LIGO Cybersecurity

VO secruity from a physicist's perspective

Warren G. Anderson

LIGO Scientific collaboration

Securing What/Whom

Users and systems

LIGO

- Laser Interferometer Gravitational-Wave Observatory
- Built in the 1990s, operational since the early 2000’s
- Looks for ripples in space-time from astronomical sources.
- Made first detection in Sept. 2015, announced it in Feb. 2016.

Two LIGO User Populations

- LIGO Laboratory
  - Smaller population (190 people)
  - More accountable (can be fired)
  - More likely to have access to high-value systems
  - Use systems we control
- LIGO Scientific Collaboration
  - Larger population (881)
  - Less accountable (can refuse to renew MOU)
  - Have some access to high-value systems
  - Use systems we don't control

LIGO Scientific Collaboration

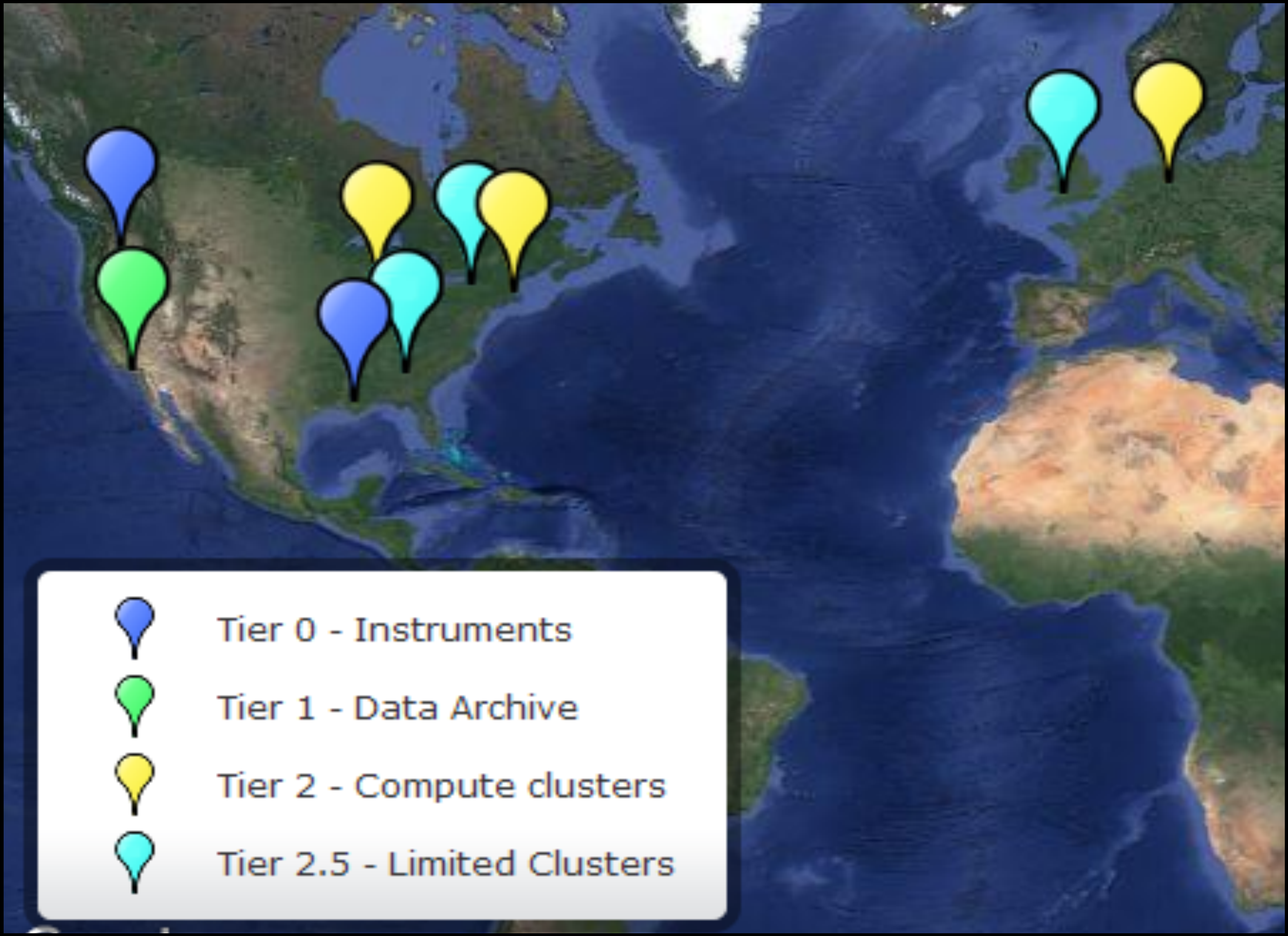
86 institutions, 17 countries, 5 continents

TRINITY UNIVERSITY
UNIVERSITY OF MARYLAND
Andrews University
WASHINGTON STATE UNIVERSITY
CALIFORNIA STATE UNIVERSITY FULLERTON
UAH THE UNIVERSITY OF ALABAMA IN HUNTSVILLE
SONOMA STATE UNIVERSITY
indigo
MONTCLAIR STATE UNIVERSITY
University of Glasgow
Australian National University
WHITMAN COLLEGE
AMERICAN UNIVERSITY WASHINGTON, DC
UNIVERSITY OF THE WEST of SCOTLAND UWS
TEXAS TECH UNIVERSITY
清華大學 Tsinghua University
R·I·T
Max Planck Institute for Gravitational Physics ALBERT EINSTEIN INSTITUTE
UNIVERSITY OF STRATHCLYDE
MICHIGAN
CITA ICAT
Università degli Studi del Sannio
NASA GODDARD SPACE FLIGHT CENTER
ICTP SAIFR
THE UNIVERSITY OF WESTERN AUSTRALIA
PAH
ACU
UNIVERSITY OF CAMBRIDGE
THE UNIVERSITY OF CHICAGO
MONTANA STATE UNIVERSITY
SOUTHERN UNIVERSITY Agricultural & Mechanical College
COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK
Caltech
UNIVERSITY OF MINNESOTA
THE UNIVERSITY of MISSISSIPPI
THE UNIVERSITY OF ADELAIDE AUSTRALIA
UNIVERSITY OF BIRMINGHAM
THE UNIVERSITY OF MELBOURNE
UIB Universitat de les Illes Balears
UNIVERSITY OF WASHINGTON
GEO 600
UTRGV
CARLETON COLLEGE NORTHFIELD, MINN.
UNIVERSITY of WISCONSIN UWMILWAUKEE
SYRACUSE UNIVERSITY FOUNDED AD 1870
CARDIFF UNIVERSITY PRIFYSGOL CAERDYD
Northwestern
UNIVERSITÄT HAMBURG
MONASH University
INPE
UF UNIVERSITY of FLORIDA
Georgia Institute of Technology
Korean Gravitational-Wave Group
LSU LOUISIANA STATE UNIVERSITY
ACIGA
University of Southampton
CHARLES STURT UNIVERSITY
EMBRY-RIDDLE AERONAUTICAL UNIVERSITY
Leibniz Universität Hannover
PennState
WILLIAM SMITH COLLEGE
Science & Technology Facilities Council Rutherford Appleton Laboratory

External User Populations

- VIRGO (French-Italian project)
  - 405 people
  - Access to most systems available to LSC
  - Less accountability – no security aspect to MOU
- Other astronomers
  - A few hundred
  - No access to high value systems
  - No real accountability

Systems - Geography



Systems - Types

- Detector control and monitoring systems
  - Two sets at Livingston and Hanford Observatories
  - Access billion dollar instruments directly
- AuthN/Z systems
  - Redundant copies at all Tier 0-2 sites, centralized for Tier > 2.
- Computer clusters
  - Tier 0-2.5 sites, supply most scientific computing, allow ssh.
- Collaboration services
  - Wikis, mail servers, ssh portals, etc
- General computing
  - Laptops, workstations, etc

Premise

Maximizing science opportunity is the overriding concern.

Risk Analysis

- Risks matrix tries to compare expected downtime from an incident vs expected loss of science from reduced usability (hard to do).
  - "Good" security measures have minimal impact on usability, or even enhance it (e.g. SSO)
- "Disgruntled insider" seen as largest potential threat.
- Risk posture and residual risks explained to and accepted by (or not) project management.

Risk Posture (Lower Risk)

- LIGO Laboratory users and systems (Tier 0-1 and Lab internal GC)
  - Training programs, network monitoring, system configuration controls, enforced patching, etc are feasible.
- LSC Compute clusters (Tier 2-2.5) and many collaboration services
  - Some admin training, weekly admin meetings discussing configuration controls, patching etc.
- Collaboration services software and systems
  - Largely widely used (MIT Kerberos, Shibboleth, OpenLDAP, Sympa, FOSWiki, Redmine, GIT, etc) or security reviewed.

Risk Posture (Higher Risk)

- Some collaboration services and most non-Lab GC
  - Managed by LSC scientists with little or no security training or by campus IT groups who have little or no understanding of LIGO trust relationships.
- Most scientific software
  - Written by LSC scientists with little or no security training and has not been reviewed for security.

Premise

VO environments have fuzzy borders,
risks are unavoidable

Risk Acceptance

- LIGO and other large science VOs must accept higher risks than many other organizations or they lose science opportunity.
- Incident detection and response are at least as important as risk mitigation.
- Understanding risk posture and accepting residual risk important for security team and management.

Incident Detection

- Possible on high value systems but …
  - User laptops?
  - System run by member institutions?

Incident Response

- Trust relationships exist with MANY different organizations to which LIGO scientists belong.
- Clear communication and, where possible, coordinated response between external organizations and science VOs is highly desirable.
- Building channels for security coordination with member institutions not a priority for scientists and does not scale well.
- Managing the message is important …

Incident Response

- Lessons learned from LHC (thanks Romain):
  - There is no such thing as a “small” incident once the media gets ahold of it.
  - Some scientists think they understand things they don’t and will talk about them freely to anyone who asks.
  - Governments and funding agencies will sometimes care more about perception than truth.

Current Status

- Much work left to be done on incident response both internally and coordinating with other organizations.
- One hurdle passed – major publicity for first detection in Feb, no incidents.
- CISO recently left to accept another position, we are looking if you are interested.