Setting up a Grid-CERT
Experiences of an academic CSIRT

Klaus Möller
Senior CSIRT member, DFN-CERT Services GmbH, Heidenkampsweg 41, 20097 Hamburg, Germany
e-mail: moeller@dfn-cert.de

Abstract

Grid Computing has often been heralded as the next logical step after the World Wide Web. Users of Grids can access dynamic resources such as computer storage and use the computing resources of computers under the umbrella of a virtual organisation. Although Grid Computing is often compared to the World Wide Web, it is vastly more complex both in organisational and technical areas. This also extends into the area of security and incident response, where established academic CSIRTs face new challenges arising from Grids. This paper outlines some of the organisational and technical challenges the German academic CSIRT, DFN-CERT, encountered while extending and adapting their services to Grid environments during the D-Grid project.

Keywords
Grid, Security, CERT, CSIRT, Networking

Introduction and Motivation

Grid Computing has often been heralded as the next logical step after the World Wide Web. In [5] it is defined as "controlled and coordinated resource sharing and resource use in dynamic, scalable virtual organisations". Users of Grids can access dynamic resources such as storage (for any sort of data) and use the computing resources (i.e. the CPU) or special resources (such as scanners, microscopes, telescopes, robots, etc.) under the umbrella of a virtual organisation which "enable disparate groups of organisations and/or individuals to share resources in a controlled fashion, so that members may collaborate to achieve a shared goal" [5].

Although Grid Computing is often compared to the World Wide Web, it is vastly more complex both in organizational and technical areas. One of the first lessons learned is, that there is not "the Grid", like "the Web" or "the Usenet". As in the case of the D-Grid project, there are, even at the beginning, no less than six Grid communities. The differences also extend into the area of security and incident response, where established academic CSIRTs face new challenges arising from Grids.

Computer Security Incident Response Teams

Computer Security Incident Response Teams (CSIRTs) offer a variety of services to help their constituencies with security issues, especially with regards to computer security incidents, which is regarded as the minimum requirement for a security team to call itself a CSIRT. A full list of CSIRT services can be found in [3] although which ones are offered by a given CSIRT depends on the concrete needs of the constituency, staff and funding. Cormack et al. have identified a list of services that will be most relevant in a Grid context [1]:

- Announcements and Information Dissemination – Distribution of information about good security practice, attacks and vulnerabilities and providing recommended course of action to remedy the problem, often through mailing lists and websites.
- Incident Detection and Analysis – Initial detection of security incidents and analysis of an incident: whether an event is really a security incident, understanding it and identifying the potential extent of any threat or damage.
- Incident Response on-site – Analysis, containment and remediation of an incident with direct physical access to the affected systems.
- Incident Response Coordination – The coordination of activities among parties involved in an incident. This includes information about how to contain or remedy the problem as well as the initial notification that a party is affected by the incident.
- Vulnerability Handling – Receiving and analysing information about vulnerabilities, mostly in operating system and application software, and developing fixes for the vulnerabilities.

Different types of CSIRTs are referenced: Local security teams, who are often part of the networking or IT-services group of a site; product security teams, who are responsible for the security aspects of a (software) product;

coordinating CSIRTs, such as DFN-CERT, who are responsible for the network of an organisation; and Grid-teams, which can be regarded as a sub-class of a coordinating CSIRT, with responsibility for a Grids virtual organisation.

The D-Grid Project

The German federal ministry of education and research (BMBF) has started in 2005 a strategic initiative, D-Grid, to establish a common Grid infrastructure that can be used by other scientific domains. The project consists of initially five (now six) community projects in the areas of high energy physics, astronomy, medicine and biosciences, climate research and engineering (humanities) and one integration project (DGI – D-Grid Integration). The later will develop the basic infrastructure, while the community projects will build on this infrastructure and enhance it for the specific needs of their research areas.

Part of the DGI is a work package "Networks and Security", dealing with the extension of the existing network infrastructure to the needs of Grids, building an authentication and authorization infrastructure (AAI), develop firewall concepts for Grid-environments and the set-up of Grid specific CSIRT services. The DFN-Verein which builds and operates the academic network in Germany is participating in this DGI work package, specifically the extension of the existing network and, through its CSIRT (DFN-CERT) in the set-up of CSIRT services for Grids.

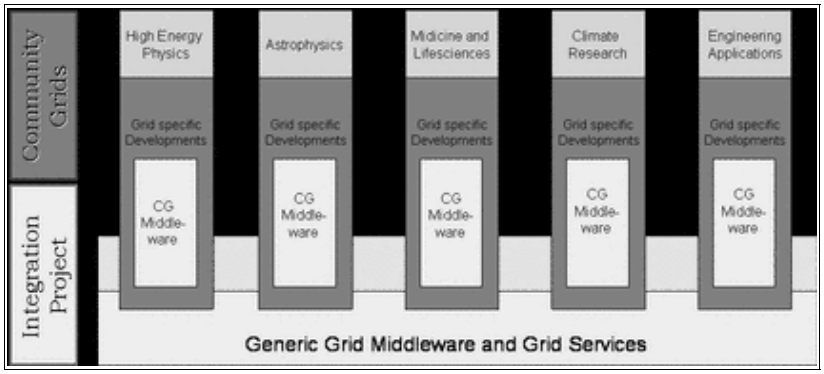

Figure 1: D-Grid project

DFN-CERT is currently offering the full range of CSIRT services to its constituency, Announcements and Information Dissemination as well as Incident and Vulnerability Handling. It operates as a coordinating CSIRT, i. e. it works as an adviser and coordinator with other sites and other emergency response teams. As such, DFN-CERT is a member international organisations like the Forum of Incident Response and Security Teams (FIRST) [2] or Terenas TF-CSIRT task force [3]. While well known inside its constituency and experienced in handling many and diverse incidents, it had at the start of the project no expertise in the area of Grids. At the initial stage of the DGI project, the idea of a central CSIRT for all Grids in Germany was seen as an advantage over having a CSIRT for each Grid project, which would have replicated efforts and thus wasted resources.

It has been argued that there is no fundamental difference between CSIRT activities in their traditional network environment and a Grid environment, from [1]:

"This analysis suggests that CSIRT activities for a Grid are not fundamentally different from those performed by 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."

In practice however, there are several challenges to be overcome to establish a CSIRT for the specific needs of Grids and Grid users. As an example, consider an incident where a stolen credential is found, which enables access to Grid resources. Practical tasks in handling this incident would be to determine to which Grid and User the stolen credential belongs and informing the affected Grid so that the credential can be revoked and the user be supplied with a new credential. This would require knowledge about security contacts for the Grid and users home organisation. Also, it would have to be determined how the credential could have been stolen, and where and when this happened. Finally, illegal use of the credential in the Grid must found and the affected systems be investigated for signs of misuse or compromise. This would require in-depth knowledge about the systems and software used at the affected Grid site.

The following two sections will give an overview about the organizational and technical challenges and experiences DFN-CERT has encountered while setting up a CSIRT for the D-Grid communities.

Organisational Challenges

The first challenge to be overcome when establishing any kind of CSIRT is making the CSIRT known to its constituency. This forms the base of all further activities. Without mutual knowledge, no incidents or vulnerabilities could be reported no could information be disseminated to the constituency. DFN-CERT is already well-known to its constituency, but this knowledge extents mostly to the local security teams at a site, not necessarily to the administrators and users of Grids, although the later are not of primary concern here, as DFN-CERT does only indirectly deal with end users through the local administrators or security teams. Further, it is not known to the security teams and Grid administrators, that DFN-CERT is dealing with Grid incidents or has expertise in this area. The D-Grid initiative provides an excellent forum because it establishes an exchange platform for the Grid communities in Germany. Making DFN-CERT known to the Grid communities is thus a simple matter of introducing it into these forums.

However, mutual knowledge alone is not sufficient for successful incident handling. The local site administrators must trust the CSIRT to handle confidential data and sensitive information properly. Building up this trust is the key problem with any the establishment of all CSIRTs. There is no patent recipe for doing this. DFN-CERT can build upon a certain credit from its other activities. However, care must be taken, as failures in the Grid area could have a negative feedback on its other activities.

Finding Security Contacts

A practical problem that arises with incident handling is the finding the responsible security contact. Typically, a coordinating CSIRT gets a report about an incident or security problem and has to contact other affected parties. This means, that the IP-address or DNS domain name of a system outside the reporting site is known. From here on, CSIRTs can employ several approaches to obtain a contact address, which is typically an e-mail address or phone number, ideally from the local security team of the site.

- The CSIRT can use its own database to obtain the right address. This approach generally yields the best results, as the CSIRTs has an interest in keeping the database up to date. For large constituencies (DFN has over 500 sites), this database may cover only a part of the constituency, due to problems in obtaining up to date information. As part of the service level agreement between the constituency and the CSIRT, sites may be required to supply this information, however, with DFN-CERT, this is not the case. Besides that, the database will not cover sites outside the constituency, or only a very small fraction of them.
- The most often used way is the WHOIS service, from which either the technical (tech-c) or administrative (admin-c) contact can be used. Terenas TF-CSIRT has, together with RIPE, developed the IRT-object [7] which is specifically geared towards supplying information about the security contact or responsible CSIRT for an IP-address block. The IRT-object can be used to hierarchically search for the CSIRT. For example, a university can supply an IRT-object pointing to its own local security team for its network and the ISP could supply another IRT-object pointing to the coordinating CSIRT attached to the aggregated net blocks it is serving. DFN pre-sets the IRT-object for each of the networks it is serving with DFN-CERT as the CSIRT.
- As a fall-back, if the domain name is known, the standard security e-mail addresses from RFC 2142 [8] can be used, i. e. abuse@<domain> or security@<domain>. However, not all sites implement these. As a last fall-back, addresses like root@<domain> or postmaster@<domain> can be used. It is sometimes possible to infer the domain name or IP-address range of the network from the other.

Two sub-problems arise here. First, the local administrators or security team may not be responsible for the Grid installation at that site because the department hosting the Grid site may operate its own computing center or network autonomously from the campus network. above. Together with the problems of scale mentioned above, asking every site in the constituency about which Grid sites are hosted in their networks is thus not practical. The IRT object would be theoretically able to achieve the desired results, however, WHOIS records are generally not well maintained. Apart from that, creating an IRT-object for a local Grid site security team would also require creating a sub network entry in the RIPE database. This would exacerbate the problem with the maintenance of WHOIS records.

Another way would be to ask the Grid communities about the sites involved. However, many of the Grid communities are in the early phases of establishment not do not yet have the information needed by the coordinating CSIRT.

Second, what if not only one Grid site is affected by the incident, but the whole Grid ? In the starting phase of a Grid, when the number of sites is small, it may be practical to contact all sites separately. With a large number of participating sites, participating sites outside the constituency or with highly dynamic virtual organisations, this approach will not scale as the coordinating CSIRT will lose track of the Grids members. Additionally, the CSIRT may become a bottleneck, if it tries to keep track of the members of multiple Grids.

The ideal solution would be a single point of contact for a whole Grid. The Open Science Grid has proposed such a point of contact in its “Security Incident Handling and Response Guide [6]. From section 5.1 of the guide (<domain> being the name of the Grid, for example “astro-grid.de”):

> “INCIDENT-REPORT-L@<domain> is a closed list comprising the Grid security contacts for all

Grid participants and the Grid operations center. Posting is restricted to list members. The list is intended solely for initial incident reporting, not for incident discussion. All email to this list is echoed onto the discussion list and replies are configured to be sent to the discussion list to keep traffic at a minimum.

INCIDENT-DISCUSS-L@<domain> is a closed list comprising the same members as INCIDENT-REPORT-L. The list is intended for discussion of reported incidents.
The differentiation between INCIDENT-REPORT-L and INCIDENT-DISCUSS-L is to allow automated alerting mechanisms to be driven by the arrival of new messages in INCIDENT-REPORT-L.

Grid security contacts utilize INCIDENT-REPORT-L and INCIDENT-DISCUSS-L to communicate regarding security incident handling and response. Communications on both lists SHOULD be signed.

The standard email addresses abuse@<domain> and security@<domain> are received by the Grid operations center, filtered for SPAM or other off-topic email and forwarded to the reporting or discussion list as appropriate. The Grid operations center provides acknowledgements (possibly automated) for incidents reported through these external addresses."

Although the separation of incident reporting and incident discussion seems artificial and cumbersome from the standpoint of established CSIRTs, this proposal has the advantage of being relatively simple to set up for the Grids themselves, so the coordinating CSIRT is no bottleneck. If the CSIRT is made a member of the mailing-list, it is automatically informed of incidents that are discussed inside the Grid. From an organisational point of view, this would be simple to set up through the D-Grid initiative. The are caveats though.

Each Grid has its own unique set of requirements that extend to the field of security. Researchers in physics for example, have few requirements about the protection of intellectual property from the participants in their Grids, contrary to that engineers place high emphasis on this particular area. This has lead to the requirement that certain data about jobs, responsible partners and their projects must be excluded from the Grids meta data directory. Participants in a medical Grid have high requirements about the protection of patient data. Grids with practically no personal data, like climate research place no emphasis on this area. As a consequence of the involvement of partners from the industry, incidents may not be discussed in a Grid, because competitors may learn about each others projects. The high emphasis on privacy protection in the medical field will generate similar problems, although it is easier to overcome as personal data is rarely used in the technical handling of incidents. If such conditions arise during the handling of incidents, the coordinating CSIRT has currently no other way, than to ask for a specific contact while not supplying enough data that other parties may infer the identity or concrete activities of the affected party.

This approach will create a second way of how incidents are reported. The coordinating CSIRT will use the direct way of contacting the local site security team for all non-Grid incidents, and the per-Grid mailing-list for Grid-incidents. Depending on which way is used, certain parties will become informed later of an incident than others. This affects especially the local security teams. Figure 2 shows the different ways an incident report may take. However, this will only be the case if the local site security team and the Grids sites security team are different entities.

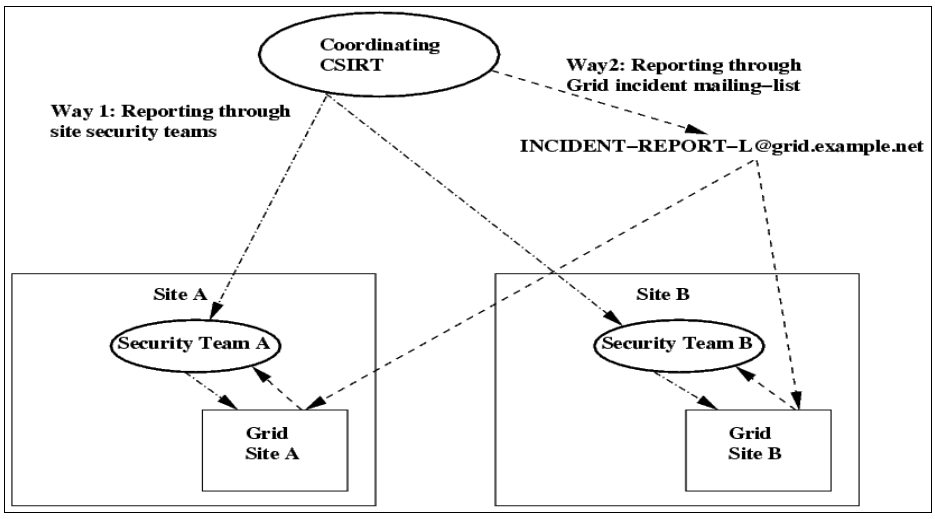

Figure 2: Different ways of reporting Grid incidents

Unrelated to Grid activities, DFN-CERT has set up a system for automated reporting of incidents. With this system,

each site can configure itself what incidents are reported to which contacts at the site. The site names one or more responsible persons that can configure whom to inform, in form of an e-mail address, for which IP-addresses at the site. Thus, a site with separate security teams for the site as a whole and the Grid could configure two contacts (i.e. both security teams) for the IP-addresses of the Grids subnet and one contact (the site security team) for the rest of the site. This does not impose a bottleneck, as DFN-CERT only supplies a resource, but is not involved with the workload of configuring every site, which is distributed among the constituency. The per-Grid mailing-list has been proposed in the D-Grid project but will probably only used if an incident occurs that really affects the whole Grid.

The approach described concentrate on sites that supply resources to the Grid. Sites that have only users of a Grid are currently not covered.

International Cooperation

Experience with CSIRT operation has shown, that international cooperation is imperative to successful establishment of CSIRTs. Without it, incident handling coordination would not be possible across national or network borders and announcements of new security threats would reach the constituency much later. For CSIRTs, two major bodies exist for European teams that further cooperation: FIRST and Terenas TF-CSRT. The former has a worldwide focus while the later is mostly concerned with European cooperation (there is a counterpart in Asia, APCERT, that full fills a similar role in that region as TF-CSIRT). At the Grid side, there is the Joint Security Group from the LCG Grid [9], to name just one. While TF-CSIRT has concerned itself with Grids since 2005, which resulted in a first paper regarding “CSIRTs and Grids”, no further activity had taken place and no activity at all had happened within FIRST.

At at joint meeting of FIRST and TF-CSIRT in January 2006, which involved also members of the Grid community, it had been agreed upon that to further international cooperation between CSIRTs with regards to Grid incidents, an exchange forum had to be established, where relevant data could be shared. This had to include relevant parties from the Grid community also. During the next months, a mailing list had been set up: “grid-cert@grid-security.net”. A website with a Wiki is in the planing to further enhance cooperation. Also, "Incident handling and security guidelines of NREN Grids" have become part of Terenas TF-CSIRT terms of reference since September 2006. Despite considerable initial interest, concrete participation has been low so far.

Technical Challenges

To handle the technical part of Grid incidents as well as to be able to pro actively help sites in securing their Grid infrastructure, a CSIRT has to develop an understanding about the software used in the Grids of their constituency.

Grid Software Expertise

The underlying operating systems are common systems, like Linux, and these are well understood by CSIRTs. The next layer, the Grid middle ware, is composed of big software packages like UNICORE, the Globus Toolkit or gLite, that facilitate access to storage and computing resources, as well as monitoring, directory services and authentication across virtual organisations. Additionally, auxiliary packages like GridSphere, Shibboleth or Torque/OpenPBS are used by many Grids.

These software packages are currently very little understood by CSIRTs. Exacerbating this problem is that there are only a few people in the academic community itself that fully understand this software. To solve this problem, a CSIRT has no only to acquire the knowledge about what the software is and how it is used, but mostly importantly about

- how to securely configure it
- how the software interacts with other software, both operating system and other Grid software
- how to detect break-ins
- to estimate the damage from a break-in, especially which other software components or Grid resources are affected

Several approaches could be taken. CSIRTs could do research into the software packages by themselves. While this has been done successfully with other software packages or with small Grid software packages like UNICORE, this approach is not feasible with the larger packages like Globus Toolkit or gLite. CSIRTs simply lack the resources (personal, systems to test on, etc.) to do this. Also, the test set-up chosen by a coordinating CSIRT may no be representative for the installations in the Grid.

The other way is to cooperate with an existing test site in the academic network. This also establishes contacts to persons with in-depth knowledge about Grid software. Also, the test site is more likely to reflect the production set-up. In practice, this means a penetration test of a Grid site. Such test start with a port scan and application scan of the sites

IP-addresses to find out which services are offered. DFN-CERT did such a scan of a test site in the second half of 2006. Some of the key results were

- Attackers can, with basic standard tools like nmap, netcat, or OpenSSL, locate Grid sites and identify to which Grid they belong.
- Grid services can be identified, even if running on non-standard port numbers. Signatures of Grid services have been obtained, that can be used with the nmap port scanner.
- Even with custom Linux distributions developed for use in Grid sites, services remain open that are not needed or services that are needed are configured in an insecure way, like SSH servers allowing logins with passwords, which makes the site vulnerable to password guessing attacks or still allow SSH protocol version 1, which is insecure.

The results of the port scanning form the base for additional CSIRT services. With it, analysts from CSIRTs can look for scans to Grid services in either production networks or in a network telescope, "a portion of routed IP address space on which little or no legitimate traffic exists" [10]. Also, the results can be used to build simple, low-interaction honeypots, for example with Honeyd [11]. The first approach has been employed on DFN-CERTs network telescope, but so far without results, i.e. no Grid-related port scanning has been noted.

Vulnerability Handling

Two vulnerabilities (CVE-2006-4232, -4233) in the Globus Toolkit, three vulnerabilities (CVE-2006-1506, -2930, -3941) in the Sun Grid Engine, and two vulnerabilities (CVE-2006-5616, -5677) in the OpenPBS and TORQUE schedulers have been reported in 2006 through various sources to the Common Vulnerabilities and Exposures (CVE) project, which maintains a public database of software vulnerabilities, while only one such vulnerability had been reported in the years before (Sun Grid Engine, CVE-2003-0841). This shows a growing interest in Grid software by the security experts and underground "hacker communities".

Although the basic procedures of handling vulnerabilities are the same, whether for normal software or for Grid software, the concrete task of obtaining the information puts up some challenges. While many Grid software packages are open source and developed among the same lines as standard open source packages, the standard security practices, like open mailing lists for security advisories or signed software packages, were often not followed at the beginning of the project (2005). Today, gLite uses signed RPM packages while the Globus Toolkit uses SHA-1 checksums provided on the web page of the project. The later is not sufficiently secure against compromises of the distribution servers. But the Globus Project is the only one that provides a public mailing list for announcements of vulnerabilities [12]. It currently remains open how to persuade other Grid projects to openly announce security problems with their software.

Conclusions

In December 2006, DFN-CERT officially started its Grid-CERT service in the framework of the D-Grid project. Since then. Some incidents were reported on cluster systems that are planned to be used in Grid, but so far, no incidents were reported that could be classified as Grid-related. However, many of the D-Grid communities are not yet fully operational, so this may change in the future. Other academic CSIRTs have had Grid-related incidents, almost all of them were related to the loss of credentials (private X.509 keys) that could be handled with the existing frameworks of Grids and CSIRTs.

The D-Grid Initiative is an ongoing project and the establishment of CSIRT services for Grids is still at an early stage. The establishment of communication channels to the various Grid communities as well as the gaining of knowledge about Grid software has required DFN-CERT to take new ways, even though the basic principles of CSIRT operation remain the same.

The establishment and piloting of CSIRT services for Grids will evolve when the the community projects evolve. One of the D-Grid projects has announced that it is considering the integration of DRM techniques into its security architecture. How this will affect CSIRT operations is currently unknown. Also, CSIRT operations are evolving too. Many CSIRTs are supplementing traditional incident reporting by sites and other CSIRTs with automated reports generated from distributed sensors, like network telescopes, honeypots and intrusion detection systems. Also, CSIRTs are working on systems for sharing of sensor information and a common analysis platform with the final goal of building an early warning system. Grids as well as other new technological developments will have to be integrated in these platforms and special sensors for Grids may have to be developed to achieve this.

In the area of international cooperation there has been much interest but little concrete results so far. Whether this will change when other CSIRTs or Grid communities can more experience over time remains to be seen. It seems to be too early to make final conclusions.

References

[1] A. Cormack: “CSIRTS and Grids”, http://www.terena.nl/activities/tf-csirt/doc/CSIRTs-and-Grids-v0.5.pdf

[2] FIRST homepage: http://www.first.org/

[3] Terena TF-CSIRT homepage: http://www.terena.org/activities/tf-csirt/

[4] Cert Coordination Center: “CSIRT Services”, http://www.cert.org/csirts/services.html

[5]I. Foster, C. Kesselman, S. Tuecke: “The Anatomy of the Grid – Enabling scalable virtual organisations”, 2001, http://www.globus.org/alliance/publications/papers/anatomy.pdf

[6] Open Science Grid: “Grid Security Incidents Handling and Response Guide”, November 2004, http://osg-docdb.opensciencegrid.org/0000/000019/002/OSG_incident_handling_v1.0.pdf

[7] A. Cormack, D. Stikvoort, W. Woeber, A. Robachevsky: “IRT Object in the RIPE Database”, 2002 http://www.ripe.net/docs/irt-object.html

[8] D. Crocker: RFC 2142: “Mailbox Names for Common Services, Roles and Functions”, 1997, http://www.ietf.org/rfc/rfc2142.txt

[9] LCG Joint Security Group, http://proj-lcg-security.web.cern.ch/proj-lcg-security/

[10] Network Telescope definition: http://www.caida.org/analysis/security/telescope/

[11] Honeyd homepage: http://www.honeyd.org

[12] Globus Project: “Reporting Potential Security Vulnerabilities”, http://dev.globus.org/wiki/Mailing_Lists#Reporting_Potential_Security_Vulnerabilities

[13] Common Vulnerabilities and Exposures project homepage: http://cve.mitre.org/