Minutes of the 3rd TF-CSIRT Meeting

Friday 1 June 2001
Ljubljana, Slovenia

John Dyer, TERENA
10 July 2001

1. Round of Introductions
2. Apologies
3. Minutes of the 2nd TF-CSIRT Meeting (Barcelona 19 January 2001)
4. Trusted Introducer Service for CSIRTs
4.1. Presentation on the Trusted Introducer, Mark Koek, M&I/Stelvio
4.2. Review on the Trusted Introducer Pilot Service, Brian Gilmore, TERENA
5. The 13th FIRST conference, FRANCE, David Crochemore, RENATER
6. Contacts with CEC, Karel Vietsch, TERENA
7. Development of Training Workshop Material
7.1. Legal Issues - Jacques Schuurman CERT-NL
7.2. Technical Issues - Klaus Möller, DFN-CERT
7.3. Organisational Issues, Gareth Price, BTSS CSIRT
7.4. Summary of Training Workshop Status
8. Clearinghouse for Incident Handling Tools, Yuri Demchenko, TERENA
9. Next Meetings
10. Any Other Business
11. Summary of New and Open Actions
Appendix 1. List of Attendees 3rd TF-CSIRT Meeting

1. Round of Introductions

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

2. Apologies

Claudia Natanson BTSS CSIRT
Klaus-Peter Kossakowski M&I/Stelvio
Don Stikvoort M&I/Stelvio

3. Minutes of the 2nd TF-CSIRT Meeting (Barcelona 19 January 2001)

The minutes of the 2nd TF-CSIRT meeting were accepted without change.

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	DONE
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	DONE
2-2	Jacques Schuurman	Produce a fully detailed programme of the Legal Issues Training Module before 1 May 2001	DONE
2-3	Claudia Natanson	Produce a fully detailed programme of the Organizational Issues Training Module before 1 May 2001	DONE
2-4	Klaus Möller	Produce a fully detailed programme of the Technical Issues Training Module before 1 May 2001	DONE
2-5	Andrew Cormack	Produce a fully detailed programme of the Market Issues Training Module before 1 May 2001	DONE
2-6	Gareth Price	Produce a fully detailed programme of the Operational Issues Training Module before 1 May 2001	DONE
2-7	Andrew Cormack	Prepare demonstration of Remedy System for September Seminar	
2-8	Jan Meijer	Prepare presentation on CSIRT workflows for May seminar	DONE
2-9	Claudia Natanson	Prepare presentation on Magic System for September seminar	DONE
2-10	Yuri Demchenko	Coordinate questionnaire on CSIRT tool usage	ongoing
2-11	John Dyer	Investigate information on Interpol and Europol activities	DONE

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	DONE - report during this meeting
2-13	Secretariat	Arrange seminar session about current practice of CSIRTs in May seminar	DONE
2-14	David Parker	Invite representative of the UK National High-Tech Crime Unit to give a presentation in the September seminar	DONE
2-15	Gorazd Bozic and Secretariat	Organise next TF-CSIRT meeting in Ljubljana on 31 May and 1 June 2001	DONE

4. Trusted Introducer Service for CSIRTs

4.1. Presentation on the Trusted Introducer, Mark Koek, M&I/Stelvio

Mark Koek gave a report of the status of the Trusted Introducer after the first nine months of operation. He said that many operators regard security as a serious problem and are aware of the existence of IRTs, but in the case of an incident find it hard to identify which one they need to approach. Even if an operator manages to identify a geographically appropriate IRT, how can they be sure that they can trust them? If the IRT is a member of FIRST this may be taken as some indication of authority, but in reality it conveys no information about operational competence or even the existence of an IRT.

As a result, TERENA with the help of interested IRTs set about establishing a mechanism that would provide a directory of all known European IRTs, and give them the opportunity of becoming accredited by an independent authority to be known as the Trusted Introducer (TI). The TI process defines three levels of status. All known European IRTs are entered into the TI register as a matter of course as soon as they become known. The listed IRTs are invited to check the information held about them and send in updates. All teams listed in this manner are known as having Level-0 status. Teams are also invited to consider becoming accredited to the highest level of status known as Level-2. Teams applying to be accredited to Level-2 are raised to Level-1 status whilst the independent TI undertakes the evaluation. Evaluation results in either accreditation to Level-2 status at which time the IRT is fully integrated into the trusted circle of TI members or reversion back to Level-0. To remain at Level-2 teams have to submit to a periodic re-appraisal by the TI. The accredited IRTs participate in

maintaining their own more detailed TI web pages, accessible only by TI Level-2 teams and the exchange of TI-restricted information, only available to Level-2 IRTs.

On 1 June 2001 there were 55 IRTs registered in the TI directory of known IRTs, with ten already fully accredited to Level-2. There were a further three in the process of been assessed. The directory and other public information regarding the TI can be found at URL: http://www.ti.terena.nl/

In discussions, some Level-0 teams said they would be willing to consider going to Level-2 if they could be surer of the benefits. The major benefits are being part of an accredited and trusted community in which one can be confident of the validity and authenticity of information, the advantage being that this provides secure channels for rapid communications for sensitive information that should be kept away from the public gaze. In addition TF-CSIRT is planning to experiment with automated incident information exchange based on the system independent IODEF standard between Level-2 IRTs to speed the exchange of information and avoid the need for re-keying of data, thus raising responsiveness and efficiency. It was also noted that now the number of Level-2 teams is into double figures, it had probably reached the minimum critical mass and the advantages in communicating with the larger community will accelerate as more teams become accredited. Some of the teams that already had been accredited, thought that the expert consultancy they had received during the assessment process had been worth the small fee alone, as it had provided them with expert help thinking through formal issues.

4.2. Review on the Trusted Introducer Pilot Service, Brian Gilmore, TERENA

Brian Gilmore started his presentation by saying he was going to report on the operation of the TI from the perspective of the TI-Review Board, a body set up to review the performance of the TI process and the contractor, M&I/Stelvio. The Review Board received reports from M&I/Stelvio every four months containing data on various parameters describing the operation of the IT process. These reports have to-date been made privately to the Review Board on the basis that this would encourage more open and forthright comments from the contractor. After nine months of operating in this fashion there has been no instance in which privacy has been an issue. Brian therefore proposed that in future the Review Board consider making the reports public.

After nine months of operation of TI, the Review Board's assessment is that the TI process has been operating satisfactorily. It has not met the target of 15 Level-2 teams with half of these from the commercial sector. It is therefore seen as too early to make a judgment on the overall success and as a result, it has been agreed that it would be useful to extend the pilot for another year.

TERENA had approached M&I/Stelvio about what it would charge to operate the pilot for a further year and the organisation had made a proposal. They have proposed that all Level-0 activities will be undertaken free-of-charge and fixed charges for each Level-1

and Level-2 activity will be levied as follows. For each IRT that applies for Level-2 accreditation TERENA will be charged a 900 Euro fee once in any one year. This fee will cover either a single assessment if successful, or up to a maximum of 2 assessments if they are unsuccessful in the first instance. Once a team achieves Level-2 accreditation TERENA will be charged 50 Euros per month for each such team (600 Euros per year) for maintenance at that level for the remainder of the pilot.

On this basis, M&I/Stelvio is offering to run the TI pilot service for a second year after the end of the current one-year pilot, should TERENA and TF-CSIRT consider that appropriate.

Brian reported that if it is decided to extend the pilot for another year, it is time to re-constitute the Review Board from the existing volunteer members to a panel made up from Level-2 teams as originally envisaged when the TI was setup. It was agreed that members of the current Review Board would develop a scheme on how to elect a new Review Board. The aim is to have the new Review Board in place before the next TF-CSIRT meeting in Manchester during September 2001.

The meeting unanimously recommended TERENA to extend the pilot for another year as proposed. The charges could be re-invoiced by TERENA to the CSIRTs concerned; TERENA would consider paying itself 450 euro of the 900 euro charge for CSIRTs from TERENA member organisations.

To conclude the agenda item on the TI, attendees were asked which of the organisations not already at Level-2 would be applying for assessment. The overall majority confirmed that they would be putting their organisation forward for assessment before the end of the second year of the pilot period. The only reasons given for reservation were internal organisational problems or the need to develop an internal business case. To assist organisations in developing cases, M&I/Stelvio were reminded of their action to produce a management information sheet. It was agreed that this should be issued via TERENA, so as to avoid any potential for the material being considered commercial advertising. Mark of M&I/Stelvio agreed to draft a list of the advantages for management by 15 June 2001.

5. The 13th FIRST conference, FRANCE, David Crochemore, RENATER

David Crochemore reported on the proposed programme for the forthcoming FIRST conference in Toulouse, France 17-22 June 2001. The programme includes tutorials, hot-topic, work-in-progress and BoF sessions. Gorazd, Don and Peter will be involved in a session on IRT operation. There will also be a panel discussion on the CSIRT model in the real world.

6. Contacts with CEC, Karel Vietsch, TERENA

Karel Vietsch reported on two visits he had made with others to the European Commission in Brussels on TF-CSIRT business. The first visit was to participate in a workshop orgainised by DGIS (Unit 1) on 2nd February 2001. The concept of IRTs working together was well accepted with positive support from the German and British governments, only the KPN CERT expressed objections, preferring a hierarchical structure. It was agreed at the workshop that security and IRT awareness are big issues and need active promotion in the European Internet community. In discussions on specific topics, the idea of a European Security observatory did not find favour.

On 23rd February 2001, a deputation from TF-CSIRT visited the Commission to talk about areas in which the EU might consider funding projects. The main themes that emerged from the discussions were potential project proposals for:

1. A handbook of what network related activities are against the law in the individual European countries and what evidence is required to enable prosecution.
2. Best Practice to study the scope of possible awareness activities
3. A project to promote the establishment of new CSIRTs
4. An action to train new (staff of) existing CSIRTs

In the context of item 1, Andrew Cormack had written a short document, which was sent to the Commission explaining which acts our community want to be covered in such a handbook (explaining sniffing, spamming etc.). As yet, no reply has been received from the Commission as a consequence, Andrew Cormack agreed to remind them. If this would lead to a positive response from the Commission, the idea could be discussed further in the next TF-CSIRT meeting.

It was agreed that one approach to promoting best practice is to illustrate with examples from real life, maybe supplemented with a collection of horror stories. This could be a potential new activity for TF-CSIRT members initially developing a plan of how best practice could be developed and used.

It was reported that although TF-CSIRT suggested a project to promote the establishment of new IRTs, specifically addressing those networks that don't yet have teams, in political circles, not everybody is supporting the idea of IRTs. The Commission thought this would need a lot of justification.

Finally, the idea of a training workshop was mentioned.

Karel asked the Task Force members which, if any of the above proposals should be followed up. He remarked that although proposals can be submitted at any time, due to the practicalities of funding cycle we probably make our target date before the end of 2001.

Jacques Schuurman and Andrew Cormack agreed that a handbook would be an important and useful project that could deliver lasting results. Producing the handbook would be a diversion from usual IRT and TF-CSIRT activities and be interesting exercise to undertake. There was also interest in holding an awareness workshop for "organisations that ought to start an IRT".

Wilfred asked if we could come up with a catalogue of activities that are against written law or Service Level Agreements of typical networks. He reported that in many cases spamming is actually against the national law. He also added that the ISP's signup contracts can specify restrictions that would allow an ISP to take action against bad behavior without going to law. It is Wilfred's opinion that collecting these details would be a precursor to producing a handbook and should be tackled first. He also thought that tackling bad behavior by proactive means was better than prosecution after the event. Karel suggested that although the handbook is a good idea it would also need the cooperation and involvement of external agencies such as the police, probably in a supervisory role.

The consensus of the meeting is that item 4: the proposal to develop training material for new IRTs should be the TF-CSIRT priority. Item 2 is probably rather too large an undertaking, and item 3 is somewhat related to item 4 and maybe there is some scope for including some of both of these elements.

It was agreed that TF-CSIRT should develop a proposal for item 4 and continue discussing the viability of developing a proposal for item 1 on the email distribution list. Karel asked for volunteers to work on these two items to make themselves known to the TERENA Secretariat staff.

- Gilles offered to make a start with preparations for yet another possible project proposal, namely concerning the secure emergency back-up infrastructure for CERTs and the software patents that had been mentioned in TF-CSIRT's first letter to the Commission; he would draft a project proposal and circulate it on the email distribution list.
- Andrew Powell offered to make an internal investigation in UK government to see if the information on prosecution requirements exists and will report back at the next TF-CSIRT meeting.
- Accompanying the preparations for TF-CSIRT's autumn training workshop (see next agenda item), Karel Vietsch and Andrew Cormack would start preparations for a project proposal to the Commission to have part of the workshop costs funded by the EU.

7. Development of Training Workshop Material

7.1. Legal Issues - Jacques Schuurman CERT-NL

Jacques Schuurman said it is important for all those involved to have a common perception of the issues. The problem is that the law is developing very slowly, whereas the speed of Internet development is very rapid. There are new forms of "misbehavior" which fall outside of boundaries foreseen by existing rules.

Jacques suggested that as a start, we need to focus on the existing rule-sets in nations (The Law), which is generally sub-divided into Criminal and Civil Law.

He reported that "Internet Law" was very difficult as there are very many areas of inconsistency on several levels. In order to have any hope of successful prosecution, it is important to prepare the CSIRTs for legally correct operation, maybe with legal backup. In particular teams must make sure there is no conflict between the contractual obligations regarding the parties involved.

In summing up, Jacques asked Task Force members to let him have suggestions of the elements that need to be covered. He added that we should attempt to make the module as generic as possible and before presentation have the material reviewed by a legal expert.

7.2. Technical Issues - Klaus Möller, DFN-CERT

In presenting the work he had completed on the Technical Issues module, Klaus Möller reported that he has found that the material will take more than 1.5 hours to present and as a result, he had concentrated on the most common incidents (but this could be different for each CERT). The prerequisite skills for the module will be basic UNIX and TCP/IP administration. The total length of material to be presented is about one hour and will include information gathering (scans, probes), breaking in (buffer overflows, format string bugs), hiding, digging in (Trojans and Backdoors), abuses (DOS). The material suggested was well received and the next step is to produce the detailed content and test the module.

7.3. Organisational Issues, Gareth Price, BTSS CSIRT

Gareth Price gave a presentation on the proposed content on the Organisational Issues module. He reported that the main areas are:

- Introducing the concept of CSIRT within organisations
- Discussions of how to establish a CSIRT and where will it be in the organisational structure.
- Links with external security organisations
- Funding of CSIRTs in the market place.

In discussion, Gareth asked if anyone tried to sell CSIRT services commercially? He suggested that there maybe some conflict if you are a supplier of services to customers who may be the origin of problems. Andrew Cormack reported that in the UK there has

not been a problem in supplying Ireland with services where the approach JANET-CERT has taken is to consider them as part of an extended constituency.

It was agreed that it would be helpful to include an overview of both academic and commercial CERT structure to give an insight for all about the similarities and differences. Gareth asked for a volunteer from the academic community to provide information on how academic CERTS fit into the academic structure.

7.4. Summary of Training Workshop Status

It was agreed that the Task Force should attempt to complete the draft training material in advance of the September meeting. Each of the module leaders was asked if this could be achieved.

Module Name	Editor	Completion by Sept.
Legal Issues	Jacques Schuurman	Will try
Organisational Issues	Claudia Natanson	Will try
Technical Issues	Klaus Möller	Confident of completion
Market Issues	Andrew Cormack	Confident of completion
Operational Issues	Gareth Price	Confident of completion

Karel Vietsch and Andrew Cormack agreed to write a draft proposal for the Commission regarding the funding of a training workshop programme. It was agreed that the writing and editing of the material is funded by the contributors under the auspices of the Task Force activities. It was also agreed that the proposal request funding for travel and subsistence for the presenters, for the presenters time in delivering the material and sponsorship of attendees. It was also noted that in writing the proposal it will be important not to forget items such as room hire and equipment hire .

John Dyer and Karel Vietsch agreed that TERENA Staff will undertake the organisation of the workshop logistics.

Andrew Cormack agreed to be training programme chair, draw-up a workshop programme and pull material together.

Authors agreed to email the completed material to TERENA two weeks in advance of Manchester meeting and it will be placed in a password-protected area of the TERENA web server.

It was agreed that it would be useful to add in a bibliography. Klaus said he had identified several papers on the Internet that would be cited.

Andrew mentioned that JANET-CERT had recently run a workshop on Computer Security implications aimed at computer staff with several papers presented by lawyers but. See the URL: http://www.ja.net/conferences/security/january01/prog.html

8. Clearinghouse for Incident Handling Tools, Yuri Demchenko, TERENA

Yuri presented the concept of creating a repository of commonly used tools. He has recently sent out a questionnaire regarding the nature of the tools being used in the various different areas of CSIRTs work. In reviewing the questions, it was suggested that a further question on licensing arrangements should be included.

Yuri reported that he has so far received 5 responses, however even this small number of responses allows to make some suggestions. All CSIRTs use in their practice tools for data/evidence collection and incident tracking and reporting. Using specific tools for incident investigation and system recovery is not common. Also not all CSIRTs use proactive tools. All responders see that Clearinghouse should contain a list of tools with descriptions of their use and functions. Most also think a collection of incident handling procedures would also be useful.

Yuri requested all those Task Force members who had not responded to his questionnaire to try and do so in the next two weeks

It was agreed that the follow-on work should address the following:

- Requirements of Incident Handling (inc Forensics) tools
- Forensic CD with tool collection (could supply via the workshops)
- Compilation of incident handling procedure

9. Next Meetings

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

5th Meeting 24 & 25 Jan 2002, hosted by Telia-CERT in Stockholm, Sweden

6th Meeting May 2002 in Copenhagen, Denmark

For the next meeting Andrew Cormack requested bookings are made to UKERNA by the end of August. Andrew will create a key we can use to encrypt credit card details.

10. Any Other Business

SURFnet invited anyone who would like a demonstration of REMEDY as a general-purpose system to contact Jan Meijer. Jan is proposing a demonstration sometime during July 2001.

Note: this is different from Andrew's presentation of the JANET-CERT system, which is built as a specific implementation on the REMEDY platform.

11. Summary of New and Open Actions

ACTION			STATUS
1-10	all	Send pointers to legal information to Andrew Cormack	Nothing received by Andrew - REMINDER to all to send information
2-07	Andrew Cormack	Prepare demonstration of Remedy System for September Seminar	For September
2-10	Yuri Demchenko	Coordinate questionnaire on CSIRT tool usage	Ongoing
3-01	M&I/Stelvio	Prepare a contract with TERENA on the provision of the second year of the TI pilot	
3-02	TI Review Board	Develop a scheme on how to elect a new Review Board.	
0-02 3-03	Mark M&I/Stelvio	Draft a list of the advantages of TI accreditation by 15 June 2001.	
3-04	Andrew Cormack	Contact Commission and remind them, of our specification for handbook contents and request their reply.	
3-05	Gilles André	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 email distribution list	

3-06	Andrew Powell	Make an internal investigation in UK government to see if the information on prosecution requirements exists. Report back at the next TF-CSIRT meeting.	
3-07	Academic CSIRTs	Provide to Gareth Price information on how academic CERTS fit into the academic structure.	
3-08	Module Editors	Complete draft module material 2 weeks before next TF meeting and mail to TERENA - DEADLINE 12 September 2001	
3-09	TERENA Secretariat	Put Training material in password protected area of web server	
3-10	Karel Vietsch & Andrew Cormack	Draft a proposal to the Commission regarding the funding of a CSIRT training workshop	
3-11	TERENA	Organise Training Workshop Logistics	
3-12	Andrew Cormack	Draw up Training Workshop Programme and act as Programme Chair	

Appendix 1.
List of Attendees 3rd TF-CSIRT Meeting

1 June 2001
Ljubljana, Slovenia

Name	**Affiliation**
Wilfried Wöber	ACOnet
Gozard Bozic	ARNES
Pascal Delmoitié	BE CERT
Tom Mullen	BTCERTCC
Gareth Price	BT IGNITE

Nataa Glavor	CARNet CERT
Vlado Pribolsan	CARNET CERT
Michelle Danho	CERT RENATER
Rodrigo Castro	IRIS-CERT
David Crochemore	CERT RENATER
Gilles André	CERTA
Michel Dupuy	CERTA
Philippe Bourgeois	CERT-IST
Jacques Schuurman	CERT-NL SURFnet
Jan Meijer	CERT-NL SURFnet
Matthias Etrich	Deutsche Telekom AG
Klaus Möller	DFN-CERT
Preben Andersen	DK-CERT
Sandra Hermández	esCERT
Matias Bevilacqua	esCERT
Chelo Malagón	IRIS-CERT
Andrew Cormack	JANET-CERT
Robert Morgan	JANET-CERT
Ian Bryant	JSYCC (UK MODCERT)
Mark Koek	M&I/Stelvio (TI)
Peter Bivesand	SESIC
Christoph Graf	SWITCH-CERT
Jimmy Arvidsson	TeliaCERT
Brian Gilmore	TERENA
John Dyer	TERENA
Karel Vietsch	TERENA
Yuri Demchenko	TERENA
Per Arne Enstad	UNINETT/NORDUNET CERT
Andrew Powell	UNIRAS