Meeting to Discuss Future Collaborative Activities between CERTs in Europe

---

Revised Minutes of the 2nd Meeting to Discuss Collaborative Activities Between CERTs in Europe

Amsterdam, 21 January 2000

Issued by: John Dyer, 28 Jan 2000

Agenda

- Welcome and apologies
- Round of Introductions
- Minutes and Actions from the Last Meeting
- Presentation of "Trusted Introducer" Report
- Discussion and Decision on "Trusted Introducer" way forward
- Report on Status of TERENA/UKERNA project on Information for taking Legal Action
- Incident Classification Schema
- Progress of Open Actions
- TERENA's Role
- Date of Next Meeting
- Any Other Business

1. Welcome and apologies

Apologies were received from: Danilo Bruschi (CERT-IT), Marcus Pattloch (DFN), David Chadwick (University of Salford), Olaf Schjelderup (Uninett), Pege Gustafsson (TeliaCERT) and Marc Roger (BELNET).

2. Round of Introductions

The meeting was attended by 25 delegates representing 18 organisations / networks from 12 countries. A list of the attendees can be found in the appendix to these minutes.

3. Minutes of the last meeting

The Minutes of the last meeting of the CERT Coordination Group (CERT-COORD) which took place on 24 September 1999 were accepted without change. The actions arising from the last meeting are covered by the agenda items and discussed below.

4. Presentation of the Report on the "Trusted Introducer" Process

The report for a foundation on which trust can be based was presented by Don Stikvoort. The presentation closely followed the structure and text of the report itself. Both slides and full report text can be found on the TERENA web site. Don explained that he thought the community of CERTs was currently too young and not sufficiently mature to warrant a formal certification scheme. There is an urgent need for a foundation on which to base trust in an rapidly expanding community where reliance on personal contacts is becoming increasingly difficult because of the large number of people involved.

The report presents a three phase model in which CERTs are encouraged to advance reasonably quickly from the entry level to the highest level through one intermediate step.

The major objective behind this scheme is not to provide a certificate of competence, but to provide information about a team including the protocol by which it was collected (and by whom), as a means by which third parties (other CERTs) can make a judgement about how much trust they wish to accord to a (new) team. Don's view is that there are several organisations that should be considered potential candidates to provide the implementation and he went on to explain the pros and cons for each.

- The Forum of Incident Response and Security Teams (FIRST) is an organisation, formed in 1990 as an international consortium of computer incident response and security teams, who work together to handle computer security incidents and to promote preventative activities. The FIRST secretariat is based in the United States of America. FIRST is currently going through a transition to an organisation that could take on the "trusted introducer" role, but probably will not be in a suitable state for at least a couple more years. This is too long to wait for our needs in Europe. It was noted that current FIRST membership costs the IRT's that belong 500 US$ per annum irrespective of the community that they serve. More information on FIRST can be found at their web site http://www.first.org/.
- IETF - Although the IETF has a Working Group looking at Guidelines and Recommendations for Security Incident Processing (grip), (for more information see http://www.kossakowski.de/grip/), the IETF does not set up infrastructure so is clearly an inappropriate place to consider for the implementation of this function.
- Another possibility is for the function of "trusted introducer" to be associated with the formal law enforcement authorities. It was generally thought that there could be a problem with this in that the formal process of law acts too slowly and often attracts publicity that we wish to avoid. This might lead to high numbers of teams not wanting to be involved in a process under this umbrella.
- TERENA has been active by providing an umbrella under which CERT co-ordination takes place for a considerable amount of time, dating back before the production of the CERTs in Europe Report, published in October 1995 (http://www.eurocert.net/history/cert-task-force-report.html). It was thought that although TERENA has a good track record in bringing people working in this area together, the organisation was not (currently) part of the web of trust and would find it difficult to undertake the executive function of "trusted introducer".

The consensus of the meeting was that the activity should be carried out under the TERENA umbrella, but the implementation of the executive function of "trusted introducer" should be sub-contracted to entity/entities within the web of trust.

In the discussion of the functions described in the report, significant attention was devoted to understanding the element of the site visit. It was agreed that a site visit might be necessary in some, but not all, instances for checking the written claims of (new) teams and evaluating physical security etc. It was made very clear that if a site visit was undertaken the protocol adopted must be documented. This would demonstrate the objectivity of the assessment. A number of other issues were also debated and the report authors were given guidance on changes that should be made for the final version of the report. These included:

- The need to establish in (Appendix E) that teams being evaluated have some sort of positive track record, e.g. by listing some of the CERTs that they have actively collaborated with.
- The idea of an IRT's details being displayed on a public web site might discourage some teams from seeking assessment by this process. It might be necessary to maintain a public list and a confidential list viewable only by Level 2 teams. - Public awareness is considered a very positive attribute by most teams in the process of building the web of trust.
- The Review Board, mentioned in the report, should have a fixed membership consisting of at most 10 people.

Don Stikvoort went on to explain the process and implementation in some detail. It was agreed that the process being described is scaleable (up to maybe 100 teams) provided it is given sufficient time to get going properly. One member of the meeting suggested that since the RIPE NCC will have 2000 members at some time during the year 2000, if only 25% of them operated a CERT, then the mechanism would have to deal with potentially 500 teams. It was thought that being part of the web of trust fostered by the mechanism being described would be a benefit and would have a positive effect on the number of teams applying for assessment. Once the number gets to about 100 or so, it will be necessary to a move to something more akin to the original EuroCERT plan, but by that time the operation would be well above the critical mass of membership which was found so difficult to achieve before.

5. Discussion and Decision on "Trusted Introducer" Way Forward

The "trusted introducer" proposal was well received by the meeting. There was much enthusiasm and it was felt that something lightweight such as Don suggested should be got going without delay. There was overwhelming support for this course of action and the meeting requested TERENA to start the implementation process.

It was agreed that the various tasks described in Don's report should be divided in parts that are limited both in extent and in time, and that each of these parts should be subcontracted separately by TERENA or taken on by TERENA itself (or others). This

division in parts should be in the documentation to be produced by TERENA in the next 4-6 weeks.

In order to reach the sustainable level of funding it is clear that the system will have to reach both commercial and NRN communities. The issue of how TERENA would approach this was raised. It was agreed by all that the primary target should be the NRN community and once this had been properly satisfied, we should target ISPs in the RIPE community and only then open it up to all-comers. This phased approach will allow the "trusted introducer" scheme to gain experience in a known environment before expanding.

With respect to the funding, Don Stikvoort made a tentative suggestion of a figure around 200 Euro per team per year. There was universal agreement that the figure had to be low, although no agreement on the precise level of the fee. It was clear that there should not be a direct connection between making a payment and receiving Level 2 status. Objectivity must be seen to be the over-riding element in granting status. One suggestion that found support was the notion of a voluntary contribution. Whilst the voluntary contribution might apply for Level 0 and Level 1, a contribution would be mandatory after Level 2 status had been achieved.

Having reached agreement to go ahead with implementation, the chairman requested that TERENA prepare a document describing the requirements and propose a timescale. It was agreed that the timescale TERENA should be aiming for is as follows :

- Production of documentation calling for bids - 4-6 weeks
- Out for community comment - 2 weeks
- Revisions and issue - 1 week
- Period allowed for formal responses - 3 weeks
- Award of contract - 1 week

In practical terms, this means that there should be something in place before June 2000. The consensus is that this should run for a year in the first instance. TERENA agreed to draft the required documents.

6. Survey of Legal Requirements (UKERNA / TERENA contract)

Andrew Cormack of UKERNA presented the original objectives of the project proposed by Damir Rajnovic from UKERNA. The aim had been to collect information from the authorities in six countries giving contact information and a description of the sort of information that would be required in order to take legal action in cases of computer crime. The task had proved much more difficult than had been envisaged as to-date there is very little information available anywhere. A conference was held in London during late 1999 attended by over 200 law enforcement agents interested in solving IT crime cases, however many of the sessions at the event were restricted to recognised law enforcement agents. It seems that the view since the meeting is that it may have been better to open at least some of these closed sessions to suitably qualified delegates.

One of the outputs of the conference is an agreement on a minimum set of procedures which will be internationally acceptable for taking legal action, at least in the industrialised nations. Andrew will attempt to get hold of a copy of this document and circulate to CERT-COORD group.

In view of the apparent unfeasibility of carrying out the project as originally envisaged, TERENA and UKERNA have jointly decided not to pursue it any further.

7. Classification of Security Related Incidents

Andrew Cormack (UKERNA) and Jan Meijer (SURFnet) presented a top level classification of incidents scheme. The rationale behind this is that both UKERNA and SURFnet had reasonably similar lists in place and it seemed sensible to exchange statistics in a standard way so as to be able to compare trends. This would enable:

- Identification of anomalies
- Following of trends
- Identification of new attack types
- Substantive evidence of performance for management

There have been at least three attempts at classification from other quarters in the past:

- A Common Language for Computer Security Incidents by Howard and Longstaff, published in October 1998 describes the nature and motivation of attacks on 7 axes (type of attacker, the tool they used, vulnerability, action that was undertaken, target, the unauthorized result and the objective of the hacker). Whilst this was useful in understanding the nature of hacking in some detail, it is overly complex and would not meet the simple objectives of exchanging statistics. Further details of this work can be found at: http://www.cert.org/research/taxonomy_988667.pdf
- The Intrusion Detection Exchange Format Working Group of the IETF (idwg) http://www.ietf.org/html.charters/idwg-charter.html web site gives details of some work that is being undertaken to provide automated real-time communications about events using SMTP format or XML.
- Common Vulnerabilities and Exposures (CVE) http://www.cve.mitre.org/ gives a complex and rather cryptic set of identifiers. It provides a flat list of common/typical vulnerabilities and exposures. The level of detail is far greater than is required for our community and is not suitable for the sort of high level exchange of information that TERENA has in mind.

The SURFnet/UKERNA scheme consists of 11 top level classifications for the purposes of statistics exchange with other teams:

- Abusive Communications
- Denial of Service
- Packet Sniffing

- Other
- Probe
- Root Compromise
- Spam
- Trojan
- Unauthorised Use
- Virus
- Warez

In addition, the schema has the concept of "extensions" that provide for other locally defined categories which are intended for internal or local use only. Such extension could include headings such as: "Administrative" or "Query" which are needed for local reporting tasks.

The proposed classification was well received and adopted by the meeting. It was agreed that it would be useful to continue to develop the scheme and include a wider community in the discussions (such as the CERT-CC community). It was agreed that CERT-CC should be invited to join the email list to assist this process. So as to not burden CERT-CC (and others) with our general discussions on European CERT coordination, it was agreed to open a second mailing list consisting of all current cert-coord members where interested external parties could be added. This list will be known as incident-taxonomy@terena.nl. Requests for additions or removals should be sent to Yuri Demchenko demch@terena.nl.

In response to questions on whether teams would be willing to exchange their statistics, a large majority said they would exchange statistics with other trusted teams and more than half the teams said they would be happy for their statistics to be displayed publicly.

In discussion with those that did not want to expose their figures, the motivation was given that it could reveal areas of vulnerability to hackers. In response to this, many teams thought that displaying such details would equally give a message of vigilance and was therefore a positive thing to do.

8. Clearing House for Tools

It is clear that there are many collections of software for hackers, but no single repository for tools that assist in dealing with Incident Response.

It was agreed that the Clearing House for Tools would be an area of the TERENA Web server were pointers to Incident Response Tools and information about them, could be shared. Members of the CERT-COORD group should mail pointers and information about tools to Yuri Demchenko at TERENA (demch@terena.nl). The information should include notes on usage experience.

9. Regular Meetings and Workshops

It was generally agreed that there are many things that teams will need to do to achieve Level 2 status under the "trusted introducer" scheme. Workshops would be valuable in assisting new teams in meeting the criteria. Some of the experienced teams present mentioned that they would be interested to send their new team members to such training workshops. This was particularly relevant because many teams are faced with a high number of staff changes.

In addition there is a need for advanced teams to be able to present their latest developments and techniques to other teams. The consensus of the meeting was that both these events are a good thing, but it would be wrong to try and address both requirements with single events. It was agreed that there is a demonstrable need for both:

- Seminars for presentation of new techniques, exchange of experiences, discussion of common issues etc.
- Training workshops to teach new teams and new staff members of existing teams

It was agreed that the seminars should run before or after CERT Coordination meetings and should last one full day with maybe 4 or 5 detailed presentations and some time devoted to discussion. There was little interest in the suggestion of half-day events with 2-3 presentations. Many of the teams present also expressed a positive intention to be involved with the training element, however the training content will need further discussion at the next meeting. The first seminar will be associated with the next cert-coord meeting.

10. Need for a Security Entry in the RIPE Database

At the previous meeting held on 24 September 1999, it was thought that an entry detailing the appropriate security contact for each ISP would be a useful thing to have. At this meeting, there was a view expressed that the brokerage activity would for the limited number of ISPs that have their own CERT provide similar information to a security entry in the RIPE database, albeit by a different mechanism. However the RIPE database and how to use it is very well known and might be a more suitable vehicle on that basis alone. On balance, it was agreed that the group should still investigate the possibility of using the RIPE database. Jacques Schuurman agreed to draft a one page statement of the requirements on what new attributes would have to be associated with what objects. This would then be mailed to the RIPE WG-Database list. A presentation and discussion on what the RIPE database could mean for the CERT community could be a useful topic in the next seminar.

11. Web Information on Existing CERTs

In the September 1999 meeting UKERNA had volunteered to maintain the web page with contact information on CERTs that had resulted from EuroCERT, for an unlimited period of time. Since then it had implemented at least one update. The meeting decided to continue with this arrangement. The web page at the UKERNA server will be the

authoritative contact list and all updates should be sent to Andrew Cormack at UKERNA for inclusion.

12. Help for New CERTs

CERT-NL kindly offered to provide help to new CERTs as an interim solution at the first meeting in September 1999. Since that meeting, no requests had been received by CERT-NL. CERT-NL agreed to continue to provide a first point of contact on an interim basis until the situation is formalised. JANET-CERT reported that they had provided support in one case since the last meeting.

A more permanent solution for assistance to new CERTs still has to be found. In the September meeting this function had been envisaged to be part of the Trust Broker function, next to the "trusted introducer" process and a number of other responsibilities. Plans for these would be developed and discussed in subsequent CERT-COORD meetings.

13. TERENA's Role

Brian Gilmore and John Dyer explained that the CERT Coordination activity had been supported by TERENA in an ad-hoc manner since the end of SIRCE. Whilst this had been effective, if the support is to continue it should have some formal status in the structural framework of the organisation. The correct way to support this sort of focussed work is through the formation of a Task Force which must have an agreed programme of work and set of deliverables described in a charter. There would of course be the need to select a Task Force convenor. The meeting was keen for the work to continue in the TERENA context as a Task Force. The Secretariat agreed to produce a draft charter that will be circulated to the CERT-COORD list before the next meeting. Once agreed on, the charter will be submitted to the TERENA Technical Committee for formal adoption

14. Date of Next Meeting

11-12 May 2000, Amsterdam. This will be a one day meeting followed by a 1 day CERT seminar.

[NOTE: Since the meeting it has been discovered that hotel rooms are extremely difficult to find in Amsterdam around those dates. The TERENA Secretariat will find a solution, if needed by moving the event to another location. Information will be sent to the cert-coord@terena.nl list as soon as possible.]

Summary of Actions

ACTION ITEM	RESOLUTION
1. Prepare an Implementation Plan and Timeline and documentation for the "trusted introducer" scheme.	TERENA
2. Obtain a copy of Law Enforcement Agents list of minimum requirements for taking legal action	Andrew Cormack to attempt to obtain copy
3. Establish a Clearing House of Incident Response Tools	CERT-COORD members to mail information to Yuri Demchenko at TERENA demch@terena.nl
4. Draft one page statement of requirements for security entry in RIPE database and mail to RIPE list	Jacques Schuurman to draft
5. Open new Incident Classification email distribution list	TERENA
6. Draft TF Charter, circulate to the cert-coord list and submit to the TTC once agreed	TERENA
7 Organise Next Meeting (11-12 May 2000), CERT COORDINATION and SEMINAR	TERENA

Attendees

Wilfried Wober	UniVie/ACOnet
Gorazd Bozic	ARNES
Pascal Delmoitie	BELNET
Denise Heagerty	CERN
David Crochemore	CERT-RENATER
Kick Fronenbroek	CONCERT
David Harmelin	DANTE
Gemma Perez	ESCERT

Jordi Linares	ESCERT
Leila Pohjolainen	FUNET-CSC
Roberto Cecchini	GARR-CERT
Christos Aposkitis	GRNET-CERT
Francisco Monserrat	IRIS-CERT/RedIRIS
Chelo Malagon	IRIS-CERT/RedIRIS
Klaus Peter Kossakowski	-
Don Stikvoort	Stelvio
Jacques Schuurman	SURFnet/CERT-NL
Jan Meijer	SURFnet/CERT-NL
Christoph Graf	SWITCH
John Dyer	TERENA
Brian Gilmore	TERENA
Yuri Demchenko	TERENA
Karel Vietsch	TERENA
Andrew Cormack	UKERNA
Per Arne Enstad	UNINETT

Apologies

Marc Roger	BELNET
Danilo Bruschi	CERT-IT
Marcus Pattloch	DFN
David Chadwick	University of Salford
Pege Gustafsson	TeliaCERT CC
Olav Schjelderup	UNINETT