LIGO LABORATORY
MS 18-34
PASADENA CA 91125

TEL: 626.395.2129
FAX: 626.304.9834

MEMORANDUM

DATE: November 25, 2008

TO: LIGO Laboratory Personnel

FROM: A. Lazzarini, J. Marx

SUBJECT: AUTHORIZATION OF MONITORING ACTIVITIES BY THE CYBER SECURITY TEAM

Refer to: LIGO-M070072-C-M

Summary

This is an update of a memo previously issued in 2007.

LIGO supports a strong computer security policy and associated activities needed for its enforcement. At the same time, LIGO is cognizant of the importance to provide assurance that user privacy will be respected to the greatest extent possible. Nonetheless, some necessary actions taken by the cyber security team may be construed to otherwise infringe on user privacy. For this reason, it is important that authorization of such activities be documented and made public to the laboratory at large. We hereby authorize the cyber security team to engage in only those security activities they deem necessary to allow them to fulfill their role. We also provide guidelines for restrictions on these activities. Last, we define the obligations of users to support the cyber team's security activities.

Importance of security

The LIGO Laboratory Directorate believes that continued successful operation of Laboratory computing resources requires implementation and support of a strong and effective security plan for those systems.

The LIGO Laboratory Computer security Policy, M040352, and LIGO Laboratory Computer Use Policy, M020105, provide requirements to ensure that LIGO staff and users operate computing resources at all sites in a manner designed to promote the protection of those resources from abuse, damage, or unauthorized use.

As a distributed NSF national facility, LIGO Laboratory has obligations that go beyond Caltech's computing policies. For example, at the time of this writing, the DOE in Hanford, WA, Louisiana State University in Livingston, LA, and Charter Communications host the networks for the sites.

Sensitivity of Security Activities

Security activities may require monitoring — i.e., collecting and evaluation information on system and user activities and communications. Computing resource users may consider some of this information sensitive, confidential, private, or personal.

Furthermore, Federal and State law, in addition to Caltech policy, prohibit monitoring of electronic communications except under particular circumstances. Additionally, security activities may require exercising the same methods as used by an attacker, which, without express authorization, the law could interpret as illegal. For these reasons we are issuing this memorandum.

Scope of this Memorandum

The intent of this memorandum is to (i) provide LIGO personnel with an understanding of the types and scope of security activities that may be undertaken, (ii) authorize specific staff members to engage in these activities, and (iii) identify the obligation of all other staff to cooperate and/or provide assistance as requested.

Authorization of the cyber security team to conduct needed investigations

LIGO prohibits any form of network monitoring and other related security activities *except to those explicitly authorized by this memo*. Where noted, authorized staff may designate other users on a limited or ongoing basis. Such designations must be made in writing and the Directorate shall be kept apprised of them (email is acceptable).

This memorandum authorizes the Laboratory Computer Security Officer (CSO), Computer Security Coordinator (CSC), and their designees to conduct assessment, monitoring, investigations, and incident response in the course of their duties in a manner consistent with the LIGO Laboratory Computer Security Policy.

The security team will determine specific activities appropriate to the task at hand. Typical examples of these activities include:

- Collecting documentation of network topologies, system configuration, system administrator activities, user information (e.g. which users use particular systems, contact information for users).
- Monitoring of systems and communications for the purposes of verifying security configurations (e.g., ensuring encryption utilization for passwords, checking network access controls) detecting suspicious activity (e.g. observing attack attempts), determining the state of an incident and monitoring intruder activity during an intrusion.
- Installation of devices and software, and configuration changes to systems, in order to enable monitoring as needed.
- Collection and analysis of system and application logs for use in assessment, auditing, intrusion detection, incident response.
- Penetration testing, vulnerability scanning, port scanning, and examination of host and network configuration in order to detect unnecessary services, services

known to carry unacceptable risk of exploitation, and misconfigurations which create security exposures.

- Computer forensics & evidence collection after an incident is detected to determine the nature of the intrusion, the extent of the intrusions, and the damage, if any, to LIGO systems and data, etc.
- Changes to systems, networks and services, and/or removal of computing resources from the network in order to contain and control ongoing intrusions or to rebuild affected systems.

Obligations & responsibilities of other Laboratory personnel

The security team may call on any LIGO staff member or user, as necessary and appropriate, to assist in particular security activities. In particular, the team will often require the assistance and support of system administration staff. LIGO expects staff to provide assistance in a timely manner, especially with regard to assistance in dealing with an incident in progress.

LIGO believes the security of LIGO systems contributes directly to the success of LIGO; an intruder could cause physical damage to critical systems, interfere with the Laboratory's scientific mission, and/or corrupt irreplaceable data. In that regard, we expect all staff to treat incident response as a *high priority item* and to provide *immediate* assistance to the security team whenever they are asked; at times this assistance may require canceling or changing other planned activities.

Common examples of activities which the security team may request of staff include:

- Providing privileged access (e.g. root password or domain admin rights) for the security team to LIGO systems for the purposes of to enabling assessment, installing monitoring and intrusion detection capabilities, investigation of suspicious activity, and incident response
- Providing and setting up equipment as requested by the security team, in particular, monitoring and intrusion detection systems.
- Removing compromised systems from the network.
- Providing any information required by the security team necessary to conduct an assessment or investigation. Common examples of such information include topological, logical, physical, and other network and system information. However, the team may also require information about user activities and user contact information.

Reporting

The security team does not require prior approval from the LIGO Directorate for reactive actions required to stop an attack or to defend LIGO's data or infrastructure. However, the CSO or CSC will apprise the Directorate, the Site Head and any other other designated personnel as soon as possible. The CSO will also file an incident report in a timely manner after all episodes.

Compliance with Institutional Policy

At all times, LIGO staff shall conduct computer security activities in full compliance with applicable Caltech policies for those LIGO sites administered by Caltech, and with applicable MIT policies for the MIT LIGO Laboratory.

Definitions

To avoid misinterpretation of this memorandum, we provide here definitions of the terms used to describe the security activities.

We define *LIGO systems* as consisting of any and all systems connected to LIGO Laboratory networks, including network connectivity devices. For clarity of simplicity, we will use this term below to avoid listing all possible devices.

Assessment

Assessment activities provide information about systems and networks in order to identify weaknesses (*vulnerabilities*) which a malfeasant person (*attacker*) can use to compromise security, or which may unintentionally expose confidential information. The resulting information informs LIGO about the potential risks to systems and data, from which we then determine measures to eliminate unacceptable risks.

Assessment consists of a variety of activities, most of which simply require collecting documentation. Examples of such documentation include network addresses and topology, location of computer systems (*hosts*) and the services each provides, configuration of systems and services, procedures for managing systems, users of the systems and their authorizations.

More active assessment activities include the use of automated tools to identify hosts, services (*network mapping*), and potential vulnerabilities (vulnerability scanning).

Auditing

Assessment also includes *auditing* to verify that documentation of systems match the actual system configurations, and to verify the proper implementation of security features.

Audit Trail

Auditing and monitoring (defined below) may require the ongoing collection of transactional information, called an audit trail.

Incident

We define an incident as the set of events which include actual unauthorized access to or use LIGO systems. Unauthorized use can result from a person with no access to LIGO systems gaining access, or a user with access to some LIGO systems gaining access to systems for which they have no authorization to use. Furthermore, unauthorized use may result from use of authorized access to perform acts in violation of LIGO policies, Caltech policies, or State or Federal laws.

Attack

An attack consists of the steps taken to gain access to LIGO systems. A successful attack becomes a compromise.

Intruder or Attacker

We call the person who compromises a system an intruder or an attacker. Note that we do not apply this term to users who violate policy. We call the that activity abuse or misuse.

Investigation

An investigation occurs when something raises suspicion (suspicious activity)of an incident with the security team. The event may come from an automated monitoring system, observation of unusual activity by a LIGO user, or notification from a third party.

Incident Reponse

An investigation which uncovers an incident results in an incident response, where the security team will assess the situation and take action to contain tand remedy the situation, determine that nature of the incident, and identify the source and identify of the intruder or abuser.

Monitoring

Monitoring generally refers to collection and analysis of information from systems and networks,. Monitoring can occur on a routine, ongoing basis for the purposes of detecting suspicious activity, and on an as-needed basis during an investigation. The information analyzed can include, but is not limited to, network communications including the content of those communications, logs from systems and applications, contents of stored files, and user activity such as commands entered on the keyboard.