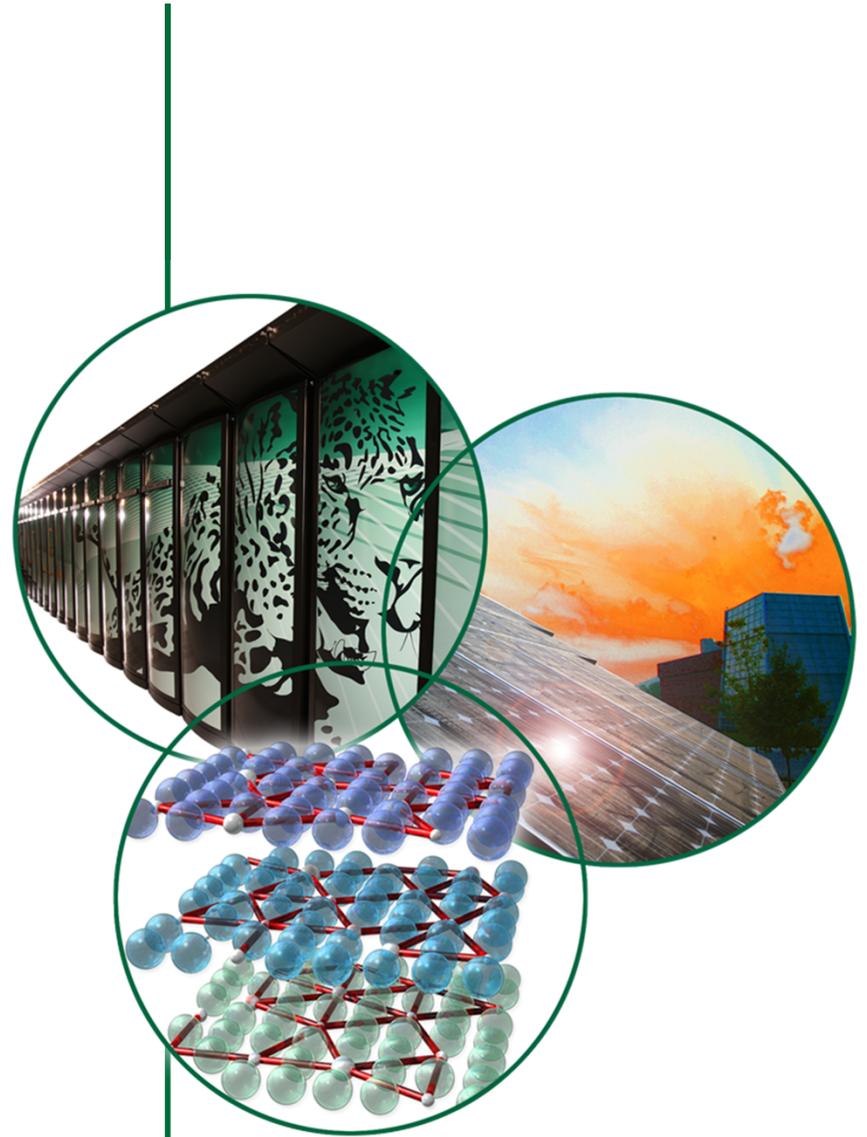


ORNL Cyber Security Issues

David Freeman
ORNL/SNS

Accelerator Safety Workshop
Tuesday Sept. 20, 2011



U.S. DEPARTMENT OF
ENERGY

 **OAK RIDGE NATIONAL LABORATORY**
MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY

Chronology Overview

- April 7, 2011 - Phishing email attack; individual with “Administrative Privileges” clicked on it
 - Appeared to be downloading image - downloaded executable
- April 11 – Malware intrusion identified
- April 11 to 15 – Malware was monitored in attempt to learn origin, intent, purpose
- April 15 (Friday ~ 4:15 pm) – ORNL disconnected from internet – protect information from being exported.
- May 1 – Essential functionality restored – internet contact restored.

What Happened

- Zero-day vulnerability exploited (Windows XP)
- Windows Explorer phishing expedition
- Shotgun phishing email sent to ORNL staff
- Individual with Administrative Privileges clicked on it
 - Auto-executable downloaded
 - Administrative password decoded
- Laid dormant for ~ 2 weeks before becoming active (Friday surprise!)
- Started Ex-filtrating data at high rate (full blast)

What Happened

- ORNL shuts down – physically disconnects from outside world; all email functionality shutdown
- Email shutdown
- Smart phones interface shut down
- All outside “VPN” access shut down
- ORNL uses large “heterogeneous” network - all machines work the same way
- Compromise allowed access to every windows machine on the network.
- All ORNL Safety Systems remained operational

What Happened

- DOE heavily involved in recovery - approval required to reconnect to grid
- War Room Established - Army of experts from Microsoft, LANL, PNNL, Various gov't agencies, Security Engineers, etc.
- Emails restored – text only
- Emails restored – hyperlinks disabled (~ 1 month)
- Rebuild required for many machines/systems

Some Corrective Actions

- Re-architecting of Systems
- Greatly reduced number of folks with administrative privileges
- Lab based phishing expeditions – folks still fall for it
- Situation Improved - Still vulnerable

What Happened

- SNS Impacts

- NScD/SNS physically disconnect from ORNL network on April 15
- Accelerator Control and Safety Systems unaffected
 - Continued to operate
 - Firewalled from the ORNL network
- Instruments
 - Parts of Instrument Systems taken down
- Instrument Data Acquisition System unaffected
 - In different “protection zone”, not part of ORNL network
- Event occurred during maintenance outage - all systems restored by end of maintenance period.

Other Challenges at SNS

- Users come and go with USB devices – lots of viruses
- Scientist culture – often reluctant to run virus scanners
 - Often times would be transparent to their operations
 - Often times conflicts with vendor supplied software, etc.
 - many machines run off the network, IT unaware of their status
- Balance cyber security with facilitating science and users