=library.txt

Success!

This has enabled us to automate the refreshing of data on Director's Station while keeping peace with the CIO.

Hopefully others can make use of this process.

Thank You

Questions?

paula.deutsch@nist.gov