

**Minutes of the 14<sup>th</sup> TF-CSIRT meeting  
London, 28 January 2005**

[Please note that a seminar was held the previous day. Presentations from the seminar and the meeting can be found at <http://www.terena.nl/tech/task-forces/tf-csirt/meeting14/programme.html>]

**1. Welcome and apologies**

Gorazd Božič welcomed the participants. The list of those present and the list of people who sent their apologies are below at the end of these minutes.

Adam Peake from GLOCOM, Japan gave a short presentation about their activities. They were preparing a questionnaire for CSIRTs in order to understand the current situation and during their European visit had meetings with various involved parties. He said that the results of the questionnaire would be accessible on-line and presented at the next FIRST conference in Singapore. Adam Peake also promised to make available a summary report about their meetings with people in Europe. He expressed thanks for the opportunity to talk with the TF-CSIRT community.

**2. Approval of the Minutes and Status of Actions from the last meeting**

The minutes of the last meeting held on 24 September 2004 were approved.

Action items:

11-05 Jacques Schuurman – to send the information related to CHIHT from SURFnet's repository.  
*Done, see agenda item 8.*

11-06 Marco Thorbrügge – to produce a new survey about the tools for CHIHT and present latest developments of CHIHT in the next TF-CSIRT meeting.  
*Done, see agenda item 8.*

12-01 Damir Rajnovic – to investigate the possibility to organise a workshop about product vulnerabilities.  
*Done. The workshop will be held on 8 February 2005 in Paris. Damir Rajnovic said that the workshop would be a closed one for vendors and many of them would participate. He would give a report about the workshop in the next TF-CSIRT meeting.*

*ACTION 14-01: Damir Rajnovic – to give a report about the Product vulnerabilities workshop in the next TF-CSIRT meeting.*

12-03 Karel Vietsch – to create a short slide show for marketing the TRANSITS courses outside the NREN community.  
*Dropped. Karel Vietsch said that it had not been done intentionally, because the last TRANSITS workshop was overbooked. See agenda item 4.1.*

12-07 Marco Thorbrügge – to ask people in the mailing list to send him information about the teams' work flows.  
*Done, see agenda item 8.*

12-08 Wilfried Wöber and Jan Meijer – to investigate which certificates are possible to use for the IRT objects and how to extend this list.  
*Ongoing. Wilfried Wöber and Jan Meijer would come up with a report about all the things that should be done to the IRT object and later to contact the TI to ensure x.509 objects from the TI repository would get merged into IRT objects as well.*

13-01 Wilfried Wöber – to announce the TRANSITS training courses on the RIPE mailing lists.  
*Dropped. Karel Vietsch said that it had not been done intentionally, because the last TRANSITS workshop was overbooked. See agenda item 4.1.*

13-02 Gorazd Božič – to send documents about ENISA stakeholders group to the TF-CSIRT mailing list.

*Done.*

13-03 Gorazd Božič – to lead the discussion on how to nominate and elect somebody to represent TF-CSIRT on the ENISA Stakeholders group.

*Done. Andrew Cormack has been appointed to the ENISA Stakeholders group.*

13-04 Jacques Schuurman – to send the latest version of the MoU with APCERT to the TF-CSIRT mailing list.

*Done. See agenda item 7.*

13-05 Marco Thorbrügge – to send a reminder to the TF-CSIRT mailing list to review the questionnaire.

*Done.*

13-06 Gorazd Božič, Baiba Kaškina – to invite somebody from the Grid community to make a presentation in the next TF-CSIRT seminar in London.

*Done.*

Wilfried Wöber proposed to remind the group about the action items some weeks before the next meeting. Baiba Kaškina promised to do that.

### **3. Trusted Introducer - Report from the meeting of accredited CSIRTs**

Don Stikvoort presented the TI status report and feedback from the meeting of accredited CSIRTs that was held on the previous day. He emphasised the importance of building the trust network and the means that the TI uses for that, i.e. the accreditation process. The TI database contains data on listed teams and accredited teams. He also presented charts with the number of CSIRTs in the TI repository and accredited CSIRTs.

The TI domain name has been changed to *trusted-introducer.nl*. Don Stikvoort mentioned the free services provided by the TI and other services which were available only for the accredited teams. He told the group that the CSIRT Code of Practice would be ready for signing in one of the following TI meetings.

### **4. Update on the EC funded projects**

#### **4.1. TRANSITS**

Karel Vietsch spoke about the TRANSITS project. He gave details about the 5 training courses which have been held, including number of participants, represented countries, etc. The last TRANSITS workshop in November 2004 in Prague was overbooked. After a review of the available budget it has been decided to organise two more workshops (7 in total). The 6<sup>th</sup> workshop will be held in Chantilly, France on 17-18 February 2005 and it was already fully booked. The last TRANSITS workshop will be held in April or May 2005 in Portugal.

Karel Vietsch mentioned the agreement between TRANSITS and FIRST that FIRST would use the TRANSITS materials for courses in Latin America and the Asia-Pacific region. A very successful course has been held in November in Rio de Janeiro for Latin America. No course has been held yet in the Asia-Pacific region; it had been discussed that the cultural differences will make a successful course more difficult in Asia..

The future of the TRANSITS materials and courses in Europe was discussed. One possibility would be that FIRST would take responsibility for updating the materials and organising workshops in Europe as well as in other regions. Karel Vietsch and Andrew Cormack would have a meeting with FIRST executives on 8 February 2005. Other alternatives are being investigated as well.

*ACTION 14-02: Karel Vietsch – to report about the results from the meeting with FIRST about the responsibility for TRANSITS in Europe.*

Wilfried Wöber pointed out that security has been mentioned as a very important topic in many communities, including the EC, therefore CSIRTs should apply for new funding. He also proposed to ask for some support from the national ISP associations and ENISA. Karel Vietsch replied that it would be easier to receive money from a single source of funding i.e. the EC, but lately they have been supporting mostly large projects only like GN2 or EGEE. Regarding ENISA he thought that it was focusing on general awareness raising but did not have funds for practical courses. Gorazd Božič replied that one of ENISA's goals was to support and facilitate formation of CERTs in countries where they were not yet established. The TRANSITS courses would be an ideal tool for achieving this goal. He promised to discuss this with Mr. Pirotti and report back in the next TF-CSIRT meeting.

*ACTION 14-03: Gorazd Božič – to investigate if ENISA could give some funding for the TRANSITS workshops.*

Serge Droz added that it would be useful to organise courses even if participants would have to cover full costs. Karel Vietsch replied that it would be doable for richer countries but unaffordable for others. Also he was worried about the maintenance of the materials.

#### **4.2. Relation to GN2, discussion on GN2/JRA2 advisory panel**

Jacques Schuurman spoke about GN2's relationship with TF-CSIRT. He gave an overview of the GN2 project including the project partners, dates, structure, timelines, budget, and manpower. All five JRA2 work items were discussed.

WI1 had to produce deliverable "Security recommendation and policy based on operational experiences and new requirements". The deliverable was completed and would be reviewed in October 2005.

WI2's main deliverable was "Toolset for proactive monitoring traffic on live networks with high bandwidth". Jacques Schuurman said that it was an ongoing deliverable and would be discussed in the GN2 NRA2 meeting that would follow this TF-CSIRT meeting.

WI3 would implement the results of the WI2 work. Claudio Allocchio said that it would be not only the technical implementation but also a lot of coordination effort and human networking. He noted that all the deliverables will be public.

WI4 was the relationship with TF-CSIRT. A report would have to be produced after first 18 months of the GN2 project.

WI5 was the establishment of the advisory panel. Jacques Schuurman explained the goals of the panel and gave a roadmap. Gorazd Božič emphasised that the panel should be created during the following GN2 JRA2 meeting. The first meeting of the panel would be held in May 2005 in Zürich and the deliverable would be in due in August 2005. The proposed specification and composition of the panel were given. The following people have been appointed – Gorazd Božič (TF-CSIRT chair), Christoph Graf (JRA2 activity leader), Jan Meijer, Jimmy Arvidsson, Marco Thorbrügge, Urpo Kaila, and Wilfried Wöber. A place for a government representative was still empty and Gorazd Božič asked for volunteers.

The JRA2 meeting was held after the TF-CSIRT meeting.

#### **4.3. LOBSTER**

Baiba Kaškina gave a short overview about the LOBSTER project. The main goal of the LOBSTER project is to deploy an advanced pilot European Internet traffic monitoring infrastructure based on passive monitoring sensors at speeds from 1 Gbps and possibly up to 10 Gbps. She spoke about the project partners, objectives and technical challenges.

There would be many possibilities for collaboration between the LOBSTER project, the TF-CSIRT community and the GN2 JRA2 group. As the first one Baiba Kaškina mentioned a questionnaire which would be prepared by the LOBSTER project in order to get information about the situation with regard to passive network monitoring in various organisations as well as to collect needs and expectations of potential LOBSTER users. She promised to send information about the questionnaire to the TF-CSIRT mailing list.

*ACTION 14-04: Baiba Kaškina – to send information about the LOBSTER questionnaire to the TF-CSIRT mailing list.*

Also she invited people from GN2 JRA2 to participate in the next LOSBETR project meeting which will be held on 21-22 March 2005 in Amsterdam. LOBSTER people would be available to follow GN2 JRA2 activities as well.

After the presentation various issues were discussed, e.g. Combo cards vs. DAG cards, legal implications, standards, motivation, etc. It was decided to have an update about the LOBSTER project in the next TF-CSIRT meeting. Andrew Cormack proposed to give an overview about the legal situation regarding network monitoring.

*ACTION 14-05: Andrew Cormack – to give an overview about the legal situation regarding network monitoring issues.*

## **5. Update on European Abuse Forum**

Don Stikvoort gave an update on the European Abuse Forum (EAF) activities. The forum was founded to discuss pragmatic abuse handling issues. It organised 2 workshops per year. Three workshops have been held, Don Stikvoort gave details about all of them. The 3<sup>rd</sup> EAF workshop was held in November 2004 in Amsterdam, the Netherlands. It was hosted by KPN-CERT. Don Stikvoort outlined the workshop results and the consensus reached as well as the operational framework elements including membership, support function and coordination.

The membership of the EAF was team-oriented, but individual members also could join, for example people from TF-CSIRT who were not working for ISPs, but contributing to the forum.

## **6. Update on FIRST**

Udo Schweigert reported about the latest activities in FIRST. The FIRST website has been relaunched, rollout of the FIRST authentication certificates was scheduled for February 2005, the library of FIRST best practice guides has been published and was partly publicly available. The new FIRST membership process was in operation and some teams have been suspended due to non-compliance to the new process.

FIRST had identified four major regions, i.e. North America, Europe, Asia/Pacific, and Latin America and would try to hold either the Technical Colloquium (TC) or the FIRST conference in each of these regions each year.

FIRST had recognised TF-CSIRT as a key player in Europe and proposed to coordinate the planning and logistics activities regarding its European meetings with TF-CSIRT. Udo Schweigert gave figures on how many FIRST-Team members and non-FIRST-Team members were participating in this TF-CSIRT event. He emphasised that co-location of the meetings would be beneficial for both organisations.

Gorazd Božič summarised that the TCs were usually held on Monday and Tuesday, the TF-CSIRT event on Thursday and Friday, and the Wednesday could be used for other side meetings like the European Abuse Forum meeting or others. The downside of such an arrangement would be that people would have to be away from their workplace for the whole week. Also the logistics would become more difficult.

The group discussed this proposal. Gilles André said that his organisation would send different people to both events usually. David Parker pointed out the funding issues of organising such long event. It

was decided to ask the FIRST SC if they could cover the expenses of organising joint meetings in Europe. In case of a positive answer the TF-CSIRT meeting in September 2006 could be adjacent to the FIRST TC. Udo Schweigert promised to discuss this within the FIRST SC and report back to the group.

*ACTION 14-06: Udo Schweigert – to discuss funding issues of joint meetings with the FIRST SC and report back to the TF-CSIRT group.*

## **7. Memorandum of Understanding with APCERT**

Jacques Schuurman spoke about the Memorandum of Understanding (MoU) between TF-CSIRT and APCERT. The purposes of the MoU would be mutual recognition as regional expertise bodies, provision of an established channel of information exchange, establishment of a framework for joint project undertakings, direct operational contact points, etc. He pointed out that it has been intended to be a lightweight document.

Jacques Schuurman reminded the group that the MoU has been discussed on the mailing list and he had received few comments. The group discussed the information disclosure issue once again and Jacques Schuurman promised to circulate the final version of the MoU. He hoped that the MoU will be signed at the next FIRST conference in Singapore.

*ACTION 14-07: Jacques Schuurman – to circulate the final version of the Memorandum of Understanding to the TF-CSIRT mailing list.*

## **8. Improvements to CHIHT**

Marco Thorbrügge gave an update on the CHIHT improvements. Adding more information to the clearing house, particularly completing the information for the existing tools, was ongoing. He pointed out the lack of feedback and some technical problems.

The next phase of the re-organisation was the creation of a new questionnaire. It was designed, reviewed by teams and the survey was started in November 2004. So far 5 teams have answered it. Marco Thorbrügge encouraged people to provide more feedback. He informed the group that the last step – adding workflow descriptions - would be dropped because he has received input from only 2 teams. Andy Bone proposed to make it an action for all the teams to provide information to CHIHT.

*ACTION 14-08: All the teams – to provide input to CHIHT.*

Marco Thorbrügge also told the group about SURFnet's special language for handling incidents. It was decided that he and Jacques Schuurman would review it and send the details to the mailing list.

*ACTION 14-09: Marco Thorbrügge, Jacques Schuurman – to review SURFnet's special language for incident handling and send the details to the TF-CSIRT mailing list.*

## **9. Update on RTIR working group**

Andy Bone gave an overview of the RTIR tool and the working group activities. RTIR was the only open source incident handling tool. The RTIR WG met on 26 January 2005 in Didcot. Andy Bone told the TF-CSIRT group about the issues they have discussed including teams updates, RTIR 1.2 version, Code of Conduct and others.

The Code of Conduct was finalised and would be signed by the teams in the first week of February 2005. TERENA will hold the Code of Conduct for the Working Group.

## **10. Results of the seminar sessions, ideas for the future sessions**

Andrew Cormack proposed to move the seminar to the afternoon of the first TF-CSIRT day in order to save time for those who are not involved in the TI or GN2 meetings. The group discussed this proposal and agreed to try swapping Thursday sessions in the next TF-CSIRT event. The evaluation of that layout should be done after the event.

For future seminar sessions Kauto Huopio suggested to talk about case studies in handling large-scale incidents at various points including the coordination issues, and vulnerability coordination.

### **11. Status of the Terms of Reference and other TF-CSIRT work items/deliverables**

Gorazd Božič summarised that the progress of the work items and deliverables has been discussed during the meeting and there was no need to review the Terms of Reference.

### **12. Date of the next meetings**

The next meeting will be held 12-13 May 2005 in Zürich, Switzerland (hosted by SWITCH-CERT). Serge Droz invited the group to Zürich and showed some pictures from the city and the planned social event venue. He asked people to inform SWITCH about other meetings adjacent to the TF-CSIRT event as soon as possible.

The subsequent TF-CSIRT meeting will be hosted by CERT.PT in Lisbon, Portugal on 15-16 September 2005. Gorazd Božič asked participants to volunteer for hosting the January 2006 meeting.

### **13. Any Other Business**

Gorazd Božič and the group expressed their thanks to JANET-CERT for organising a very nice meeting.

Andy Bone thanked the participants and announced that he will be leaving the JANET-CERT team.

### **List of meeting participants**

<i>Name</i>	<i>Organisation</i>	<i>Country</i>
1. Claudio Allocchio	GARR-CERT	Italy
2. Preben Andersen	DK-CERT	Denmark
3. Gilles André	CERTA	France
4. Jimmy Arvidsson	TeliaSoneraCERT CC	Sweden
5. Dmitriy Avramenko	RU-CERT	Russia
6. Andy Bone	JANET-CERT	United Kingdom
7. Gorazd Božič (Chair)	SI-CERT	Slovenia
8. Martin Camilleri	mtCERT	Malta
9. Domingo Cardona	esCERT	Spain
10. Tim Charrot	QinetiQ CIRT	United Kingdom
11. Garaidh Cochrane	JANET-CERT	United Kingdom
12. Andrija Condor	CARNet	Croatia
13. Andrew Cormack	UKERNA	United Kingdom
14. Michelle Danho	RENATER CERT	France
15. Sander Degen	TNO	the Netherlands
16. Gary Dooley	Royal Mail Group	United Kingdom
17. Serge Droz	SWITCH-Cert	Switzerland
18. Jan Drömer	PHILIPS	the Netherlands
19. Michel Dupuy	CERTA	France
20. Ralf Dörrie	Telekom-CERT	Germany
21. Per Arne Enstad	UNINETT CERT	Norway
22. Lionel Ferette	BELNET	Belgium
23. Carlos Fuentes Bermejo	JANET-CERT	United Kingdom
24. Mikhail Ganev	RU-CERT	Russia
25. Stefan Grinneby	SITIC	United Kingdom
26. Mike Harris	Royal Mail	United Kingdom
27. Kauto Huopio	FIGORA / CERT-FI	Finland
28. Przemek Jaroszewski	CERT Polska / NASK	Poland
29. Richard Jones	BT SBS	United Kingdom
30. David Joyce	BTCERTCC	United Kingdom
31. Mike Kadylak	BT Plc	United Kingdom
32. Urpo Kaila	FUNET CERT	Finland

33. Baiba Kaškina (Secretary)	TERENA	-
34. Ulrich Kiermayr	ACOnet-IRT	Austria
35. Adrian King	SI-CERT	Slovenia
36. Johanna Kinnari	FICORA / CERT-FI	Finland
37. Georgios Koutepas	GRNET	Greece
38. Andrea Kropacova	CESNET z.s.p.o.	Czech Republic
39. Sergey Linde	RU-CERT	Russia
40. Stelios Maistros	GRNET-CERT	Greece
41. Mirosław Maj	CERT Polska	Poland
42. Chelo Malagón	IRIS-CERT, RedIRIS	Spain
43. Jan Meijer	SURFnet / CERT-NL	The Netherlands
44. Milda Mimiene	LITNET CERT	Lithuania
45. Keith Mitchinson	QinetiQ CIRT	United Kingdom
46. Martin Mogensen	DANTE	United Kingdom
47. Maurizio Molina	DANTE	United Kingdom
48. Ian Neilson	CERN	Switzerland
49. Gustavo Neves	FCCN (CERT.PT)	Portugal
50. Carol Overes	GOVCERT.NL	the Netherlands
51. David Parker	UNIRAS/NISCC	United Kingdom
52. Adam Peake	GLOCOM	Japan
53. Joao Pagaiame	FCCN	Portugal
54. Scarlet Pruitt	IDG News Service	United Kingdom
55. Damir Rajnovic	Cisco Systems	United Kingdom
56. Maria Rådström	Telia Abuse	Sweden
57. Jacques Schuurman	SURFnet / CERT-NL	The Netherlands
58. Udo Schweigert	Siemens-CERT	Germany
59. Sharon Sciberras	mtCERT	Malta
60. Krzysztof Silicki	NASK/CERT Polska	Poland
61. Don Stikvoort	Trusted Introducer	the Netherlands
62. Marco Thorbrügge	DFN-CERT	Germany
63. Maris Urkis	LITNET CERT	Lithuania
64. Karel Vietsch	TERENA	-
65. Torbjörn Wictorin	SunetCert	Sweden
66. Wilfried Wöber	ACOnet-IRT	Austria
67. Dimitris Zacharopoulos	AUTH-CERT	Greece

***Apologies were received from:***

Roberto Cecchini	GARR-CERT	Italy
Natasa Glavor	CARNet CERT	Croatia
Christoph Graf	SWITCH-CERT	Switzerland
Mark Koek		the Netherlands
Klaus-Peter Kossakowski	PRESECURE	Germany
Antonio Liu	PRE-CERT	Germany

## **RESULTING ACTION ITEMS**

14-01	Damir Rajnovic	Give a report about the Product vulnerabilities workshop in the next TF-CSIRT meeting.
14-02	Karel Vietsch	Report about the results from the meeting with FIRST about the responsibility for TRANSITS in Europe.
14-03	Gorazd Božič	Investigate if ENISA could give some funding for the TRANSITS workshops.
14-04	Baiba Kaškina	Send information about the LOBSTER questionnaire to the TF-CSIRT mailing list.
14-05	Andrew Cormack	Give an overview about the legal situation regarding network monitoring issues.
14-06	Udo Schweigert	Discuss funding issues of joint meetings with the FIRST SC and report back to the TF-CSIRT group.
14-07	Jacques Schuurman	Circulate the final version of the Memorandum of Understanding to the TF-CSIRT mailing list.
14-08	All the teams	Provide input to CHIHT.
14-09	Marco Thorbrügge, Jacques Schuurman	Review SURFnet's special language for incident handling and send the details to the TF-CSIRT mailing list.
12-08	Wilfried Wöber and Jan Meijer	Investigate which certificates are possible to use for the IRT objects and how to extend this list.