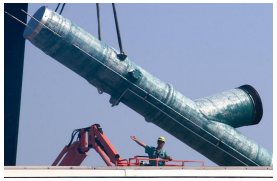
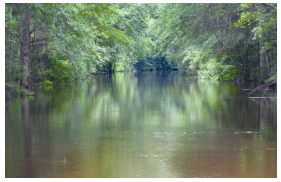
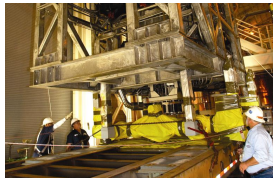
Securing the Laboratory Network

Rob Clark
Senior Engineer
Washington Savannah River Company
October 18, 2006

Securing the Laboratory Network

Background

- **Savannah River Site is a Department of Energy Facility**
- **Located in Aiken, SC**
- **Primary work is environmental restoration**
- **Multiple laboratories across the Site**
  - **Ranging from large to small labs doing a variety of work**

Securing the Laboratory Network

Risks

- **Computer Security Concerns**
- **Worried about electronic eavesdropping**
- **Disruption of Site Network**
- **Eliminate Clear Text Protocols – FTP and Telnet**
- **Use encrypted protocols - Windows shares, sFTP, SSH**

Telnet

- **Telnet – terminal emulation program**
- **Primarily used with legacy systems**
- **Logon is in plain text – accounts and passwords**
- **Data screens are in plain text**

FTP

- **File Transfer Protocol**
- **Send files to a server**
- **Receive files from a server**
- **Logon is in plain text – accounts and passwords**
- **Particularly useful in scripts**
- **Transfer data files from instrument computer to the server**

Securing the Laboratory Network

ICP's (EM)

- **Lab has two ICP's – Perkin Elmer Optima 3000 XL, and Optima 4300 DV**
- **Processes 500 analyses per year**

Workflow –

Log samples in LIMS

Run the analysis on the instrument

Copy the data file to predefined directory

A LimsLink method parses the data file

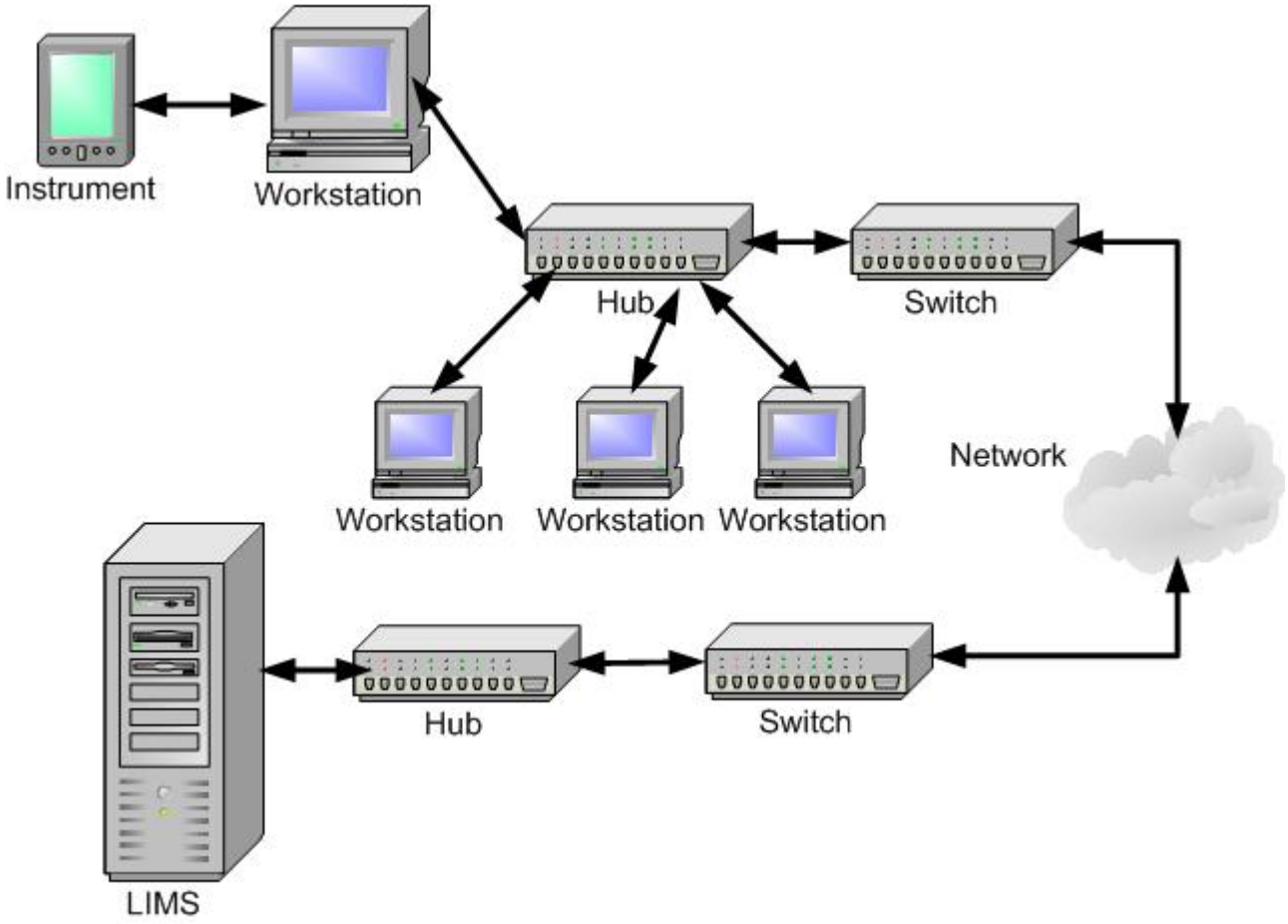
Technician reviews, edits

Technician sends results to LIMS.

Results available in LIMS

Securing the Laboratory Network

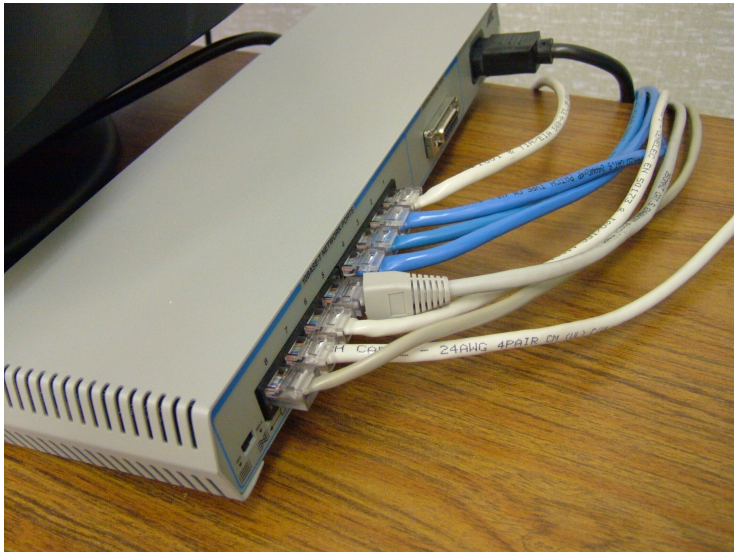
Laboratory Network



Securing the Laboratory Network

Hub

- **Network Hub**
- **Multiple computers share one line**
- **Network segment**
- **Can be daisy-chained**
- **Data is broadcasted to all computers on hub**



Securing the Laboratory Network

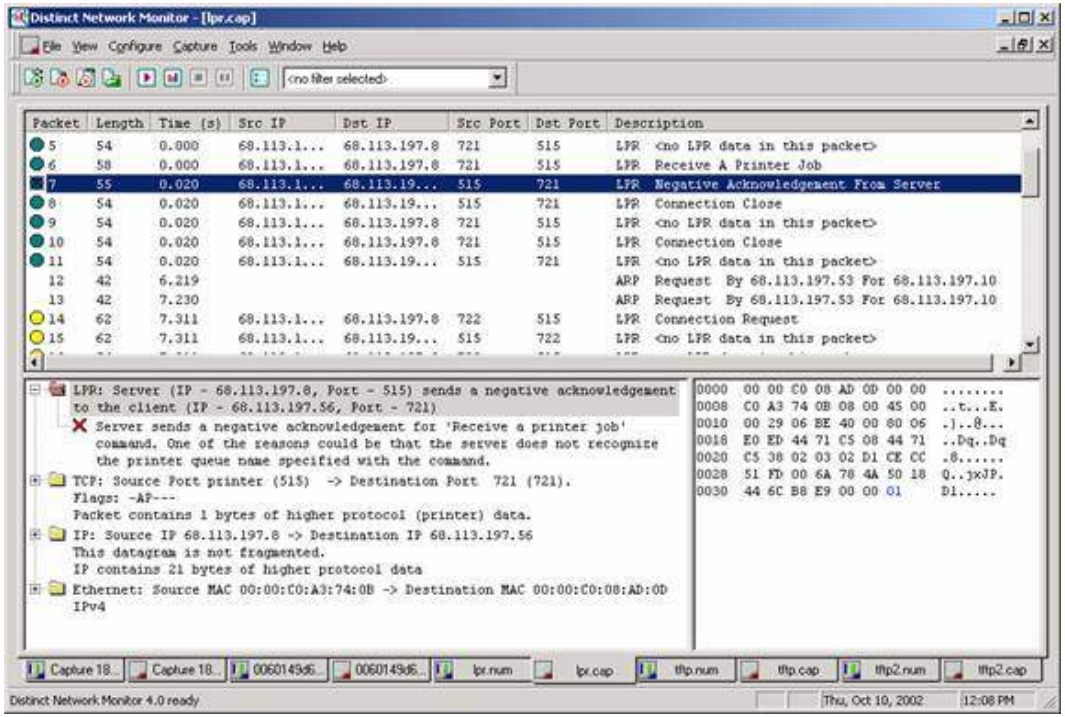
Hub

- **Every network device has a unique address**
- **MAC address – preset at the factory for every network card**
- **Usually, a TCP/IP address**
- **Normal operation – device only pays attention to messages addressed to the itself**

Securing the Laboratory Network

Network Sniffer

- **Used for network maintenance and troubleshooting**
- **Laptop computer**
- **Ethernet card in "promiscuous" mode – listens to all traffic**
- **Displays all data, including accounts and passwords**
- **Can be programmed to trigger on specific events**



Securing the Laboratory Network

Encryption

- **Encrypt data before sending it across network**
- **Decrypt it after receiving it**
- **Does increase overhead, but fast enough to not be a problem**
- **Typically uses public key encryption – key pairs based on very large prime numbers**
- **Difficult for casual users to break**

Securing the Laboratory Network

Windows Shares

- **Windows domain networks – shared drive on server**
- **Looks like a local drive on the instrument computer**
- **Supports IPSec TCP/IP data encryption standard *or***
- **Kerberos network authentication protocol**
- **Activated by administrator of Windows .NET or 2000 Server**
- **Transparent to end users**
- **Preferred for all-Windows networks**

Securing the Laboratory Network

Windows Shares

- **Supports IPSec TCP/IP data encryption standard**
- **Transforms data packets before sending, adds security data to packets**
- **Uses Internet Key Exchange (IKE) for key management**

Securing the Laboratory Network

SSH

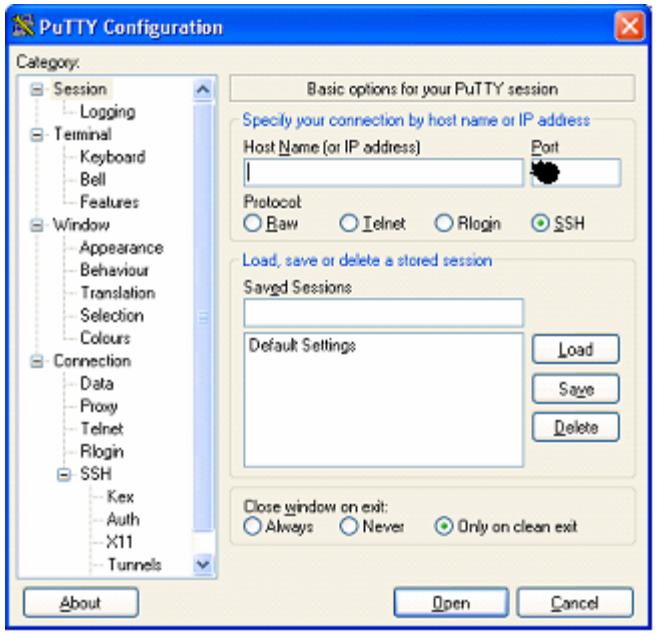
- **Secure Shell (SSH)**
- **Encrypted replacement for Telnet**
- **Originally developed for UNIX**
- **Requires component on server and PC**
- **Two versions – SSH1 and SSH2**
- **SSH2 is preferred**

Securing the Laboratory Network

SSH Client

- **PuTTY – free client software**
- **Open source under MIT license**
- **Download from http://www.chiark.greenend.org.uk/~sgtatham/putty/**
- **For Windows or Unix**
- **Available at SRS from WinInstall**

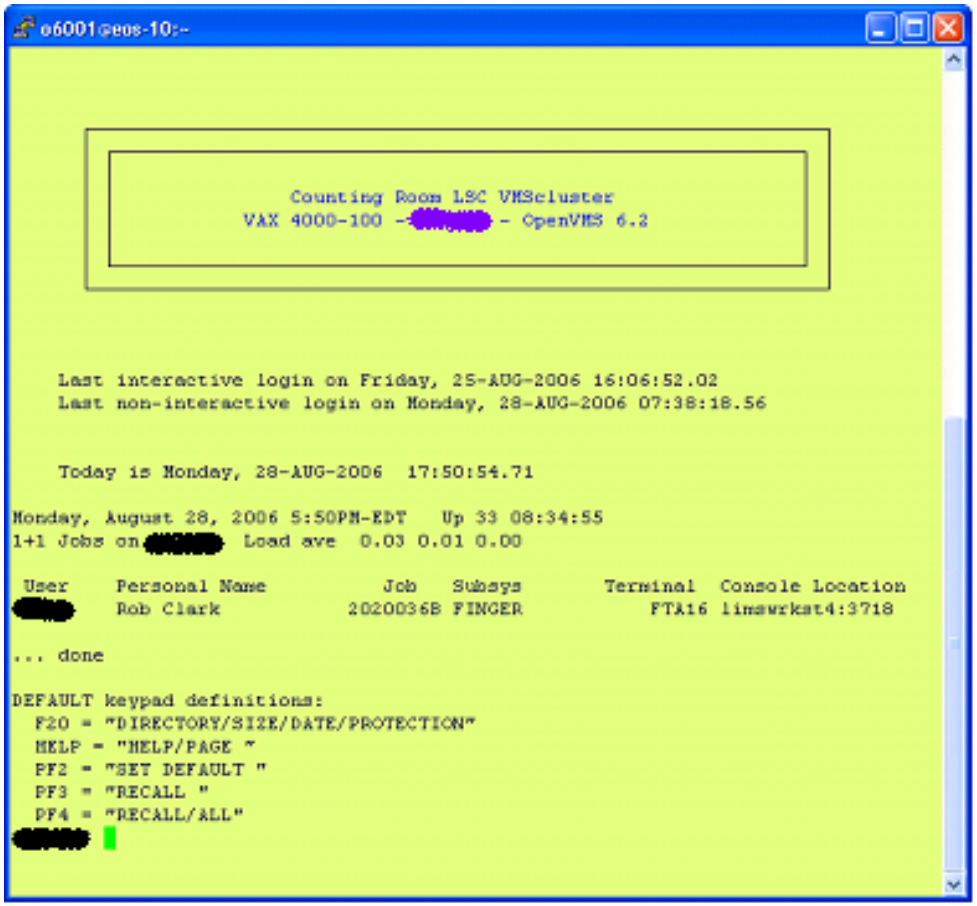
- **Enter the computer name in the Host Name field**
- **Click the Open button**
- **For the first connection only, it will ask if you want to accept key from server.**



Securing the Laboratory Network

SSH Client

- **Log on with user name and password**
- **Default colors for foreground, background, bold are configurable**
- ***CANNOT* set up DEC keys like HELP, DO, F12**



Securing the Laboratory Network

SSH Host

- **Very easy on Unix/Linux – from root account, enable service and generate keys (ssh keygen)**
- **For VMS systems - included in DEC TCP/IP Services, Multinet 4.3 or higher**
- **SSH daemon or detached process handles sFTP also**
- **Multinet – patches needed in version 4.x**

SSH Installation - VMS

- **Log on using system account, start configuration**

  $ multinet configure /serv

  MultiNet Server Configuration Utility V4.4(42)

  [Reading in configuration from MULTINET:SERVICES.MASTER_SERVER]

- **Enable the service**

  > enable SSH

  > Exit

- **Define logicals and generate keys**

  $define multinet_ssh2_hostkey_dir –

  _$ multinet_specific_root:[multinet.ssh2.hostkeys]

  $multinet sshkeygen /ssh2 /host

  -- generates 1024 bit DSA keys. Creates file HOSTKEY. Owned by SYSTEM, only readable by system
  HOSTKEY.PUB world readable, editable only by system

  $ copy multinet_specific_root:[Multinet.ssh2]sshd2_config.template –

  _$ multinet_specific_root:[Multinet.ssh2]sshd2_config.

- **Restart Multinet**

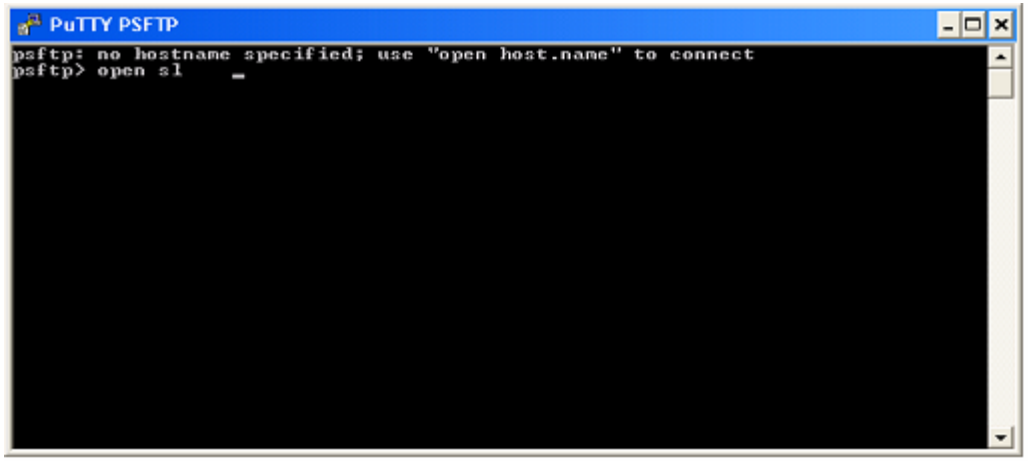
  $ @multinet:start_server restart

- **Option – Autologin**
- **Uses client's security to validate user**
- **Not recommended**

Securing the Laboratory Network

sFTP Client

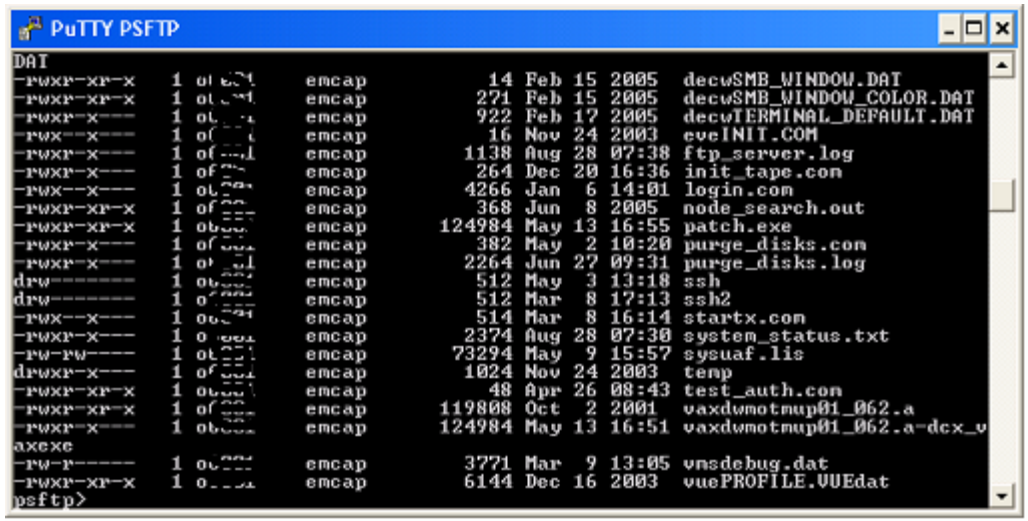
- **PuTTY – free client software**
- **sFTP command line only**
- **Transfer files between PC and server**
- **Can be used in scripts (investigate Plink)**
- **Start the DOS command prompt**



Securing the Laboratory Network

sFTP Client

- **Converts VMS directories to Unix appearance**
- **Uses Unix commands (ls, cd) or dir**
- **Similar to FTP, but…**



sFTP Client

- **sFTP – binary mode transfers only**
- **get and put commands, but no mget or mput**
- **Scripts will need to be revised to use it.**
- **VMS to VMS only – Multinet takes care of file characteristics automatically, preserves file structure**

Securing the Laboratory Network

Disabling FTP and Telnet

- **Test and make sure lab processes run before turning off Telnet and FTP**
- **Make backups**
- **Multinet Commands:**
  $ multinet configure /serv

```
MultiNet Server Configuration Utility V4.4(42)
[Reading in configuration from MULTINET:SERVICES.MASTER_SERVER]
> disable ftp
> disable telnet
> show ssh /full
> exit

$ @multinet:start_server restart
```

Securing the Laboratory Network

Conclusion

- **Encrypted protocols prevent snooping**
- **Planning is essential**
- **Software installation and configuration needed**
- **Some script modifications required**
- **Use Windows File sharing if possible**
- **Test and verify**