Minutes of the 2nd TF-CSIRT Meeting

19 January 2001
Universitat Politècnica de Catalunya, Barcelona, Spain

John Dyer, TERENA
01 February 2001

1. Welcome and Apologies

Apologies were received from:

Don Stikvoort, Stelvio
Brian Gilmore, University of Edinburgh
David Harmelin, DANTE

2. Round of Introductions

A list of the 38 attendees for the meeting is attached as an annex to these minutes.

3. Minutes of the 1st TF-CSIRT Meeting (Paris, 29 September 2000)

The minutes of the previous meeting held on 29 September 2000 were approved without change.

Status of open actions from previous meetings

ACTION			STATUS
0-2	TI	Produce document(s) to explain benefits of TI to managers	Not yet done - on the agenda at item 4
0-3	TERENA and TI	Discuss and arrange server certificate for TI Web site	Not yet done - on the agenda at item 4
0-9	Secretariat	Arrange seminar session about experiences with specific incident handling tools, adjacent to a future TF-CSIRT meeting	DONE - Andrew Cormack provided a session on Remedy at the previous days seminar session
0-10	TI	Give a presentation at a future RIPE meeting	Not yet done - To be undertaken at the RIPE 39 meeting, 30 April - 4 May 2001, Bologna
1-1	Gorazd Bozic	Submit a paper to present TF-CSIRT activities at the FIRST conference 2001	DONE - Result not yet known
1-2	TI	Submit a paper to present the TI pilot service at the FIRST conference 2001	DONE - Result not yet known
1-3	Speakers at Paris seminar sessions	Send their slides to Yuri Demchenko	DONE
1-4	Secretariat	Arrange seminar session about current practice of CSIRTs, adjacent to the next TF-CSIRT meeting	DONE
1-5	Don Stikvoort and Christoph Graf	Prepare a discussion at the next TF-CSIRT meeting about a certification authority for the European CSIRT community	DONE - Christoph Graf to speak about this at Agenda item 5
1-6	Gorazd Bozic	Ask Wilfried Wöber to explain to the TF-CSIRT mailing list the status of the discussion in RIPE on the security entry in the RIPE database	DONE
1-7	Andrew Cormack	Find out about (the availability of) the material from CERT/CC courses	DONE Not practical, courses given by CERT/CC possible, but expensive
1-8	Andrew Cormack, Claudia Natanson, Jacques	Send a draft programme outline of the training workshop to the TF-CSIRT mailing list for discussion. Then update the outline so that the programme can be completed in	ACTION in progress. Discussion of work completed so far at Agenda item 7

	Schuurman	the next TF-CSIRT meeting.	
1-9	Karel Vietsch	Arrange a meeting between a TF-CSIRT delegation and CEC representatives on the action in the *e*Europe 2002 Action Plan. Summarise the discussion in the Paris meeting in a briefing paper for that meeting with the CEC.	DONE - Report to be given at agenda item 8
1-10	all	Send pointers to legal information to Andrew Cormack	Nothing received by Andrew - REMINDER to all to send information
1-11	all	Send information about incident handling tools to Yuri Demchenko	DONE, but also ongoing. Questionnaire to be sent out by Yuri
1-12	Yuri Demchenko	Change the TF-CSIRT Web pages, to reflect the new procedure for subscribing to the mailing list.	DONE
1-13	Jaime Agudo and Secretariat	Organise next TF-CSIRT meeting in Barcelona on 18-19 January 2001	DONE

4. Trusted Introducer Pilot Service, Klaus-Peter Kossakowski, Stelvio

The Trusted Introducer Pilot Service has now been running for four months. At the time of the report there were 54 CSIRT teams known and listed by TI. An up-to-date list can be found on the TI web page at http://www.ti.terena.nl/teams/level0.html. The directory contains all known teams within Europe.

As of 1 January 2001 there are three Level 2 teams: CERT-NL, GARR-CERT and JANET-CERT. Klaus-Peter also reported that there were two Level 1 teams and a further 7 teams which were outstanding and might soon become Level 1 and possibly five more within a few months. Six of these organisations seeking accreditation are from the commercial sector.

TI has been working on a management overview document that will provide information on the benefits for organisations becoming TI accredited which might be especially useful in persuading commercial organisations to join up.

Members of the three teams that had achieved LEVEL 2 status reported their experiences in going through the accreditation process. The three teams were unanimous in their praise for Stelvio for the assistance they have given. They all thought that thinking about and formally documenting the CSIRT service that they provide to users was a helpful process for them internally.

Peter asked that all teams look at the information held on the directory page http://www.ti.terena.nl/teams/level0.html and check it for accuracy, reporting any changes by following the methods list on page http://www.ti.terena.nl/howto.html#S02. The TI would send the same request to all Level 0 teams, as a one-off action. Claudia Natanson of BTSS CSIRT said she was interested to see how the process of accreditation would translate from the academic community to the commercial sector.

Karel Vietsch reported on the closed meeting of the TI Review Board that had taken place on the evening of 18 January 2001. Stelvio had presented a written report covering the four months up until the end of December 2000. The Review Board are very happy with the format and the content of the report. The only addition to the report that had been requested was the inclusion of an analysis of the TI web page usage. Karel reported that in the interest of encouraging free exchange of information between TI and the Review Board, the full reports would be kept confidential to that group but an overview of the report would always be given to the TF-CSIRT meeting.

It was pointed out by Karel that the TI Pilot is for a period of one year which will end on 1 September 2001 and in advance of this there will be a formal review on which a decision about its future will be based. The options are:

- If it has not been successful, it will be stopped
- The pilot could be extended to prove its worth if there is some doubt
- If sufficient support is found, it could be turned into a full service

There was some discussion about what criteria might be used judge whether the pilot had indeed been successful or otherwise. These might include:

- How many teams had been accredited at LEVEL 2 ?
- Are a substantial number of the LEVEL 2 teams commercially based ?
- Usage of the TI Web pages.
- Experiences from the LEVEL 2 teams.

The composition of the TI review board was discussed. An interim review board had been made up of volunteers with the intention of putting in place a longer-term replacement populated with members elected from the LEVEL 2 teams. Since there are currently just three LEVEL 2 teams and the formal review of TI will take place soon, the interim review board was asked if it would be willing to serve until after the review had taken place, so as to take of their knowledge of the background. The TF-CISRT meeting agreed this as an acceptable arrangement.

5. CA for CSIRTs in Europe, Christoph Graf

Christoph started by explaining that the problem that needs to be solved is limiting access to TI restricted resources to groups within the accredited TI community (LEVEL 1 and LEVEL 2 teams). The responsibility for achieving this lay with Stelvio acting as the TI.

An obvious way of achieving this is with the use of certificates issued by a Certification Authority; however Christoph said he could see no other benefits arising from the use of formal certificates, other than as a "showcase" application of the technology. Since there is currently little in the way of an established CA infrastructure in our community, perhaps alternatives should be explored, at least for the interim. This might be through the exchange of messages using HHTPS, PGP and shared secrets.

There was support from the other members of the TF for the alternative approach. Wilfred said that CA's and certificates are more appropriate in hierarchical structures which we don't have in the CSIRT environment. Andrew Cormack's view was that the CSIRT requirement did not justify setting up CA's and if there was a demonstrable need for the certificates, we could turn to a commercial CA and purchase them. Christoph thought that the Swiss academics would probably outsource their requirements for supply of certificates. It was agreed by the TF that we should proceed with an interim solution based on the use of HHTPS, PGP and shared secrets, but be aware that new (as yet unseen) requirements could come up and we might need to reconsider the use of CA's and certificates.

6. Update on FIRST Activities, David Chrochemore

David Chrochemore of Le CERT RENATER said that the FIRST programme committee for the 13th Annual Computer Security Incident Handling Conference had selected the papers that will be presented and that in his view the programme looks interesting. (Details of the conference can be found at http://www.first.org/conference/2001/). This year's conference will focus on incident response and related issues, rather than being general in nature. Michel Miqueu added that they were still looking for additional sponsors. He also mentioned that the conference registration form will be available on the web page from the end of February and an announcement will be posted to the cert-coord email list.

7. Development of a Training Workshop for New (Staff of) CSIRTs, Andrew Cormack

Andrew explained that the target audience for the proposed training workshops would be members of new teams or new members of existing teams. The workshops will not be about the CSIRT set up process. It will be assumed that all attendees have a reasonable idea of how the Internet works as a prerequisite. The workshop will teach how security incidents can break Internet service, not how the Internet works. The current estimate of workshop duration is eight or nine hours of material which will mean that if sufficient time is included for questions and discussion, then the event will need two whole days. It was agreed that the course should be modular in structure, which would make it easier to compile in a distributed fashion, to deliver and to maintain. It is anticipated that each module will consist of a presentation followed by discussion. Some of the modules will also include an element of practical experience (indicated below by "workshop") such as

evaluating printed log-files. It is not intended to include hands-on hardware exercises as this will increase the logistic problems in delivering the course. The following modules areas were agreed, the framework structure of each being defined in the presentation slides on this website. The individuals also shown in the table below agreed to become editors for the module against their name.

MODULE NAME	Editor	Includes "Workshop"
Legal Issues	Jacques Schuurman, CERT-NL	No
Organisational Issues	Claudia Natanson, BTSS CSIRT	Yes
Technical Issues	Klaus Möller, DFN-CERT	Yes
Market Issues	Andrew Cormack, JANET- CERT	No
Operational Issues	Gareth Price, BTSS CSIRT	Yes

These editors took responsibility that well before the next TF-CSIRT meeting a fully detailed description of the contents of their module would be available. All present were invited to send their suggestions to the editors.

Claudia mentioned that in view of the potentially different needs of the commercial and academic communities, she will think about the appropriateness of each modules contents.

There was some discussion on protecting the course material from unscrupulous elements that might just copy it and use it for their own commercial gain. Karel explained that TERENA's general policy was to put its information in the public domain so as to achieve the most benefit for its membership. John Dyer mentioned the arrangements TERENA had made for the Guide to Network Resource Tools (GNRT). TERENA has contracted with Addison Wesley publishers who sell a paperback version of the material in the English language (ISBN 0-201-61905-9) whilst TERENA retains the rights for an online version (http://www.terena.nl/libr/gnrt/). The non-English language national networks can exercise their rights to publish a printed version in their own language (ARNES for example has produced a printed version in Slovenian). TERENA could copyright the workshop as a whole and discuss the details of the arrangement with the section authors before publication of the documentation.

Some of the commercially based organisations were concerned that the liability issues of putting on a workshop had not been investigated (for instance if a workshop is promised and then cannot be delivered). Karel said that for many years TERENA had been organising workshops and conferences and had not yet encountered a problem in this respect.

The intention is to try and undertake the first delivery of the workshop late during 2001.

8. Relations with the CEC

Karel reported that he and a deputation from TF-CSIRT had met with Thierry Vanderpyl, Andrea Servida and Roman Tirler (all three from the Commission) on 16th November 2000. It was clear that the Commission have no fixed idea of what they would like to see in the sense of security elements in the *e*Europe Programme and were grateful for the information and ideas from TF-CSIRT. Karel subsequently sent a letter to Thierry Vanderpyl setting out the activities of TF-CSIRT, suggesting nine actions which the Commission might like to consider for inclusion. Members of TF-CSIRT that have an interest in applying for funds through the Fifth Framework Programme should look at the research topics in work-programme which can be found at http://www.cordis.lu/ist/. Sections II.4 and V.1.4 are particularly relevant to the security area.

On 19 December 2000 Mr. Vanderpyl had sent a reply letter, in which TF-CSIRT was invited to articulate a proposal for an action plan (with roadmap and milestones) to achieve the eEurope objectives, and to visit Brussels again for a meeting with the CEC officials in the week of 12-16 February 2001. TF-CSIRT members were very hesitant to take undertake to write an action plan with roadmap and milestones, thereby taking on the tasks of the Commission. It was pointed out however that an alternative would be to re-write the earlier letter in action plan format, and then have the proposed meeting with the Commission. That meeting would have to be in the week of 19-23 February, because the week suggested by the CEC coincides with a major FIRST event. Andrew Cormack, David Parker, Gilles André, Don Stikvoort and Pascal Delmoitié volunteered for the TF-CSIRT deputation for this next meeting with the CEC, which would be organised by Karel Vietsch.

Michel Miqueu reported that in January he had had another meeting with the same CEC officials, to discuss actions regarding commercial CSIRTs. Andrew Powell reported that in February the CEC would also have meetings with representatives of various national infrastructures.

9. Report on the Seminars (18 January 2001)

It was agreed by those that had attended the seminar sessions that it had been a successful day, but the duration had been too long and future events should be shortened by perhaps half-an-hour. Karel requested all seminar contributors to make their presentation material available to Yuri to enable it to be put on the TERENA web server.

With regards to the presentation on the inclusion of a security contact entry in the RIPE database, Gorazd encouraged TF-CSIRT members to write a letter of support and mail it to the RIPE database working group (Email address: db-wg@ripe.net).

It was agreed that a further seminar session should be arranged to take place the day before the next TF-CSIRT meeting. There was support for presentations on present practice from CSIRT teams. Andrew Cormack agreed to demonstrate the use of the

Remedy package if he can sort out the licensing issues involved. Jan Meijer agreed to present CERT-NL's ideas on CSIRT workflow but stressed this would involve a description of the flows rather than the use of an automated tool.

Claudia offered to talk about the BTSS CSIRT experiences of using the Magic package at the September 2001 TF-CSIRT meeting.

Yuri Demchenko will be coordinating a questionnaire to be sent to CSIRTs on the use of tools in their work. Jan Meijer, Andrew Cormack and Andrew Powell will provide advice to Yuri on the text of that questionnaire.

10. Other Work Items

This session was used to allow teams to share information regarding their CSIRT activities and information they had recently discovered. It was agreed that on the agendas of future TF-CSIRT meetings this agenda item should be called "Other Report Items" rather than "Other Work Items".

JANET CERT stated that they are currently in the process of sponsoring a new FIRST member, namely the team led by Ian Bryant.

Gorazd Bozic said that the ARNES experience with Eastern European countries is that they are having problems forming IRTs, the reason being that generally the networks have limited financial resources and the first priority is building the underlying network infrastructure. Gorazd is disseminating information about TF-CSIRT to those groups so that they will have some understanding of the need and importance of setting up a CSIRT team.

Gorazd Bozic also mentioned that TF-CSIRT members had been asked to forward information about the legal framework relating to computer security incidents to Andrew Cormack of JANET CERT. Andrew is trying to track down a EU database of information on IT legislation, which he believe may already exist. There was some discussion on whether Interpol or Europolmight have this information or be interested in collaboration with TF-CSIRT on this issue, but little was known about either of their activities. John Dyer agreed to see if he could obtain any relevant information from a friend he has working in the organized crime unit of the Dutch Police.

There was some discussion on the emerging requirements of European governments on ISP's to hold log files for extended periods of time. In Belgium, the government is attempting to make the period 12 months, whilst in the UK a period of seven years has been mentioned.

Ian Bryant explained the purpose and background of the new National High-Tech Crime Unit in the UK that becomes operational in April 2001 as a multi-agency partnership hosted by the National Crime Squad. The Unit will have primary responsibility for

investigating the most serious and organized hi-tech offences, ranging from attacks on national infrastructure and networks to more traditional crimes that have moved to the e-world. The Hi-Tech Crime Unit represents a major component of a national strategy that calls for integrated partnerships between Government, Industry, Police Forces and other Law Enforcement agencies. The role of the unit will be to:

- investigate serious and organized hi-tech crime;
- provide strategic intelligence and assessments;
- provide tactical intelligence, both for the Unit and for police forces;
- provide technical support for investigations;
- take a major role in the development of national standards and expertise for the investigatio n of hi-tech crime
- David Parker would check if someone from the National High-Tech Crime Unit could give a presentation in the September 2001 meeting of TF-CSIRT.

11. Dates and Locations of the next meeting of TF-CSIRT

3rd Meeting 31 May & 1 June 2001, hosted by ARNES in Ljubljana, Slovenia

4th Meeting 27 & 28 Sept. 2001, hosted by JANET-CERT in Manchester, UK

12. New and Open Actions

ACTION			STATUS
0-2	TI	Produce document(s) to explain benefits of TI to managers	Still open
0-10	TI	Give a presentation at a future RIPE meeting	To be undertaken at the 39th RIPE meeting, 30 April - 4May 2001, Bologna
1-10	all	Send pointers to legal information to Andrew Cormack	Nothing received by Andrew - REMINDER to all to send information
2 -1	all	Check the accuracy of the information on their own team at the TI web pages	
2-2	Jacques Schuurman	Produce a fully detailed programme of the Legal Issues Training Module before 1 May 2001	
2-3	Claudia	Produce a fully detailed programme of the	

	Natanson	Organizational Issues Training Module before 1 may 2001	
2-4	Klaus Möller	Produce a fully detailed programme of the Technical Issues Training Module before 1 May 2001	
2-5	Andrew Cormack	Produce a fully detailed programme of the Market Issues Training Module before 1 May 2001	
2-6	Gareth Price	Produce a fully detailed programme of the Operational Issues Training Module before 1 May 2001	
2-7	Andrew Cormack	Prepare demonstration of Remedy System for May seminar	
2-8	Jan Meijer	Prepare presentation on CSIRT workflows for May seminar	
2-9	Claudia Natanson	Prepare presentation on Magic System for September seminar	
2-10	Yuri Demchenko	Coordinate questionnaire on CSIRT tool usage	
2-11	John Dyer	Investigate information on Interpol and Europol activities	
2-12	Karel Vietsch	Re-write earlier letter to the CEC in action plan format and organise new meeting of TF-CSIRT deputation with CEC officials in week of 19-23 February 2001	
2-13	Secretariat	Arrange seminar session about current practice of CSIRTs in May seminar	
2-14	David Parker	Invite representative of the UK National High-Tech Crime Unit to give a presentation in the September seminar	
2-15	Gorazd Bozic and Secretariat	Organise next TF-CSIRT meeting in Ljubljana on 31 May and 1 June 2001	

Appendix 1.
List of Attendees of the 2nd TF-CSIRT Meeting

19 January 2001
Universitat Politècnica de Catalunya, Barcelona, Spain

Name	Affiliation
Tom Mullen	BTCERTCC
Claudia Natanson	BTSS CSIRT
David Parker	UNIRAS
Andrew Powell	UNIRAS
Christian Blanc	Concert NL
Pascal Delmoitié	BELNET
Michel Miqueu	CERT-IST
Robert Morgan	JANET-CERT
Andrew Cormack	JANET-CERT
Michel Dupuy	CERTA
Gilles André	CERTA
Jimmy Arvidsson	TeliaCERT
Pege Gustafsson	TeliaCERT
Matthias Etrich	Deutsche Telekom AG
Klaus Möller	DFN-CERT
Chelo Malagón	IRIS-CERT
Jordi Linares	EsCERT
Francisco Monserrat	IRIS-CERT
Ian Bryant	JSYCC
Karel Vietsch	TERENA
Gerard Bozic	ARNES
Preben Andersen	DK-CERT
Torbjorn Wictorin	SUNET-CERT
Gareth Price	BTSS CSIRT
Pekka Kytölaakso	FUNET-CERT
Christoph Graf	SWITCH-CERT
Jan Meijer	CERT-NL SURFnet
Wilfried Wöber	ACOnet
Roberto Cecchini	GARR-CERT
Michael Behringer	CISCO
Vlado Pribolsan	CARNET CERT

Per Arne Enstad	UNINETT CERT
Klaus-Peter Kossakowski	
Svein Johan Knapskog	UNINETT CERT
David Chrochemore	CERT-RENATER
Jacques Schuurman	CERT-NL SURFnet
Yuri Demchenko	TERENA
John Dyer	TERENA