LIGO Cybersecurity Status

Albert Lazzarini

NSF Annual Review of LIGO
LIGO Hanford Observatory
October 23-25, 2006

Outline

- Recommendations from last review
- Overview of cybersecurity within LIGO Laboratory
- Summary of activities during the past year
- Engagement outside LIGO Laboratory

Responses to recommendations from 2005
LIGO Computing

Develop, document, qualify a computing model

- Released the first version of the collaboration computing plan covering the era of LIGO I -- prior to Advanced LIGO operations(~ 2013+)
  - Update plan to reflect accrued experience since plan's first release
  - Extend plan to address Advanced LIGO needs

Continue working with the Open Science Grid (OSG)

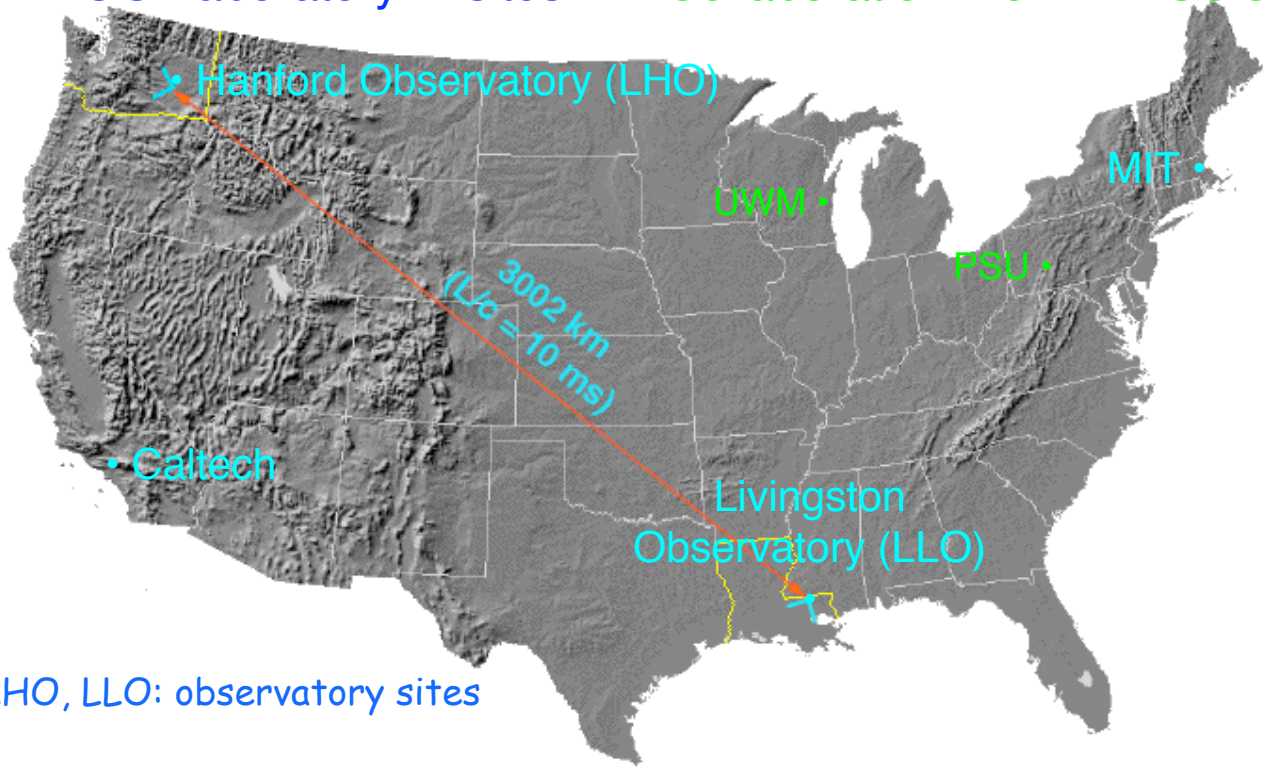
- LIGO is an integral member of the Open Science Grid project -- recently funded by NSF/DOE
  - Resource Manager on OSG Executive Team (K. Blackburn)
  - OSG Council representative (W. Anderson, UWM)
  - OSG Virtual Organization(VO) Support Center (M. Ramsunder, PSU)
  - LSC production analysis is being integrated with OSG
    - Physics at the Information Frontier (PIF) awarded to LSC data grid institutions concurrently with OSG
    - P. Brady (PI, UWM), ex officio member of OSG executive board

Overview

The LIGO Scientific Collaboration and the LIGO Data Grid

LIGO Laboratory: 4 sites

Collaboration Tier 2: 2 US sites + 3 EU sites



*LHO, LLO: observatory sites

- LSC - LIGO Scientific Collaboration
  - Not under organizational control of LIGO Laboratory
  - Funding provided through separate grants - NSF /EU
  - Cybersecurity policy allows them to join trust relationship with laboratory via MOUs

Overview
Cybersecurity within LIGO Laboratory

- LIGO's sole mission: gravitational wave fundamental scientific research -- principal goal: maximize scientific output
- Computer security for LIGO must be consistent with mission & goals
  - ***Primary***: avoid disruption of operation or corruption of data
  - ***Secondary***: avoid serious embarrassment caused by defacement of LIGO publicly accessible websites or the use of LIGO computers in criminal activities
  - Designed to address *no more* than the specific LIGO computer security aims:
  - Caltech provides support for LIGO's payroll, accounting, purchasing and other major business systems and these are covered by Caltech policies
- All measures based on risk evaluation
- Computer security implementations *must be balanced*
  - Disruptions to science caused by intrusions vs. impediments to science caused by security measures

Overview
Cybersecurity within LIGO Laboratory

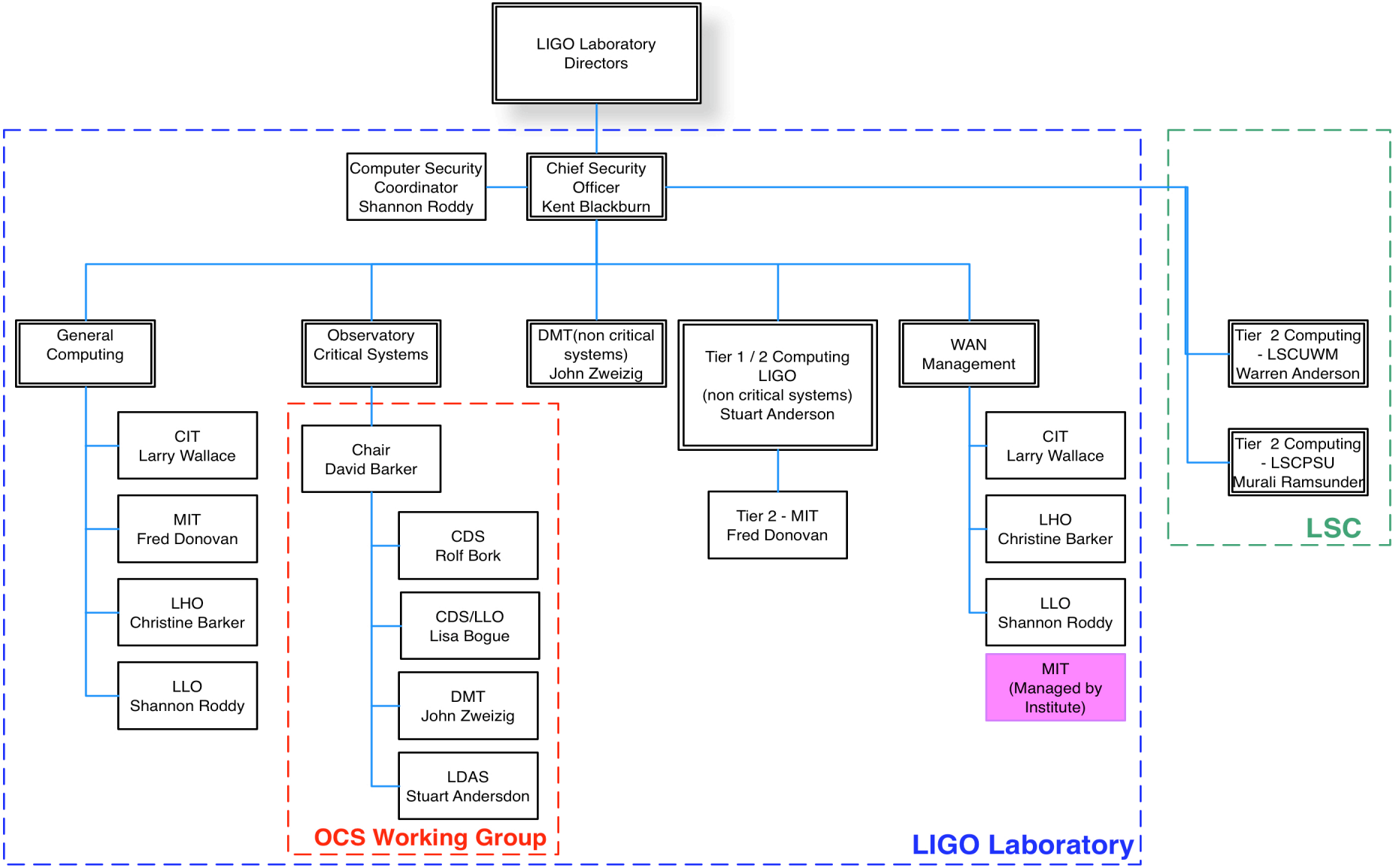
- Cybersecurity is based on a layered approach
- Ensure significant assets are fully protected and secure
- Allow flexible access to information required to allow the LIGO Scientific Collaboration to accomplish its scientific mission
- Most stringent requirement applies to resources located at the observatory sites

Overview
Observatory Critical Systems (OCS)

- Cybersecurity plan identifies the *key area* of LIGO Laboratory IT infrastructure that requires specific measures to ensure robustness against disruption of LIGO operations from cyber attacks.
  - Observatory Security Critical Systems
    - Located at the observatory sites
- Comprises of the interferometers and data caches prior to commitment of data to the permanent archive.
  - Ensures that interferometer operation and control takes place in a secure environment
  - Protects integrity of archived data
  - Interferometer controls & data acquisition (CDS - Control & Data System)
  - Data archival at observatories (LDAS - LIGO Data Analysis Systems)
  - General computing components (GC) that “touch CDS & LDAS”)
- OCS oversight assigned to an OCS Committee that is chaired by LHO CDS lead (D. Barker)
  - Charged with evaluating, assessing cybersecurity measures & needs with regard to the OCS infrastructure
  - Key personnel responsible for major OCS infrastructure are members of the committee
  - Cybersecurity personnel, CSO and CSC, attend all meetings.

Overview

Cybersecurity Organization within LIGO Laboratory



Activities during past year
New Computer Security Officer

- Kent Blackburn appointed new LIGO Computer Security Officer (CSO) in September 2006
- Shannon Roddy remains the Computer Security Coordinator (CSC)
- Internally: immediate tasks at hand:
  - Reviewing/updating cybersecurity documents & policies;
  - Cybersecurity Plan
  - Update Risk Assessment
  - Acceptable Use Policy
  - Incident Response Procedures
  - Patch Procedures
- Externally: focus on integration of cybersecurity within the larger collaboration computing infrastructure
  - New working group established under the LSC Computer Committee to address collaboration wide partnership in cybersecurity.
  - Comprises of LIGO CSO/CSC and LSC Tier II computer security officers
  - Also addresses LIGO certificate management under the DOE CA

Activities during past year

Improved security - Observatory Critical Systems

- OCS committee convened bi-monthly to assign actions, monitor progress in security implementation at both observatories
- Intrusion Detection System installed
  - IDS installed on server performing as an X2100 gentoo router, with a mySql database and web data access tool running on the base X2100 FC4 server
- Administration traffic and system logs further secured
  - New ADMINLAN installed, IDS database and syslog server on this network
- Outside access to Critical Systems reduced to single point of access
  - Dual home gateways removed. NAT router the single point of access
- CDS controls and non-controls network traffic separated
  - New PCLAN created for non control systems. RAIDS, switches and tapes moved to ADMINLAN. New TESTLAN created for offline teststands and laboratory systems
- Offsite network scans of OCS resulted in system reconfiguration/upgrades
  - Ports which should not be open were closed. Older versions of server software, e.g. apache, upgraded
- Reviewed and further restricted offsite access to the OCS
  - Access to framebuilder NDS restricted on a need-to-know basis. Access to testpoints removed. Sensitive wiki data is password protected, etc.

Activities during past year

Addressing Vulnerabilities

- Vulnerability Assessment
  - In progress: assessment using NIST FISMA supporting documentation as starting criteria
  - Targeting compliance with NIST Special Publication 800-53
    - Proving difficult in certain areas
  - Variances from NIST 800-53 will require directorate approval
- Network Vulnerability Scanning (NESSUS)
  - CY2006: performed scans of LIGO assets connected to the outside.
  - Used NESSUS (industry standard tool) with publicly available vulnerability databases
  - Network vulnerability scanning will take place annually at a minimum
  - Issues and variances from policy to be resolved by the individuals responsible for the subsystem

Activities during past year

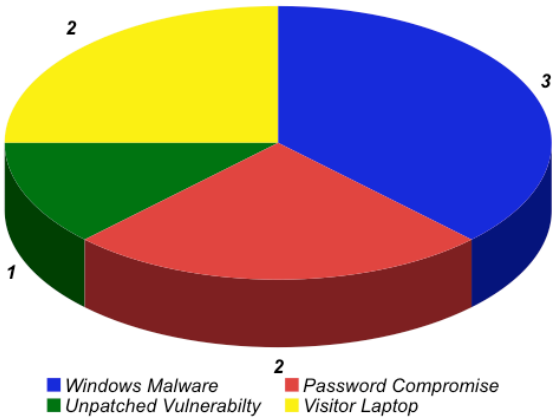
Participation within the larger cybersecurity community

- Attended security conferences, workshops & meetings :
  - NSF Cyber Security Summit for NSF Large Research Facilities Vienna, VA Dec '05 http://www.educause.edu/cyb05
    - (At the encouragement of T. Carruthers, NSF)
  - Educause Security Professionals Conference Denver, CO April 10-12 '06 http://www.educause.edu/sec06
  - 15th USENIX Security Symposium Vancouver, B.C., Canada August 1-4 '06 http://www.usenix.org/events/sec06/
- LIGO CSO engaged in OSG Security Planning through his OSG Executive Team role
  - Effective mechanism in providing visibility for LIGO into challenges faced outside the Laboratory
  - Allows us to bootstrap our security learning curve as we integrate further into the global grid computing environment

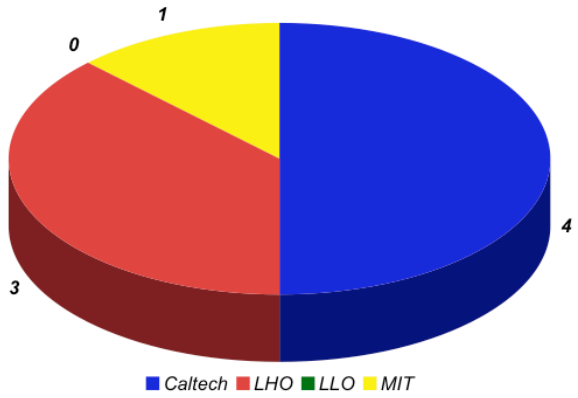
Activities during past year
Incident Summary (since last NSF Review)

- *To date, no compromises discovered within the LIGO Observatory Critical Systems*
- 8 incidents this past year were restricted to General Computing infrastructure at a number of LIGO Lab. Sites
  - Revealed several weaknesses in our policy, and identified the need to prioritize further IDS activities
  - 3 of 8 incidents led to an update of our policies

Nature of incidents



Incidents by site



Outside engagement
LIGO and the Open Science Grid

- The LIGO Scientific Collaboration is one of the original members of the Open Science Grid (OSG)
  - Operating 2 OSG Production sites at PSU and UWM
  - Operating 1 OSG Integration Testbed site at Caltech
  - Operating 1 OSG Validation Testbed site at Caltech
  - Each site must register a site security contact with OSG
    - All LSC OSG sites have registered the local system administrator
- Each Virtual Organization (VO) in the OSG manages a VO Support Center
  - LIGO's VO Support Center is located at PSU
  - Acts as a point of contact for the OSG Grid Operations Center with the VO
    - Includes cybersecurity and incident response point of contact for VO
- LIGO computer security infrastructure benefits from having a much larger collaboration from many different disciplines
  - Examples:
    - Adoption of DOE CA protocols
    - Recent Globus Security patch communicated to LIGO via OSG channels

Challenges for LIGO

- Cybersecurity was not central to the original architecture of the CDS network, developed & designed in 1995 - 1997
  - Control room operations rely on shared unix accounts for ease of work flow
  - Real-time dedicated 24x7x365 operations (including commissioning and engineering support when not in science runs) makes it very difficult to effect system upgrades
    - CDS relies on critical systems with out dated operating system that are no longer supported or lack security features, e.g., telnet session to VxWorks
- Patch installations require larger than anticipated effort due to the uniqueness of most computer configurations
  - Many patches must be backed out to allow productive work to continue for science operation
- Access to near-real-time science data by systems outside the OCS infrastructure leads to multi-homed CDS gateways with multiple links to General Computing -- these are critical to current science run
- Need to establish greater commonality of security infrastructure and strategies across all LIGO sites
  - Example: recent progress towards IDS at each LIGO Laboratory site
- Prominence of laptop computers underscores importance of physical security and protection of key information that might be stored on them (e.g., private keys).

Conclusion

- LIGO implemented a cybersecurity plan in 2004
  - General level of security awareness within Laboratory has increased
- Past two years have focused on improving security of the Observatory Critical Systems infrastructure
  - … however, scientific observation limits ability to make rapid changes
- Greater involvement in Grid Computing introduces additional vulnerabilities that need to be addressed by policies, incident response, risk assessment, and LIGO user community
  - Coordinate with LIGO Tier II computer security officers to assure partnership and ownership of solutions.
- LIGO is still assessing how compliance with NSF guidelines & expectations meshes with NIST FISMA standards
  - Level of effort for complete implementation is high!