TSec(02)059rev2

Minutes of the 7th TF-CSIRT meeting
Syros, 27 September 2002

1. Welcome and Apologies

Apologies had been received from Jimmy Arvidsson (TeliaCERT), Yuri Demchenko (TERENA), Mark Koek (Stelvio, Trusted Introducer service), Chelo Malagón (IRIS-CERT), Claudia Natanson (BT Ignite SBS) and Gareth Price (BT Ignite SBS).

2. Round of Introductions

The list of those present is below at the end of these minutes.

Karel Vietsch announced that Yuri Demchenko would be leaving TERENA's employment from 1 November 2002. Yuri's tasks in the support of TF-CSIRT would be taken over by Kevin Meynell (kevin@terena.nl). The arrangement might change again once the vacancy left by Yuri at TERENA would be filled. Yuri had prepared this meeting and Karel would take the minutes. After that, Kevin would be responsible for TERENA's support to TF-CSIRT.

3. Minutes of Last Meeting (Copenhagen, 24 May 2002)

The minutes were approved without changes. Action items:

03-05 Gilles André to make an outline for a project proposal to the EC concerning secure emergency backup infrastructure for CSIRTs and software patents, and circulate it on the TF-CSIRT list.

Gilles reported that he had written a short document but had not circulated it yet. He had investigated the use of radio networks and would now study if encryption can be used. After that he would like to conduct a small pilot project with two or three sites. Gilles would send his short document to the TF-CSIRT list immediately after this meeting. At the next TF-CSIRT meeting he would give a presentation.

04-05 Wilfried Wöber to prepare a proposal about marketing/promoting the use of the IRT contact information in the RIPE database.

Ulrich Kiermayr reported that a new RIPE document was available on how to place an IRT object in the RIPE database. Publicity was given to the matter in the last RIPE meeting. Gorazd Bozic remarked that a tool to use the IRT object should be part of the promotion. Wilfried Wöber and Ulrich Kiermayr would write a document on how to promote the IRT object and how to use it.

05-02 Yuri Demchenko to create password-protected part of the TF-CSIRT webpages initially with one password.

Karel Vietsch promised that this would be done before the end of the year. Before that it would be necessary to have a discussion on the mailing list on what to store in that password-protected part; Gorazd Bozic would initiate that discussion.

Karel Vietsch announced that he would like to replace cert-coord@terena.nl by a new mailing list called tf-csirt@terena.nl , and take that opportunity to update the subscriptions to the list. There followed a discussion on who would be allowed to subscribe to the new mailing list. Currently this is left to the discretion of the TF-CSIRT chairman. A straw poll revealed that 4 of those present were in favour of establishing a committee that would draft rules as to who could subscribe, whilst 17 were in favour of maintaining the status quo. It was concluded that the chairman will remain in charge of deciding who can subscribe to tf-csirt@terena.nl , but it was recognised that this new list should be restricted in principle to staff of (TI listed) CSIRTs.

05-07 Ian Bryant to check NATO's interest in conducting special training and assisting establishing new CSIRTs in EU and countries of the Former Soviet Union.

Open.

05-09 All to submit 1-2 statements related to security issues t o Karel Vietsch; these could then be taken up in an Open Letter to the EC to be edited by Karel.

Karel Vietsch reported that some statements had been received, but certainly not enough to result in an Open Letter. He and Michel Miqueu thought that it would only be useful to send an Open Letter to the EC if that would be in reaction to an EC document/proposal or at some specific occasion. It was agreed to drop the action and to revisit the statements when an opportunity or necessity would arise to formally approach the EC.

05-11 Jan Meijer to organise reporting on the last IODEF working group deliverables and on the INCH working group to the next TF-CSIRT meetings.

Done; see agenda item 8.

05-12 Andrew Cormack to set up before end May 2002 the Clearinghouse trial, and all TF-CSIRT members to make contributions in the trial period until the end of September.

Done; see agenda item 6.

06-01 Gorazd Bozic and Yuri Demchenko to finish forming teams for each deliverable in the new TF-CSIRT Terms of Reference.

Open. Gorazd Bozic will report in the next TF-CSIRT meeting.

06-02 Jan Meijer to initiate discussion on deliverable H (Common Incident Handling Procedures and requirements for Incident Handling Systems).

Open.

06-03 David Parker to draft document with ideas on which information can be shared between CSIRTs in the context of deliverable I.

David Parker had discussed his document with the TI accredited teams; he will now send it to the TF-CSIRT mailing list.

06-04 David Parker to organise BoF on Regional Initiatives at FIRST conference.

Done. It became a 3-hours meeting instead of a 20-minutes event as planned. FIRST has subsequently established a working group on the matter (see agenda item 7). The elections for the FIRST Steering Committee resulted in a broader geographical spread.

06-05 Gorazd Bozic to send out information about TF-CSIRT activities to the FIRST mailing list.

This action was taken over by Andrew Cormack and Jacques Schuurman and then developed into the BoF at the FIRST Conference (see above).

06-06 TERENA Secretariat to investigate possible resources for travel support for some TF-CSIRT members to attend TF-CSIRT meetings.

Done, but with negative result. No possible funding sources were found.

4. Trusted Introducer pilot service

Don Stikvoort gave a short status message (his slides are on the TF-CSIRT website). The recommendations of the TI Review Board, which were endorsed by TF-CSIRT in its last meeting, were accepted by the TERENA Executive Committee. Subsequently S-CURE and TERENA signed at the end of August 2002 the contract for the first year of the permanent TI service, starting 1 September 2002.

Instead of “level-0, level-1 and level-2 teams” the terminology is now “listed, accreditation candidate and accredited CSIRTs”. The accredited CSIRTs will meet at least once a year, in the autumn. Such a meeting took place on Syros on 26 September 2002. The TI Review Board will conduct annual reviews in the spring. S-CURE will make the TI website simpler and more accessible.

There will be a number of services for accredited CSIRTs only: a restricted website with detailed team information, a 4-monthly active maintenance cycle on team data, the availability of an up-to-date PGP key ring, CSV files with contact date for PDAs and laptops, a trusted mailing list for information exchange, formal signing of PGP keys by the TI CA (will start at the next meeting of TF-CSIRT), automatic registration and maintenance of IRT objects in the RIPE database (will start in October 2002).

There were currently 79 listed CSIRTs and 30 accredited CSIRTs. Teams that were accredited since the last TF-CSIRT meeting were CERT-RO, CERT-RUG, PRE-CERT, SUNET-CERT and CARNET-CERT.

From the meeting of accredited teams on 26 September 2002 it was reported that (subject to a verification with accredited teams to be conducted by meeting secretary Don Stikvoort) the following people were re-elected as members of the TI Review Board: Andrew Cormack for a one-year term of office, Jimmy Arvidsson for a two-year term of office and Jacques Schuurman for a three-year term of office.

5. Update on EC funded projects

Gorazd Bozic remarked that it would be useful to collect pointers to relevant projects (and not only EU-funded projects). Everyone was asked to send relevant URLs to the TERENA staff, who will then put them up on the TF-CSIRT webpages.

TRANSITS

Karel Vietsch presented the progress in the TRANSITS project (his slides are on the TF-CSIRT website). The TRANSITS project had started on 1 July 2002 and will run until 30 June 2005. It is 100% funded by the EU as an Accompanying Measure in the 5th Framework Programme. Project partners are TERENA and UKERNA. TRANSITS will produce training course materials based on the materials produced earlier by volunteers from TF-CSIRT. The first edition of the course material had just been completed. A completely revised version will be produced early in 2004. TRANSITS will organise 2 training courses per year. The TRANSITS budget pays part of the costs of course materials update, workshop logistics and lecturers' expenses. There is also a budget to cover part of the expenses of workshop participants from "poorer" European countries. Key persons involved are Andrew Cormack (UKERNA) and Karel Vietsch and Raquel Corredoira (TERENA).

The first training workshop will take place in Oegstgeest, the Netherlands from 31 October – 1 November 2002. It will have 20 participants in two parallel groups. Lecturers will be Andrew Cormack, Klaus Möller, Gareth Price, Jacques Schuurman and Don Stikvoort. The second training workshop will be hosted by CERT Polska in Warsaw from 27-28 May 2003, the days before a TF-CSIRT meeting there.

The training materials are copyright TERENA. Use (e.g. for workshops at national level) is permitted provided that one asks TERENA for permission (info@ist-transits.org) and reports on the use. All information on the project is at www.ist-transits.org .

*e*CSIRT.net

Don Stikvoort gave a short update on the project, which had been presented in more detail in the previous TF-CSIRT meeting. The project is about the application of IODEF in real life. Objectives are to multiply IODEF use, and analysis and dissemination. The consortium consists of DK-CERT, CERT Polska, GARR-CERT, IRIS-CERT, CERT Renater, JANET CERT, DFN-CERT, PreSecure and Stelvio. The project will run until the end of 2003. It had its first project meeting on Syros from 24-25 September 2002.

EISPP

Michel Miqueu gave a brief update on the EISPP project, which he had presented in more detail in the previous TF-CSIRT meeting. The project website, describing the objectives of EISPP and the project partners, will be available from mid October 2002 at www.eispp.org . The project started in June 2002 and will end in November 2003. Michel explained that EISPP will develop a charging model to be used for the services after the end of the project.

EISPP would be interested to organise a half-day workshop adjacent to the TF-CSIRT meeting in May 2003 in Warsaw. Michel Miqueu and the chairman and secretary of TF-CSIRT will discuss the arrangements for this workshop.

6. Clearinghouse for Incident Handling Tools (CHIHT)

Marco Thorbrügge and Andrew Cormack introduced the agenda item. A pilot version of CHIHT had been set up at http://chiht.dfn-cert.de/ . Earlier it had been envisaged that this meeting would evaluate the pilot phase and decide whether or not to continue CHIHT, but Andrew and Marco felt it was a success and Marco was happy to continue the work.

The links from the CHIHT webpages are checked on a daily basis. During September there have been about 10 visitors per day, and people seem to find it a useful service. Additional information on tools can be sent to chiht-submit@terena.nl .

In the discussion there were some additional suggestions: set up a facility so that people can send comments; organise in some way the feedback from CHIHT users; put links to the CHIHT site on the webpages of CSIRTs.

7. Update on FIRST and regionalisation issues

Jacques Schuurman gave a presentation on the FIRST Task Force on Regional Initiatives (his slides are on the TF-CSIRT website). Various initiatives are going on in different continents: TF-CSIRT, AP CERTF, plans in Latin America. A motion was carried at the FIRST AGM 2002 to establish a Task Force. The aim is to find out what is going on and in which way FIRST can be of help. The Task Force is an open group; any interested person can join. Its discussions are based on a kick-off paper that poses a number of questions. The main strands in the kick-off paper are: real-time operational issues, sharing information, critical infrastructure and cyberdefense, policy-making and strategic planning, facilitating bilateral contacts, trust management.

The Task Force has a mailing list first-regions@first.org . It will meet adjacent to the FIRST technical colloquia in October 2002 and February 2003, and there will be teleconferences and additional meetings as required. The recommendations from the Task Force will be drafted in the first quarter of 2003.

Jacques would find out how the kick-off document can be made available to TF-CSIRT members. David Crochemore would ask the FIRST Steering Committee if it is allowed to distribute the kick-off document widely.

Andrew Cormack reported that after contacts made by him and Jan Meijer at the FIRST Conference in Hawaii, there had been on 30 August 2002 a meeting in Amsterdam between TI accredited teams and representatives of the CSIRTs community in the Asia-Pacific region. Governments in the Asia-Pacific region are keen to improve their image in the Internet world and therefore want to do something visible about security issues. The idea is to organise the collaboration between CSIRTs in Asia-Pacific on a more formal basis than TF-CSIRT in Europe. The natural counterparts in Europe are therefore the TI accredited teams. The meeting in Amsterdam explained about the TI scheme and the object in the RIPE database. The Asia-Pacific delegation found this very interesting and they may incorporate something similar in their own plans that they are currently developing.

8. IODEF development

Jan Meijer presented the progress in the IODEF development (his slides are on the TF-CSIRT website). He explained about IODEF and its history. INCH is now finally officially established as an IETF Working Group. The requirements document is being revisited by Glenn Keeni of JPCERT/CC. The data model document is stabilising. The user guide has not been written yet; PreSecure may be interested in doing this as part of the *e*CSIRT.net project. There is much interest in the IODEF work, in particular from Japan.

The *e*CSIRT.net project is going to use IODEF for exchanging incident information, and therefore they will be providing lots of input to the IODEF development. One of the problems (to be solved by *e*CSIRT.net) is how to exchange messages using the IODEF format.

Jan then presented the IODEF Pilot Implementation project, which is carried out by TERENA and UKERNA with a little bit of co-funding from TERENA. The work has turned out to be more difficult than expected, but is expected to be completed in January 2003. It is hoped that CERT-NL and JANET CERT will be able to demonstrate the results of the project at the next TF-CSIRT meeting.

9. Results of yesterday's Seminar Sessions

On the day before this TF-CSIRT meeting there had been a full-day seminar with the following presentations:

- Securing Networks with Juniper Networks (Jean-Marc Uzé, Juniper)
- Black Hole Routers (Damir Rajnovic, Cisco)
- National Infrastructure Security Co-ordination Centre (Peter Burnett, NISCC)
- Secure Electronic Voting (Dimitris Gritzalis, Athens University of Economics and Business)
- GRNET, Greek Research & Technology Network (Athanassios Liakopoulos, GRNET)
- Best Current Practice in Handling Spam (Maria Rådström, Skanova and Pege Gustafsson, TeliaCERT).

All their slides are on the TF-CSIRT website.

Everyone was invited to send suggestions for future seminar sessions to the TF-CSIRT chairman or secretary. One suggestion made was to invite firewall and/or IDS manufacturers to a future seminar.

10. Other Work Items

Assistance to the Establishment of New CSIRTs

Przemek Jaroszewski introduced the agenda item. Work item G in the new TF-CSIRT Terms of Reference states that TF-CSIRT will prepare and publish documents on Current Practice in CSIRT organisations and will develop recommendations/measures to assist the establishment of new teams via tutorship/mentorship from experienced teams. This led to a working group of TF-CSIRT, which has the mailing list csirt-bcp@terena.nl . The working group had its kick-off meeting on Syros on 26 September 2002. There exist some documents on CSIRT Best Current Practice, but these are not always good to show to new CSIRTs (because they go too deep for example). Don Stikvoort has written a 10-page document on the CSIRT handbook, but he still has to sort out the legal aspects. The working group will look at Don's document and prepare a final version. Another deliverable from the working group will be a presentation aimed at managers. The time schedule is that Don's document will be finalised within a few days, and that the presentation will be ready before the end of 2002 and certainly before the next TF-CSIRT meeting.

A question under discussion was how to advise new teams. Advise them to become a FIRST member or join TF-CSIRT? For some beginners that may be a step too far. Attending a TRANSITS workshop could help starters. Another suggestion was to establish a point of contact (e-mail or phone) for new teams. The invitation to the first TRANSITS workshop may not have reached all teams, because it was only sent to the TF-CSIRT, FIRST and TERENA mailing lists. It might be good to send the invitation to all TI listed teams next time.

11. Presentation by Tomasz Nowocien (POL-34 CERT)

Tomasz' slides are on the TF-CSIRT website. He described the creation of a Distributed Incident Handling System (DIHS). The objectives are to simplify the collection of incident reports, to formalise the collection of incident handling, to simplify the incident handling process and to give additional features to network administrations. Incident reports are collected by a "report collector" and go from there to a "report qualifier" (one person). The data are stored in a database. From there they are distributed to various "incident handlers". A "functional analyser" analyses the database and finds correlations between incidents. The system is now being implemented. The implementation will be completed before the end of 2002. In the spring of 2003 POL-34 CERT would like to share their experiences wit h TF-CSIRT.

12. Dates and Venues of Next Meetings

The next meeting will be from 23-24 January 2003 in Zagreb. Natasa Glavor said that logistic information will be put on the CARNet website and be linked from the TF-CSIRT webpages.

Subsequent meetings will be in Warsaw from 29-30 May 2003 hosted by CERT Polska, and in Amsterdam from 25-26 September 2003 hosted by CERT-NL.

13. Any Other Business

Damir Rajnovic asked three questions:

- Do CSIRTs consider themselves "critical infrastructure"? Do they have government permission to enter their own premises in case of emergencies (cf. Manhattan on 11 September 2001)?
- Is it a good idea to have an official press relations person for TF-CSIRT?
- Can the chairman report on rejected requests to subscribe to the TF-CSIRT mailing list (only numbers, no names)?

As to the last question, Gorazd Bozic promised to make such reports in future meetings.

The meeting expressed its thanks to GRNET-CERT for organising a perfect meeting.

List of meeting participants

1.	Gilles André	CERTA	FR
2.	Jani Arnell	FICORA / CERT-FI	FI
3.	Simon Baker	JANET-CERT	UK
4.	Matias Bevilacqua	esCERT	ES
5.	Andy Bone	JANET-CERT	UK
6.	Cathy Booth	UNIRAS / NISCC	UK
7.	Gorazd Bozic	SI-CERT, meeting chairman	SI
8.	Andrew Cormack	UKERNA	UK
9.	David Crochemore	CERTA	FR
10.	Mikhail Ganev	RU-CERT	RU
11.	Natasa Glavor	CARNet CERT	HR

12. John Green	JANET-CERT	UK
13. Pege Gustafsson	TeliaCERT	SE
14. Cliff Harding	BT CERT	UK
15. Kauto Huopio	FICORA / CERT-FI	FI
16. Przemek Jaroszewski	CERT Polska / NASK	PL
17. Ulrich Kiermayr	UniVie – ACOnet	AT
18. Kostya Kortchinsky	CERT Renater	FR
19. Dimitris Lekkas	GRNET-CERT	GR
20. Sergey Linde	RU-CERT	RU
21. Stelios Maistros	GRNET-CERT	GR
22. Mirek Maj	CERT Polska / NASK	PL
23. Jan Meijer	SURFnet / CERT-NL	NL
24. Michel Miqueu	Cert-IST	FR
25. Tomasz Nowocien	POL34-CERT	PL
26. João Pagaime	FCCN	PT
27. David Parker	UNIRAS / NISCC	UK
28. Andrea Pinzani	GARR-CERT	IT
29. Leila Pohjolainen	FUNET CERT	FI
30. Alex Quintieri	esCERT	ES
31. Damir Rajnovic	Cisco Systems	
32. Maria Rådström	Skanova / Telia	SE
33. Jürgen Sander	PRESECURE	DE
34. Jacques Schuurman	SURFnet / CERT-NL	NL
35. Mikael Stamm	DK-CERT	DK
36. Don Stikvoort	Stelvio / Trusted Introducer	NL
37. Alexander Talos	UniVie – ACOnet	AT
38. Vincent Thiele	CERT-RO	NL
39. Marco Thorbrügge	DFN-CERT	DE
40. Marius Urkis	LITNET CERT	LT
41. Karel Vietsch	TERENA, meeting secretary	
42. Peter Wallström	Swedish Post and Telecom Authority	SE
43. Steven Xarhoulacos	GRNET-CERT	GR

RESULTING ACTION ITEMS

05-07	Bryant	Check NATO's interest in conducting special training and assisting the establishments of new CSIRTs in the EU and countries of the Former Soviet Union	Before 1 Jan 2003
06-01	Bozic	Finish forming teams for each deliverable in the TF-CSIRT Terms of Reference	Before 23-24 Jan 2003
06-02	Meijer	Initiate discussion on deliverable H (Common Incident Handling Procedures and requirements for Incident Handling Systems).	Before 1 Jan 2003
07-01	André	Send his short document on infrastructure backup to TF-CSIRT list	Before 2 Oct 2002
07-02	André	Give presentation on infrastructure backup in next TF-CSIRT meeting	On 23-24 Jan 2003

07/03	Wöber / Kiermayr	Write document on how to use the IRT object in the RIPE database and how to use it	Before 1 Jan 2003
07/04	Bozic	Initiate discussion on the TF-CSIRT mailing list on what to store on the password-protected part of the TF-CSIRT website	Before 1 Nov 2002
07/05	Meynell	Create password-protected part of the TF-CSIRT website with initially one password for all	In Dec 2002
07/06	Parker	Send to TF-CSIRT mailing list the document (discussed between accredited teams) on which information can be shared between CSIRTs (in the context of deliverable I).	Before 1 Nov 2002
07/07	all, Meynell	Send to Kevin Meynell URLs of projects that are relevant to CSIRTs, to be listed on the TF-CSIRT webpages	Before 1 Jan 2003
07/08	Miqueu, Bozic, Meynell	Discuss arrangements for EISPP workshop adjacent to TF-CSIRT meeting in Warsaw in May 2003.	Before 23-24 January 2003
07/09	Schuurman	Find out how Regionalisation TF kick-off document can be made available to TF-CSIRT members	Before 1 Nov 2002
07/10	Crochemore	Ask FIRST Steering Committee if Regionalisation TF kick-off document may be distributed widely	Before 1 Nov 2002
07/11	Stikvoort, BCP WG	Finalise Don Stikvoort's document on BCP in CSIRTs	Before 15 Oct 2002
07/12	BCP WG	Prepare presentation for managers	Before 1 Jan 2003