TF-CSIRT Activity Update: European CSIRT Collaboration

Gorazd Božič, SI-CERT
TF-CSIRT Chair
gorazd.bozic@arnes.si
http://www.terena.nl/tech/task-forces/tf-csirt/

Abstract

European CSIRTs have been examining different ways of cooperation since early 1990s. After trying several organisational models, the task force TF-CSIRT was formed in 2000 under the umbrella of TERENA (Trans-European Research and Education Networking Association). TF-CSIRT encompasses teams from academic, commercial and governmental organisations. The group spawned several projects addressing common issues: trust relationships between teams, a formal model for exchange of incident-related data, the training of CSIRT staff, problems related to differences in legislation, and so on. In continuous communications with the European Commission, TF-CSIRT has established itself as a credible partner in the area of network security. The growing number of participants in TF-CSIRT, as well as teams from elsewhere expressing interest in particular results of the group, can be regarded as a sign of the successfull efforts European CSIRTs have undertaken.

1 Background

The first European CSIRTs were formed in the early 1990's. Their work was done in isolation at first, but FIRST soon provided a platform for collaboration between teams worldwide. On a different level, teams from Europe started exploring ways of regional cooperation that would deal with their own specifics and diversity (many different countries with different cultures and legal systems, for example). One noted example of collaboration was the EuroCERT project, whose aim was to provide incident handling capability on a trans-national scale. This project was designed in a top-down manner and outsourced to a third party. By the end of this project (September 1999), it was clear that this kind of service was inadequate at this stage due to differences in participating teams' requirements and the needs of their constituencies.

Soon afterwards, talks between teams on future models of cooperation continued and resulted in a creation of TERENA TF-CSIRT[1] in May 2000. This time, the approach was quite different – not highly formalised, it concentrated on discussion of common issues and problems from which several well-defined projects emerged.

2 How TF-CSIRT Works

The TF-CSIRT task force is established under the auspices of the TERENA Technical Programme to promote the collaboration between Computer Security Incident Response Teams (CSIRTs) in Europe. TF-CSIRT's "Terms of Reference" document defines aims of the TF-CSIRT, participation, it's chair and secretary, deliverables of the task force and it's mandate. It also specifies that participants meet in face-to-face meetings three times a year, while between meetings all discussions are carried out on the TF-CSIRT's mailing list.

[1] http://www.terena.nl/tech/task-forces/tf-csirt/

The Task Force chair is nominated by participants from the group itself while TERENA appoints a secretary who provides support for most of logistical and organisational issues related to meetings, mailing list and web-site administration. Meetings are hosted by participant's organisations on a voluntary basis (this approach has proven itself quite successful). Each meeting is divided in two days: the first day is dedicated to seminar sessions with speakers both from within the group as well as invited speakers not normally involved in TF-CSIRT, while the second day is dedicated to a meeting where work of the group is evaluated, issues are discussed, and future work is decided on. Meetings' agendas are of course not limited only to deliverables defined in Terms of Reference, it is also an opportunity for participants to discuss all other matters that they find relevant to their work in CSIRTs.

Instead of a strict hierarchical approach to defining deliverables, working groups and other work items, TF-CSIRT relies on active participation of individuals and their initiative to outline possible common issues and work on them in smaller working groups.

At the time of the writing of this paper, TF-CSIRT is in it's second two-year mandate, which will end in May 2004. It is my expectation that participants of TF-CSIRT will decide to propose another two-year extension of the task force to TERENA Technical Committee.

3 Selected Deliverables

This section describes some of TF-CSIRT's deliverables that are thought to be of interest not only to the task force itself but also to a wider CSIRT community. The full list of deliverables of the task force is listed in the TF-CSIRT *Terms of Reference* document.[2]

3.1 Trusted Introducer (TI)

The notion of trust between teams is a well-known issue in the CSIRT community. In general, informal contacts between teams proved to be insufficient for work in incident resolution, especially given the rapid growth of the number of teams: the bilateral approach does simply not scale. This is why an accreditation scheme was designed to provide a basic degree of trustworthiness which can be checked by an independent third party. The "Trusted Introducer" (TI)[3] maintains a directory of European CSIRTs, including a label showing their accreditation status.

Team's status can be one of the following:

- "listed" means only that CSIRT is "known" and is listed in the TI directory
- "accreditted" status shows that CSIRT has applied for accrediation status and has followed a strict procedure for supplying information to TI related to it's constituency, contact details and some general operational practices
- "accreditation candidate" is an intermediary status for a *listed* team that has applied for *accreditted* status; the process of accredittation in whole takes no longer than 4 months to complete

Implementation of TI and operation of the service are commissioned by TERENA via a public tender to a third party. TI provides for meetings of accreditted teams adjacent to TF-CSIRT meetings, while the *TI Review Board* reviews the operation of the TI and addresses all special issues that might result from its operation.

The implemented scheme allows for future enhancements (like adding a Code of Conduct, or certification) and additional services that can be provided to a group of TI accredited teams.

[2] http://www.terena.nl/tech/task-forces/tf-csirt/TSec(02)017rev1-ToRTF-CSIRT.pdf

[3] http://ti.terena.nl/

3.2 RIPE IRT Object

One commonly perceived problem is finding the right points of contact for a given network. Directing incident reports to network contacts is not always successful as addresses supplied are often those of persons or teams handling registration of IP addresses, DNS entries and so forth. This led to the idea of having a separate *IRT* object, which would be used exclusively for CSIRTs. TF-CSIRT compiled a set of practical requirements, which were then discussed in the RIPE database group. The result is the *IRT object*[4] in the RIPE NCC database, which is used to describe an individual CSIRT and can be tied with objects representing allocated IP address space.

```
irt:           IRT-SI-CERT
address:       ARNES SI-CERT
address:       Jamova 39, p.p. 7
address:       SI-1001 Ljubljana
address:       Slovenia
phone:         +386 1 479 88 22
fax-no:        +386 1 479 88 99
e-mail:        si-cert@arnes.si
signature:     PGPKEY-E236BFD7
encryption:    PGPKEY-E236BFD7
admin-c:       TI123-RIPE
tech-c:        TI123-RIPE
auth:          PGPKEY-E236BFD7
auth:          PGPKEY-09E1DBB5
remarks:       Emergency telephone number +386 14798822 (GMT+1/GMT+2 with DST)
remarks:       http://www.trusted-introducer.nl/teams/si-cert.html
remarks:       This is an accredited IRT (level 2)
irt-nfy:       si-cert@arnes.si
notify:        tiirt@stelvio.nl
notify:        si-cert@arnes.si
mnt-by:        TRUSTED-INTRODUCER-MNT
changed:       gert-henk.bakker@stelvio.nl 20031222
source:        RIPE
```

IRT object provides contact information for the team, PGP keys of the team and also keys that are used when referencing *inetnum* objects to IRT object. The team representative must authenticate references to their IRT object or can alternatively delegate authentication to someone else. The IRT object also includes a reference to its maintainer. For TI accreddited teams (see previous section) this can be the TI service in which case the team's TI status also appears in the IRT object itself.

A query for IRT objects always returns the most specific inetnum object with the 'mnt-irt' reference present. This allows for tying large blocks of IP space to an ISP's CSIRT, while particular organizations that are assigned a subset of IP space can reference their own CSIRT if they have one.

3.3 TRANSITS: Training of CSIRT Staff[5]

Due to the high workload of the CSIRT staff, training new staff members is always a problem. Undoubtedly the best way to transfer the knowledge is from existing operational staff. For this reason, members of TF-CSIRT developed material for two-day courses in different modules, covering operational, legal, technical, organisational and vulnerability issues. European Commission has funded delivery and development of the materials for three years, as well as the two courses a year. The materials are available for others to use on a non-commercial basis, subject to certain conditions to ensure quality, and there have been at least as many courses held under these rules as under the EC ones.

[4] http://www.ripe.net/ripe/docs/irt-object.html

[5] Training of Network Security Incident Teams Staff, http://www.ist-transits.org/

3.4 Clearing House for Incident Handling Tools (CHIHT)

The goal of CHIHT[6] is to provide a collection of tools and guidelines for their use intended for incident handling teams. The information given would reflect the experience of a number of European CSIRTs. This kind of collection should help both new and existing teams, especially with the planned additions of incident handling workflows, procedures and best practices that will accompany the collected tools.

3.5 IODEF - Incident Object Description and Exchange Format

The IODEF working group was among the first undertakings of TF-CSIRT. Its goal was to define a common data format and common exchange procedures for sharing information needed to handle an incident between different CSIRTs, that would allow both known and new types of incidents to be formatted and exchanged. IODEF WG work resulted in RFC 3067, "TERENA's Incident Object Description and Exchange Format Requirements"[7] and by 2002, the work on IODEF was transferred to IETF INCH[8] working group. Currently, the use of IODEF/IDMEF models in incident-handling tools is being discussed (see also the section on eCSIRT.net below).

4 Related projects

It is certainly worth mentioning that one of the more important aspects of TF-CSIRT are regular meetings where participants have the opportunity to discuss things in person. This exchange of ideas and views leads to various working groups and projects. All of these do not necessarily find their way to the list of deliverables in the *TF-CSIRT Terms of Reference*[9] document for various reasons (for various practical reasons, not because of formalities). In the end, all these projects benefit the whole community. Following is a brief list of selected such projects and efforts.

4.1 eCSIRT.net: Building a European CSIRT Network

eCSIRT.net[10] brought together a number of European CSIRT teams in order to deploy new techniques and practices that will enable incident response teams to efficiently cooperate and exchange incident related data, and to collect shared data for statistical and knowledge-base purposes. The IODEF/IDMEF model was used as a common language between partners in the project. A network of IDS sensors was deployed in order to provide statistics and alert functions to participating teams. The continuation of the project is currently under discussion within TF-CSIRT, possibly as a service for TI accredited teams.

4.2 EISPP: European Information Security Promotion Programme

EISPP[11] is targeted mainly towards SMEs that have a hard time dealing with security issues. It aims to develop a shared infrastructure between established "Centres of Expertise" (existing CSIRTs), a repository of preventive material, a common advisory format and a distribution model for disseminating information to the SMEs.

4.3 RTIR Working Group

Anyone with at least some experience in incident-response work has asked himself or herself the following: "What kind of software do other teams use for incident tracking?" Most of FIRST teams use a combination of homegrown tools, interfaces and sometimes pieces of

[6] http://chiht.dfn-cert.de/

[7] http://www.ietf.org/rfc/rfc3067.txt

[8] http://www.ietf.org/html.charters/inch-charter.html

[9] http://www.terena.nl/tech/task-forces/tf-csirt/TSec(02)017rev1-ToRTF-CSIRT.pdf

[10] http://www.ecsirt.net/

[11] http://www.eispp.net/

commercial software. And nobody is really happy with their solution, as far as I have been able to tell.

In 2002, JANET-CERT started talks with bestpractical.com, the authors of open-source ticket-tracking system called Request Tracker (RT)[12]. Their goal was to have a version of RT that is tailored to the needs of a CSIRT. The specialised version (in a form of an add-on to RT) called RTIR, "Request Tracker for Incident Response" was released in August 2003 and before that presented also at FIRST 2003 Conference in Ottawa. Currently the RTIR is used in handling incidents by several European teams. Since incident tracking is a complex task with sometimes complicated workflow schemas, the plan is to collect experience and requirements for additional features. For this purpose, a RTIR Working Group has recently been formed from TF-CSIRT participants which will coordinate efforts on further development and enhancements of the tool.

5 Wider Cooperation

TF-CSIRT has also established communication outside of its community. Representatives of law enforcement are regularly invited to speak at TF-CSIRT meetings, and the continuous exchange of views with European Commission (EC) representatives has been very fruitful with regards to several EC-funded projects, such as "Computer Security Incident Response Team Handbook of Legislative Procedures"[13]. Discussions with the EC also included the EU project of setting up a *European Network and Information Security Agency* (ENISA). Also an exchange of ideas with Asian-Pacific collaboration effort (APCERT) drew much interest from the group. Further activities on a continuous exchange of information between these two regional initiatives are under way.

Since many teams that participate in TF-CSIRT are also FIRST members, discussions of FIRST issues are also a regular item on the meetings' agenda.

6 Outlook for the Future

TF-CSIRT proved to be a very solid platform for exchange of ideas between European CSIRTs and has introduced several projects and working groups which have already or are in the process of bringing results to the CSIRT community. It is regarded as a beneficial and much needed platform for regional cooperation. The diversity of teams serving different constituencies and originating in different countries makes a kind of "bottom-up" working model a very convenient way for these teams to work together.

[12] http://www.bestpractical.com/

[13] http://www.iaac.org.uk/csirt.htm