

ESnet Security Incident Response Services

Abstract

We propose a set of contact and messaging services to facilitate communication between site computer security personnel such that multi-site computer security incidents affecting the DOEGrids can be resolved quickly with minimal impact. These services would include secure e-mail services, a weblogging or journaling service, secure IM, and other secure communication mechanisms.

1 Collaborators

ESnet – PKI team; ECS team ; Technical Services
NERSC – Stephen Lau
TBD

2 Deliverables

- 2.1 Demonstration Service
Clone existing ESnet services and adjust
- 2.2 Authentication Services integration
Configuration supports appropriate authentication technologies
- 2.3 Deploy Production Services
Appropriate e-mail, IM, and weblogging identified and in place
- 2.4 Redundant Services
Seamless configuration and deployment to backup site(s)
- 2.5 FUTURE
ECS integration; offer services to wider audience, DOE collaborator sites

3 Motivation

Cross-site computer security incidents are commonplace. The increasingly collaborative nature of science and scientific computing presents more opportunities for computer security incidents at one site to affect other sites.

Currently, site security personnel responding to a computer security incident rely on an informal network of personal contacts and ad hoc tools to exchange information during an incident. Although this mechanism works, it is possible that not all affected parties may be “in the loop”. Secure communication with all affected parties has shown time and time again to be critical in the quick and complete resolution of these types of incidents.

Site security personnel need better support in setting up, managing, and closing down multi-site communication networks of incident responders.

The DOEGrids PKI, in order to maintain the trust of its subscribers and relying parties, must deal with compromises of user credentials in a reliable, consistent, and transparent manner [DGCPS]. The DOEGrids PKI has created an “Incident Response Committee” (IRC) to manage information flow and respond to security incidents. In the event of a

computer security incident affecting the DOEGrids, the committee creates an “Incident Response Team” (IRT) – the informal network of contacts – and instructs the DOEGrids PKI on how to respond to the incident (i.e. which certificates to revoke).

4 Approach and Requirements

The IRT will be provided with a secure, integrated set of services.

- Authentication services will allow new accounts to be created and existing, known good, authentication technologies (tokens) to be bound to these accounts.
- A secure weblog or journaling service will be provided to allow data collection and distribution to team members.
- Secure “Instant Messaging” technology (based on the [JABBER](#) protocols) will be provided
- One-stop, secure, instant creation of these services, on a per-incident basis, will be provided to a core group of administrators (the Incident Response Committee).

The IRT and its associated services are *ephemeral*. Once an incident is considered closed, the IRT and IRC will manage and report on incidents as appropriate, and dispose of journaled content as they see fit.

We will begin with information technology software familiar to ESnet, but requirements for authentication, ease of creation, weblogging, and redundancy will require some tuning and possible use of other products.

In parallel, we will deploy some ESnet Collaborative Services tools (see [ECSSTR]) to support “water cooler” video presence and other conferencing technology.

5 Costs and Resources

- Nonrecurring:
 - 0.75 FTE - Evaluate and deploy technology
 - 0.15 FTE - System administration and technical services support
 - 0.10 FTE - Policy document, DOEGrids
 - Servers, miscellaneous hardware, and software: \$50k
- Recurring:
 - 0.50 FTE - Service tuning, support, vendor relations
 - 0.10 FTE - System administration and technical services support
 - Marginal - staffing the DOEGrids IRC (making it a standing committee)

These estimates do not include integration with ESnet Collaborative Services (video presence and conferencing). Additional resources will be needed to integrate with ECS scheduling services.

6 References

[DGCPS] “DOE Grids Certificate Policy and Certification Practice Statement Version 2.4”, DOEGrids PMA, 31 May 2004, <http://www.doe grids.org/Docs/CP-CPS-V24.doc>

[ECSSTR] “Strategic Direction for IP Collaboration at ESnet”, ESnet ECS project, Apr 2003