



Computer Security

Ryan Hamel

University of Massachusetts Lowell
Environmental, Earth, & Atmospheric Sciences Department
Center for Atmospheric Research

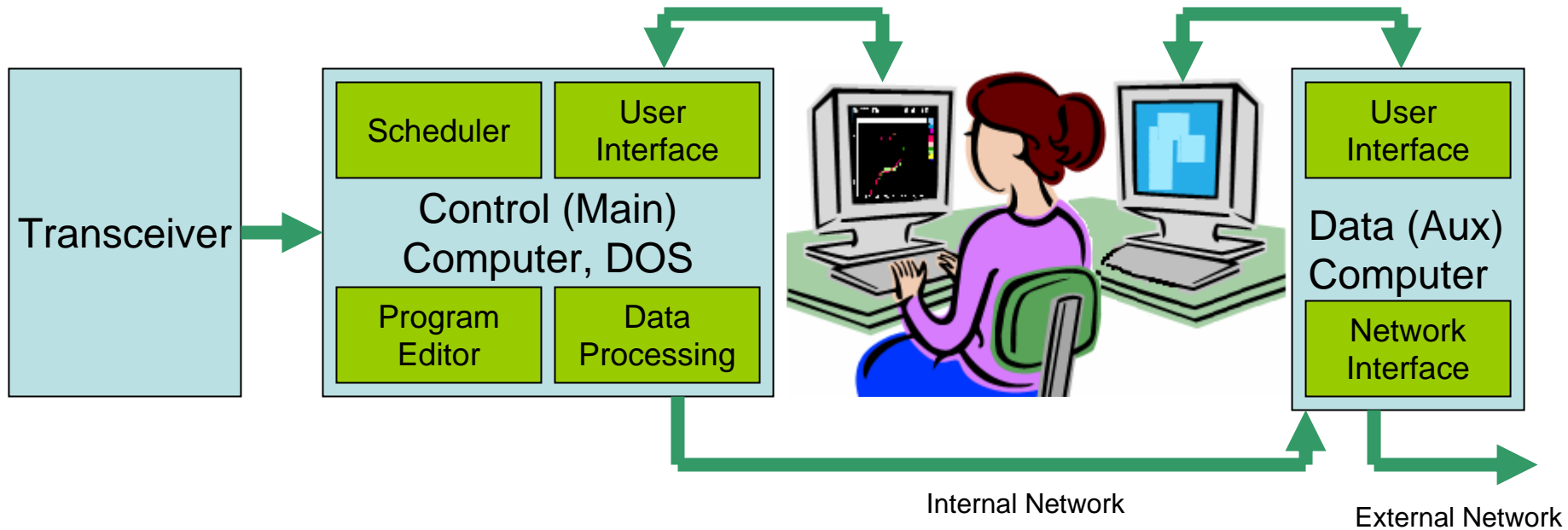


XI INTERNATIONAL DIGISONDE FORUM
30 APRIL TO 3 MAY 2007

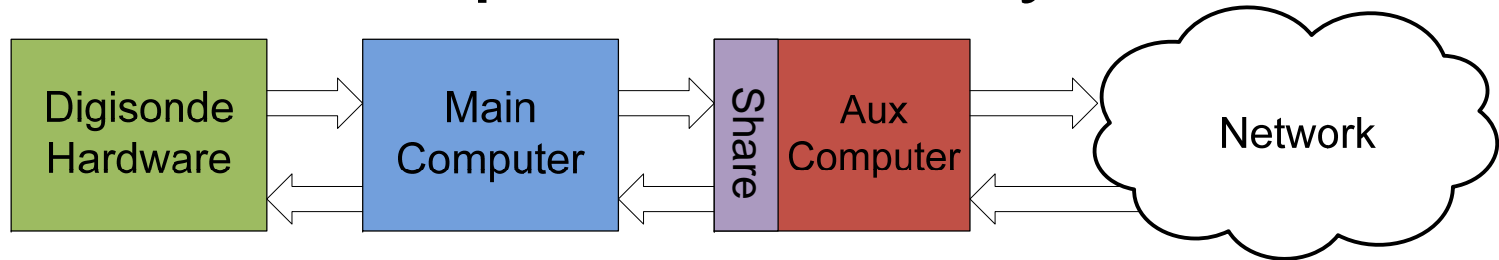
Positives and Negatives of the Internet

- Allows easy data dissemination
- Provides access to “near real time” data in the form of pictures available to the public
- Remote operation / troubleshooting
- Denial of Services
- Loss of data
- System down time
- Too much protection negates the benefits of the internet

Digisonde Data Path Block Diagram



Main Computer Security Concerns



- Limited network connectivity (NetBIOS only)
- File sharing system is used for “communication” between systems
- Requires Aux computer to be compromised
- No way to access “shares” on the Main computer system
- Requires detailed knowledge of Main computer function

Aux Computer Security Concerns

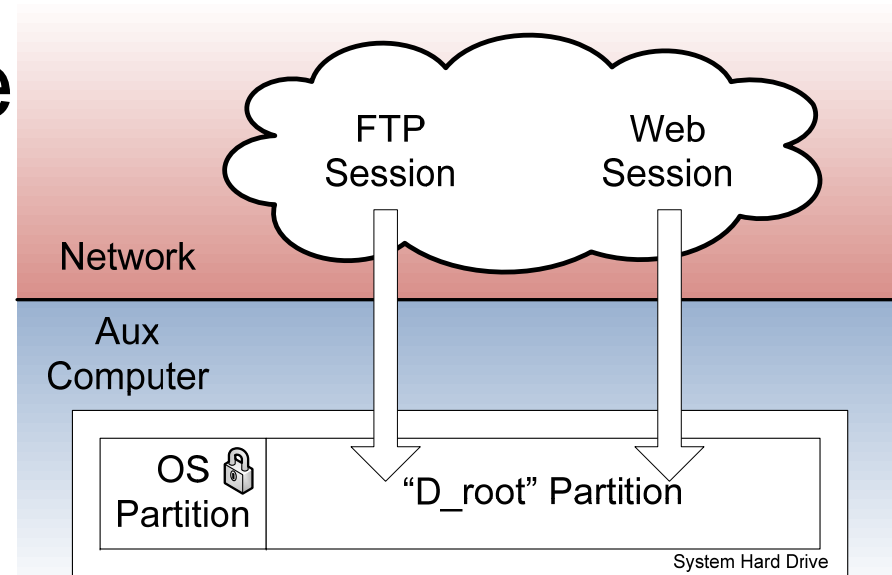
- Uses a modern operating system, an accessible / familiar operating system
- Usually sits on a network connected to the Internet
- Network services provide potential points for attack
- The Aux Computer is usually automated and doesn't function as a workstation
- The focus of this talk

Aux Computer Security Measures

- Partition structure
- Eliminate unnecessary protocols from network devices
- Users
- Event Log / Log files
- Auditing
- Antivirus
- Windows Update
- Firewalls

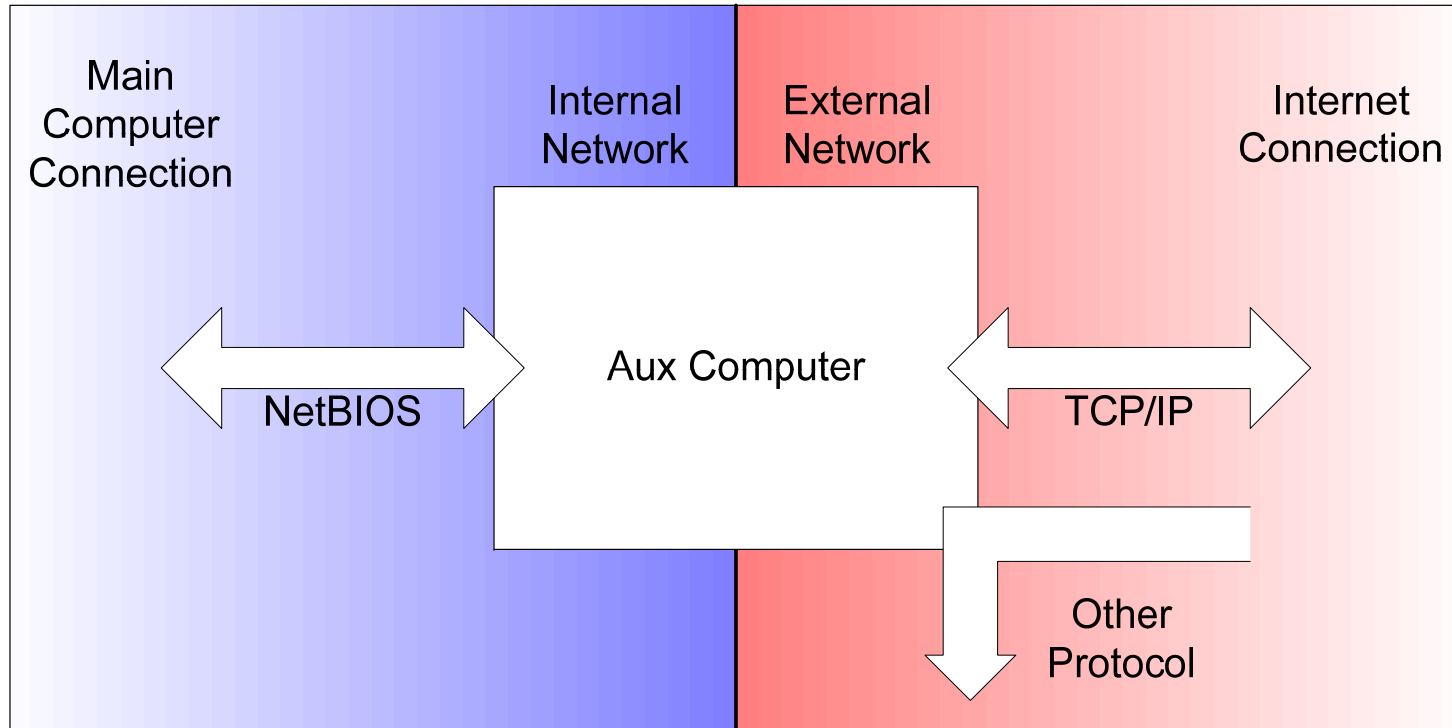
Partition Structure

- The operating system partition is segregated from the partition accessible from the internet
- Network services allow access only to the non operating system partition
 - FTP server allows access only to D_root partition
 - Web page contents are similarly on “working” partition
 - Use of these services does not access data on the operating system partition
- Could result in loss of data / software of the D_root
- “Non critical” loss of data



Eliminate Unused Protocols

- External Network uses TCP/IP
- Internal Network uses NetBIOS
- Reducing Protocols reduces services one can provide



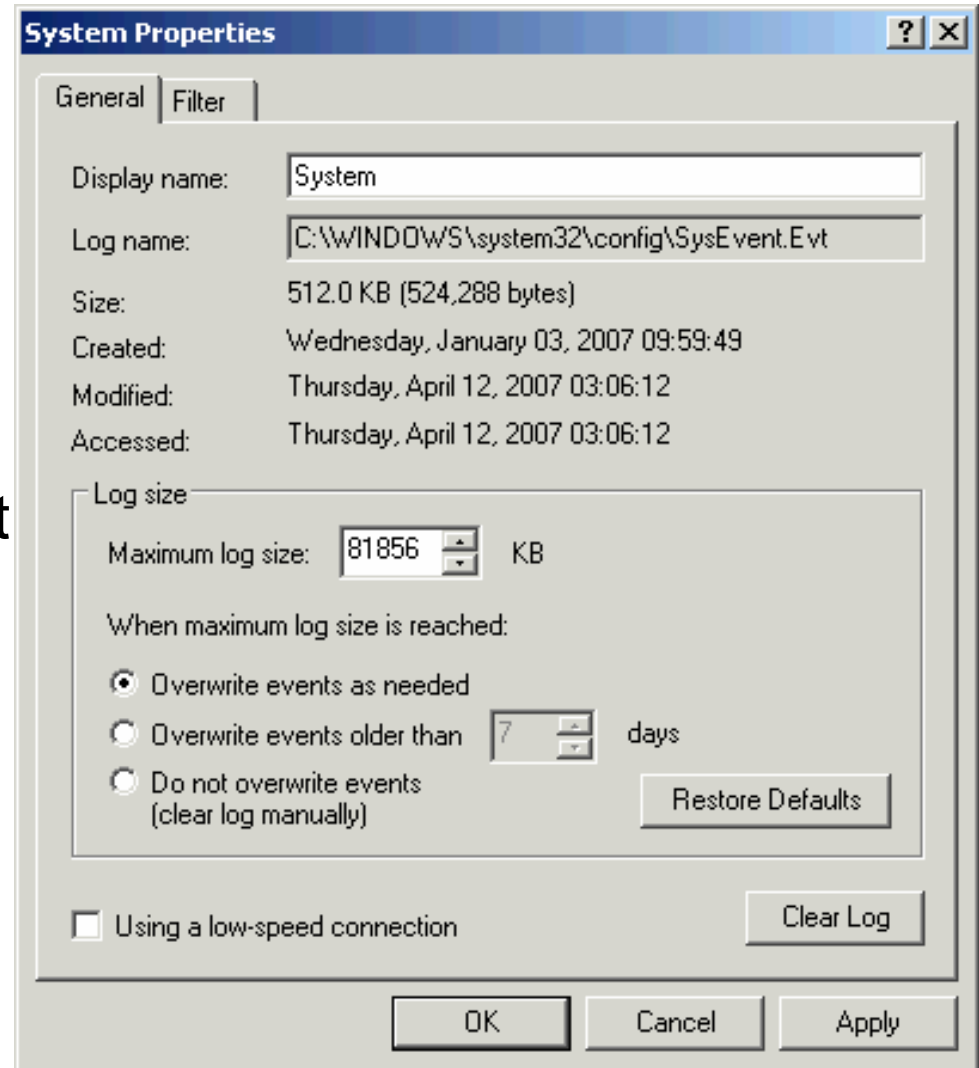
User Accounts

- Users
 - Limit number of system users
 - Rename built in accounts (Administrator, guest)
 - XXX-admin, 2 uml administrators, DPSMAIN
 - Use “strong” passwords
 - Change passwords on some regular interval
 - Disable unused users (guest, IIS user, etc)

Event Log Properties

- Control Panel / Administrative Tools / Event Viewer; Right click / Properties
- Be familiar with event log settings for all event logs:

Application
Security (Auditing)
System

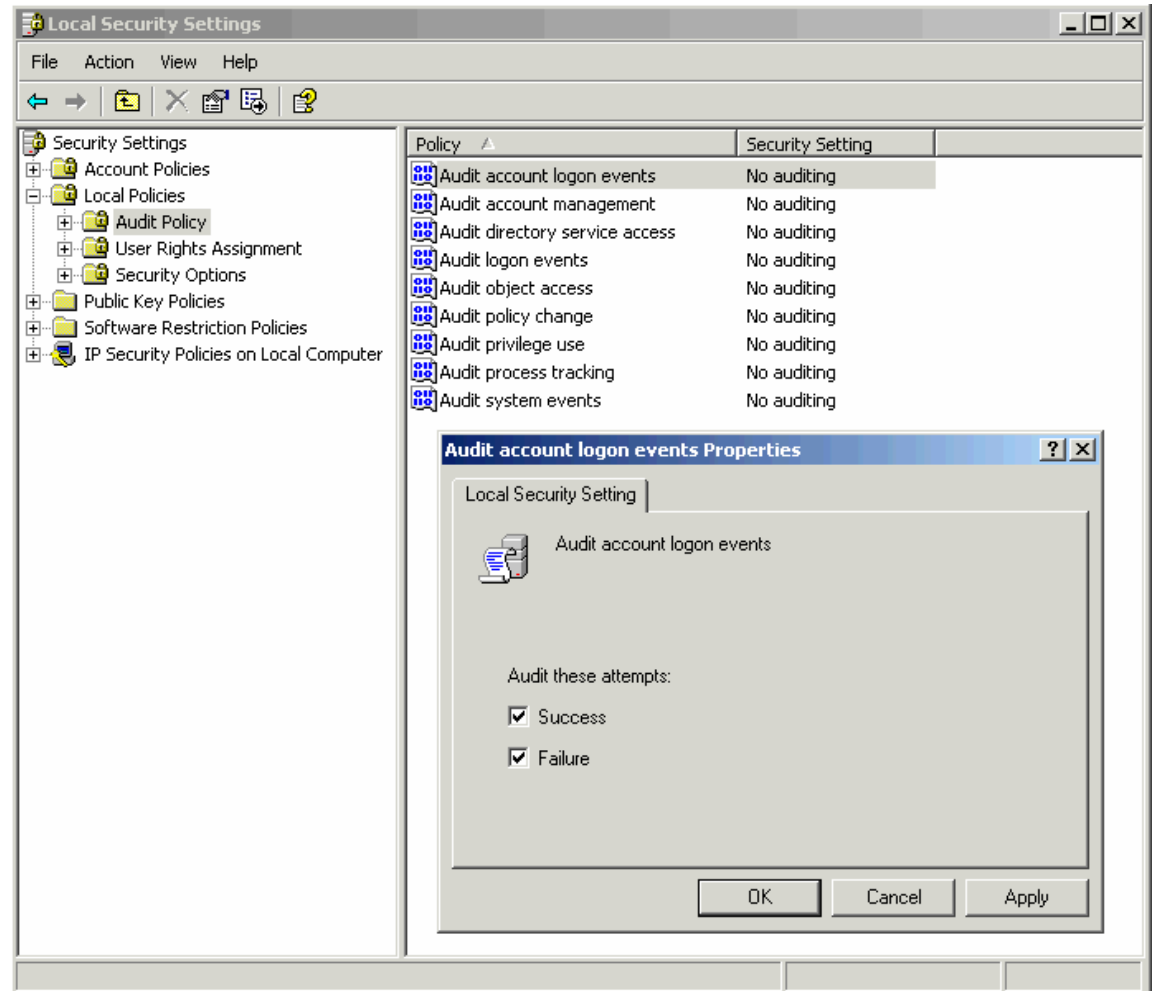


Auditing

- Powerful method for monitoring system activity
- Available in Windows 2000 and XP
- Allows custom logging (you choose)
- Auditing records are viewable from the Event Viewer / System Log

Auditing Settings

- You can choose what to audit
- Control Panel / Administrative Tools / Local Security Settings
- Audit account logon events, success and failure
- Auditing Objects can be tricky
- Beware of too much auditing



Additional Service Log Files

- Provided log files (D:\Logfiles)
 - FTP Log
 - Apache access and error logs
 - Antivirus Logs
 - Firewall Log (if you have XP)
- Log Files formats are similar in their fields.
- Look for obvious signs of malicious activity.

Antivirus

- Antivirus Software Concerns
 - For Antivirus software to be effective it must contain up to date definition files
 - Ensure the software has the ability to download updates for virus definition files
 - Ensure the antivirus is automated (scans and updates)
 - Free Antivirus
 - Avast www.avast.com

Windows Update

- Eliminates operating system vulnerabilities / exploits
- Updates should be performed on a regular basis or automated
- www.windowsupdate.com
- Updates can be uninstalled
- No updates for Windows NT

Firewalls

- A firewall is recommended
- XP service pack 2 has a built in firewall
Control Panel / Windows Firewall
- Free firewalls
 - Zone Alarm
- Usually a firewall exists at Network's edge
(network admin territory)

Firewalls

- Must be properly configured to allow services access, and access to services. Firewalls block both ways.
- Necessary Network ports that must be open for access
 - FTP:
 - 20, 21
 - Web:
 - 80
- Software that requires access to the Internet
 - D:\Dispatch\FTPS.exe
 - Antivirus Software (Main executable & Update executable)
- Shut off the firewall to troubleshoot.

Additional Helpful Tools

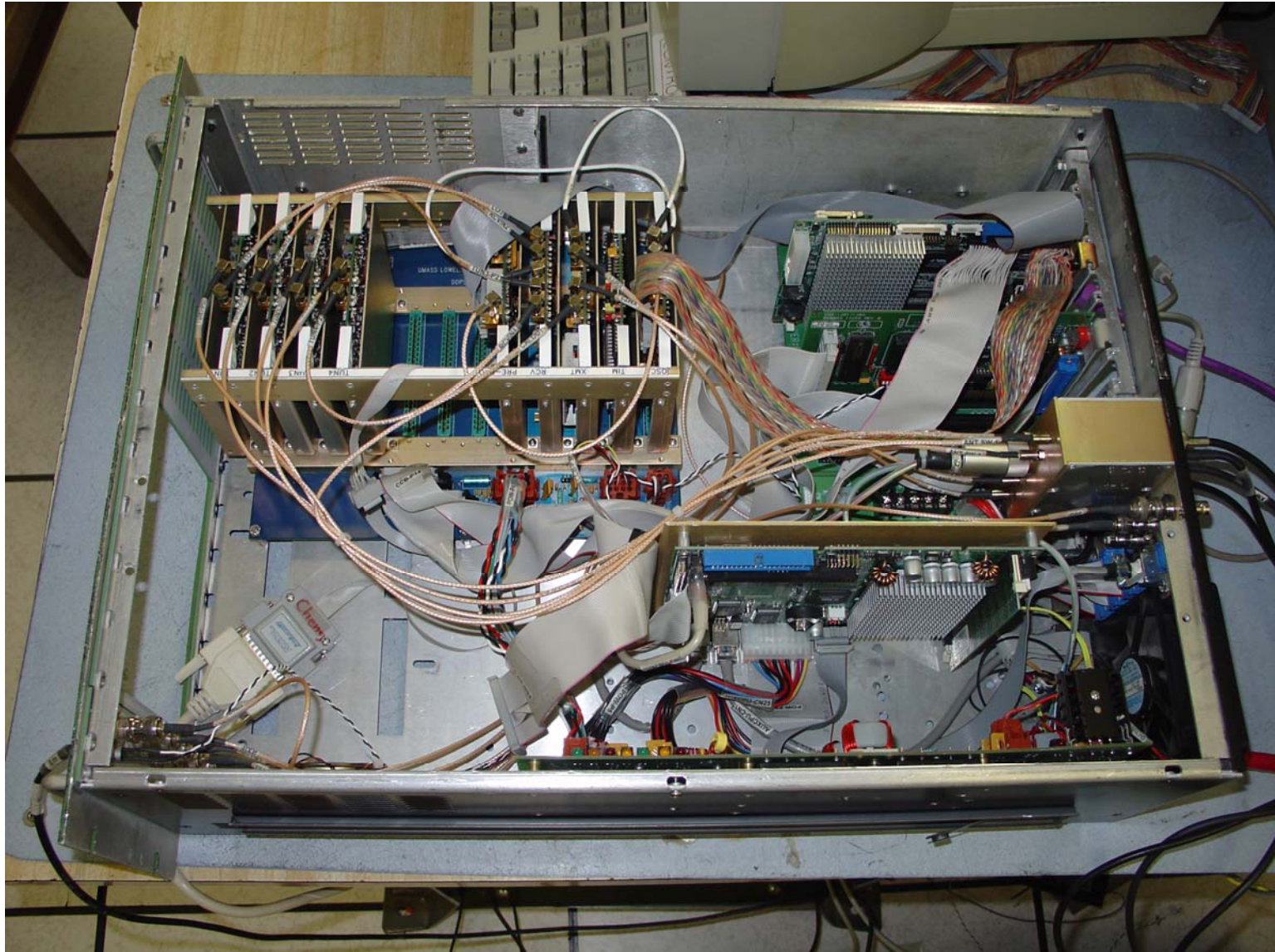
- Task Manager (Ctrl-Alt-Delete)
- Services (Control Panel / Administrative Tools / Services)
- Google for services / executables that are not familiar
- Netstat (from console: Run cmd.exe)
- Usually, investigation is required

- Contact information:
 - Ryan_Hamel@uml.edu
 - David_Kitrosser@uml.edu

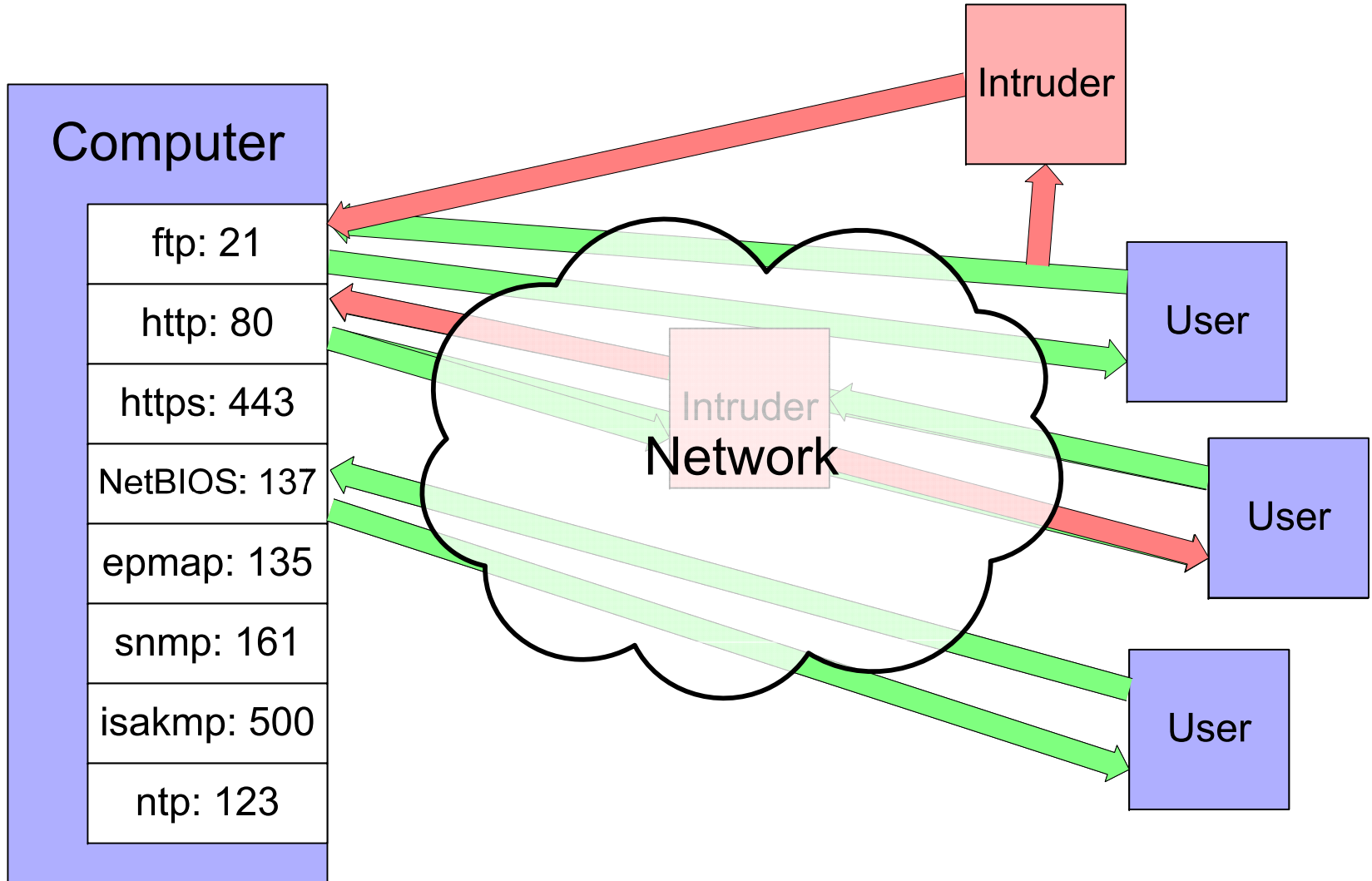
Additional Measures

- Shut down the targeted service
- Use the firewall to close network ports in question
- Use the firewall to prevent access from the attacker
- Disable the Internet network device
(unplug the system from the network)

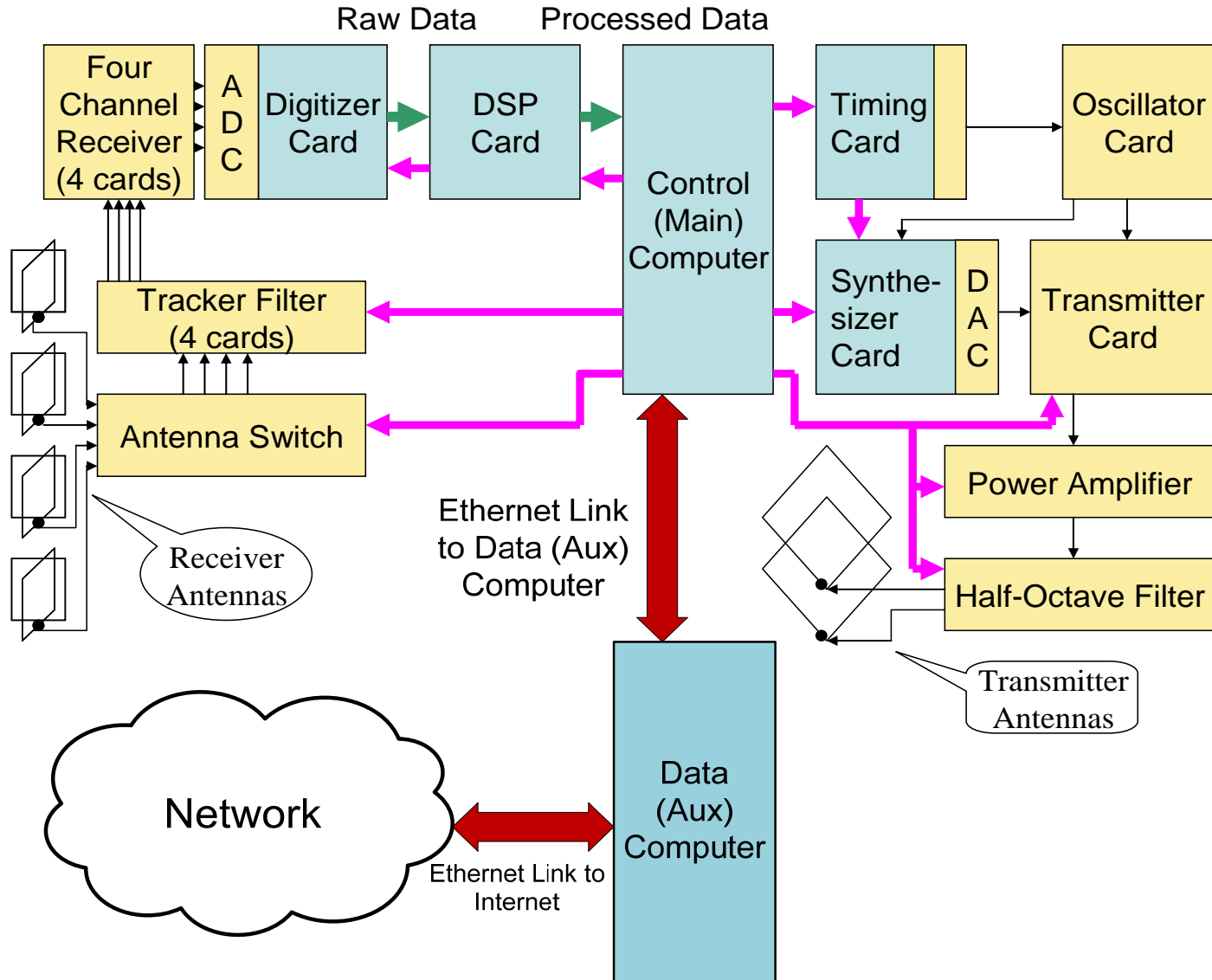
Chassis assembly



On a Network



DPS-4 Block Diagram



Apache web access log example

- 64.211.22.214 - root [08/Feb/2007:18:18:00 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - - [08/Feb/2007:18:18:01 +0000] "GET /mod_ssl:error:HTTP-request HTTP/1.0" 400 425
- 64.211.22.214 - HEWITT [08/Feb/2007:18:18:02 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - lkw [08/Feb/2007:18:18:03 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - sysadm [08/Feb/2007:18:18:05 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - - [08/Feb/2007:18:18:05 +0000] "GET /error/%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cwinnt%5cwin.ini HTTP/1.1" 404 317
- 64.211.22.214 - dhs3pms [08/Feb/2007:18:18:07 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - root [08/Feb/2007:18:18:08 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - mtcl [08/Feb/2007:18:18:10 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - mtch [08/Feb/2007:18:18:12 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - at4400 [08/Feb/2007:18:18:13 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - diag [08/Feb/2007:18:18:15 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - dhs3mt [08/Feb/2007:18:18:17 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - kermit [08/Feb/2007:18:18:18 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - admin [08/Feb/2007:18:18:20 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - halt [08/Feb/2007:18:18:22 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476
- 64.211.22.214 - install [08/Feb/2007:18:18:23 +0000] "GET //control/DCP-start.html HTTP/1.0" 401 476

sshd log example

- Apr 3 23:31:36 MahGuard sshd[22984]: Invalid user lpd from 211.137.74.58
- Apr 3 23:31:36 MahGuard sshd[22984]: Failed password for invalid user lpd from 211.137.74.58 port 59295 ssh2
- Apr 3 23:31:38 MahGuard sshd[22986]: Invalid user lpa from 211.137.74.58
- Apr 3 23:31:38 MahGuard sshd[22986]: Failed password for invalid user lpa from 211.137.74.58 port 59921 ssh2
- Apr 3 23:31:41 MahGuard sshd[22988]: Invalid user admin from 211.137.74.58
- Apr 3 23:31:41 MahGuard sshd[22988]: Failed password for invalid user admin from 211.137.74.58 port 60110 ssh2
- Apr 3 23:31:47 MahGuard sshd[22990]: Invalid user admin from 211.137.74.58
- Apr 3 23:31:47 MahGuard sshd[22990]: Failed password for invalid user admin from 211.137.74.58 port 60714 ssh2
- Apr 3 23:31:49 MahGuard sshd[22992]: Invalid user admin from 211.137.74.58
- Apr 3 23:31:49 MahGuard sshd[22992]: Failed password for invalid user admin from 211.137.74.58 port 61635 ssh2
- Apr 3 23:31:51 MahGuard sshd[22994]: Invalid user ftpuser from 211.137.74.58
- Apr 3 23:31:51 MahGuard sshd[22994]: Failed password for invalid user ftpuser from 211.137.74.58 port 61839 ssh2
- Apr 3 23:31:53 MahGuard sshd[22996]: Invalid user ftpuser from 211.137.74.58
- Apr 3 23:31:53 MahGuard sshd[22996]: Failed password for invalid user ftpuser from 211.137.74.58 port 62434 ssh2