CSIRTs and Grids, Draft v0.3 (14/04/2005)

This note compares the security support requirements for an operational Grid service with the activities performed by a classical Computer Security Incident Response Team (CSIRT) to see what aspects of the CSIRT model are likely to be useful in the Grid context and what aspects are unique to Grids and need a different approach. Three different types of CSIRT are referenced: local site security teams, who are normally part of the network or system operations group at a site, coordinating CSIRTs, such as JANET-CERT who are responsible for a network or country, and vendor security teams, such as Cisco's PSIRT who are responsible for the security aspects of a software product.

The note has been written by Andrew Cormack of UKERNA and is circulated as a draft for comment. Comments should be sent to A.Cormack@ukerna.ac.uk

CSIRT functions

The CERT Co-ordination Center (CERT-CC®) have a useful document listing and describing the services that may be provided by CSIRTs. From their list, the following seem to be most relevant to the Grid context:

- **Announcements and Information Dissemination**
  These two pro-active services allow a CSIRT to distribute information about good security practice to its community, for example through mailing lists and websites. The information may be generated within the CSIRT itself, obtained from external sources, or found within the community with the CSIRT providing quality control, technical authorship, anonymisation (or attribution!) and distribution as required. Announcements and Information Dissemination are commonly provided by coordinating CSIRTs at a national or network level, with distribution and user encouragement provided by local security teams at end sites.
- **Incident Detection and Analysis**
  This reactive service involves the initial identification and analysis of an incident: working out whether an event is in fact a security incident, understanding it and identifying the potential extent of any threat or damage. Since this requires detailed knowledge of the affected systems and technologies, it is normally done by local security teams with coordinating CSIRTs providing support and technical expertise where required.
- **Incident Response on-site**
  This reactive service involves the containment of a security incident and, as far as possible, the remediation of its effects. It is normally provided by local security teams with hands-on access to the affected systems.
- **Incident Response Coordination**
  This reactive service involves the coordination of incidents that may involve multiple sites or organisations. It may include actions to contain and remedy the problem, as well as to inform others who may have been affected. It is normally provided by coordinating CSIRTs at a national or network level.
- **Vulnerability Handling**
  This reactive service involves the handling of vulnerabilities in products, typically software or operating systems, from the discovery of a vulnerability through to the production and installation of fixed software. It involves the

producers and/or distributors of the affected product, often supported by coordinating CSIRTs both for reporting and analysing the problem and for notifying their community of the problem and its remedy through the Announcements and Information Dissemination service above.

Similarities

Announcements and Information Dissemination for a Grid will relate to Grid software and systems, but the processes of collecting and distributing the information are the same as for any other type of system. Furthermore, most Grids run on off-the-shelf computers and operating systems so the existing good practice for those platforms will also need to be disseminated. A coordinating CSIRT will normally have an understanding of the main systems used in its constituency and will know the sources of in-depth technical expertise (both on-line resources and people). If resources permit, a coordinating CSIRT may nominate one or more members of staff to specialise in particular platforms used by their constituency. In this, Grids are no different from PCs, Macs, Unix or any other particular software platform. **Incident Response on-site** is normally handled by local technical specialists, and this would be the same for Grids as for any other site system. **Incident Response Coordination** involves coordinating CSIRTs having lists of contacts at sites in their constituency with agreed processes for handling and distributing information about the incident. A Grid incident may involve additional site contacts, though the normal site contacts responsible for the local network should still be involved, but the process of coordination will be the same as for any other type of incident.

Differences

The main area of difference appears to be in the definition and recognition of incidents: the services of **Incident Detection and Analysis**. Grids, like other single-sign-on systems, place particular importance on protecting personal identity credentials since a single compromised credential may give rapid access to a very large number of computers across many organisations and countries. An event that may expose credentials to compromise may therefore be very serious for a Grid even though it only involves reading files, not altering them. Traditional CSIRT work has tended to rate modification of files as much more serious than just reading them, but on a Grid either activity may constitute a serious incident needing immediate action. Unfortunately reading a file leaves no definite traces, unlike modifying it, so it may also be harder to be sure that such an incident has actually happened.

Grids may also give rise to events that CSIRTs might identify as indicating serious incidents. Data grids in particular may routinely produce sudden and very large traffic flows. Flow statistics are often used by traditional CSIRTs as alarms: an unexpected large flow would usually be interpreted as a compromised host being used for a denial of service attack or bulk mailing. On closer inspection of the number and duration of flows it should be possible to distinguish these cases but alarm systems, and in particular those that take automated action, need to be designed with care.

Both cases indicate the need to develop rules for identifying and classifying the severity of incidents and responding appropriately. These need to be developed by the Grid community working with the site and network CSIRTs who will be involved in implementing them.

Vulnerability Handling for Grids needs to be addressed by those who write and package Grid software, as well as by local systems managers. CSIRTs and systems managers have developed processes for handling notifications of software vulnerabilities, but these rely on software producers issuing advisory notices and patches to aid systems management. As well as supplying remedies for their own software, Grid software authors and distributors need to ensure that where their packages incorporate other open source or commercial systems (including operating systems), they do not constrain the ability of sites to implement patches to those systems as soon as they are released. Particularly in open source software, the release of a patch gives intruders a lot of information on how to exploit the vulnerability so any delay in implementing the patch, for example because it is not compatible with some integrated component, will greatly increase the risk of a successful attack. Operators of Grid systems need to agree who will maintain all the components of their systems, from kernel to application software, and ensure that they have sufficient resources and up to date information to keep their systems safe.

Conclusions

This analysis suggests that CSIRT activities for a Grid are not fundamentally different from those performed a traditional CSIRT. In terms of a local security team or a coordinating CSIRT, Grids represent a new platform specialism: local teams need to be able to manage them securely while coordinating CSIRTs need sufficient knowledge to be able to handle incidents and assess the likely impact. Some discussion is needed to develop rules for identifying Grid incidents and non-incidents.

If a Grid community falls within the constituency of an existing coordinating CSIRT, the most effective approach would appear to be to use the existing systems and processes, providing additional resources to allow the CSIRT to develop a specialism in the Grid software used in its constituency. Where a Grid community does not fall within an existing CSIRT constituency, for example because it includes sites from many countries, a coordinating function may be useful to ensure effective communications when an incident or vulnerability occurs. Depending on the size and skills of the community, this coordinating function could be provided by a virtual team of technical experts from the various sites, so long as the contact list can be kept up to date. However it is provided, such a coordination function must ensure that it has good links with any site or network CSIRTs that have responsibility for part of the Grid to avoid the risk that two CSIRTs will act independently and take contradictory steps to deal with the same incident. Processes for reporting and handling incidents through two different incident response chains (the one based around the network topology and the one based around Grid connectivity) need to be designed and tested with care.

Finally, those who develop and distribute Grid software need to consider how they support their users when software vulnerabilities are discovered. Advisories and patches should be as familiar a feature of Grid operations as of any other kind. These processes must take account of vulnerabilities in standard packages, such as web servers, and operating systems on which Grids depend. Those who manage Grid systems must be able to correct vulnerabilities in all of these components as soon as they are announced.

References

CERT-CC Services list http://www.cert.org/csirts/services.html