TSec(05)091

Minutes of the 16th TF-CSIRT meeting
Lisbon, 16 September 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/meeting16/]

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.
The changes to the agenda were announced.

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

The minutes of the last meeting held on 13 May 2005 were approved.

Action items:

15-01 Don Stikvoort – to give a presentation about the issues e-coat is working on in one of the following TF-CSIRT seminars.
Ongoing. The presentation will be given in January 2006.

15-02 Baiba Kaškina – to set up email address for the CSIRT mentoring initiative, link the webpage and advertise the initiative.
Done.

15-03 Gorazd Božič – to choose the candidate for deputy chair and to ask approval from the TF-CSIRT group.
Done. See agenda item 13.

14-03 Gorazd Božič – to investigate if ENISA could give some funding for the TRANSITS workshops.
Done. Gorazd Božič has received negative answer from ENISA. Karel Vietsch said that in the final TRANSITS review he heard more positive feedback from the EC officials. See agenda item 3 and 9.1.

14-08 All the teams – to Provide input to CHIHT.
Done. Marco Thorbrügge said that in spite of leaving DFN-CERT he would continue maintaining the CHIHT in his free time and DFN-CERT would host it, but another host and maintainer should be found sooner or later. He asked people to continue to inform him about new and interesting tools to include in the CHIHT.

3. ENISA update

Marco Thorbrügge spoke about the ENISA developments. He started working for ENISA on 1 September 2005 and has participated in a couple of events on behalf of ENISA already. The ENISA office has been moved to Heraklion, Greece.

He summarised the ENISA's relationship with CSIRTs. ENISA would not create a European CERT; its main function would be giving advice to different bodies – governments, SMEs and others. Three ad-hoc working groups have been created, i.e. risk management, public relations and awareness raising, CSIRT cooperation. Marco Thorbrügge was glad to have many people from TF-CSIRT in the "CSIRT cooperation" working group. The Terms of Reference of the working groups would be on-line soon.

Next ENISA organised events will be conferences in Budapest and Vilnius. Marco Thorbrügge promised to inform the group about them. He proposed to allocate a longer slot in the next TF-CSIRT meeting to a report about the ENISA developments and a discussion of collaboration possibilities. He emphasised that TF-CSIRT is an important group for ENISA and they hope to have good collaboration.

He promised to contact officially the TERENA Secretariat regarding support for the post-TRANSITS courses. The Legal Handbook also will be facilitated by ENISA.

4. APCERT update

Yurie Ito from JPCERT/CC presented the APCERT activities. She spoke in detail about the structure, history, objectives, members and activities of APCERT. It is a different organisation than TF-CSIRT with more emphasis on the direct communication between CSIRTs in Asia Pacific for incident handling. APCERT helps to contact victims and involved sites via point of contact (POC) CSIRTs. The objectives of APCERT are to share security information among the APCERT members, to handle security issues on a regional basis, to support establishment of CSIRTs in other countries, to collaborate with other regional initiatives, etc. APCERT and APNIC share the same regional boundaries.

There are 17 members of APCERT. Two new members were BruCERT from Brunei and GCSIRT from the Philippines. Many other countries also have expressed interest to join APCERT, including India, Pakistan and even countries from the Middle-East. However, APCERT is open only to countries from the APNIC region, Middle-Eastern countries are in the RIPE IP space, and therefore they should be invited to participate in TF-CSIRT.

Yurie Ito outlined how the incidents have changed in the last two years and the incident response also had to be changed. She spoke about the APCERT methods of work and achievements. APCERT has been very active in education and training in order to raise awareness and encourage best practices, as well as collaborating with governments and advising as security experts.

Maurizio Molina wanted to know more details about the information sharing in APCERT. Yurie Ito clarified that they were informing each other about spikes in the traffic diagrams as well as exchanging anonymised IODEF data.

5. Memorandum of Understanding with APCERT, appointing the liaison

Gorazd Božič informed the group that the Memorandum of Understanding (MoU) with APCERT has been signed on 28 June 2005 in Singapore, during the FIRST conference, by Mark McPherson and Gorazd Božič. He thanked the group for their efforts in preparing the MoU.

According to the MoU liaison persons should be appointed by both sides. He proposed to appoint Jacques Schuurman from SURFnet-CERT to be the liaison from the TF-CSIRT side. The participants unanimously approved the proposal. Gorazd Božič would inform APCERT about the liason. Yurie Ito was asked if the liason from the APCERT side has been appointed. She said that it had not been done yet.

ACTION 16-01: Gorazd Božič – to inform APCERT that Jacques Schuurman from SURFnet-CERT has been apponted as the liason from the TF-CSIRT side.

Yurie Ito expressed her delight that the MoU has been signed. She invited TF-CSIRT particpants to join the next APCERT meeting in China in February 2006.

6. Collaboration with CERT CSIRT Development Team

Robin Ruefle from the CERT CSIRT Development Team spoke about the possible areas of collaboration between TF-CSIRT and the CERT CSIRT Development Team. She mentioned developing an Incident Management Body of Knowledge, collecting case studies on CSIRT organisational structures and "getting started" stories, building an archive of example incident reporting forms, incident categories and other templates, reviewing or contributing to document updates, developing a draft CSIRT taxonomy, etc. The CERT CSIRT Development Team would be interested in both formal and informal collaboration.

Gorazd Božič proposed the group to discuss these areas of collaboration. He thought that reviewing documents would be an obvious contribution from the community. Damir Rajnovic asked if a list of volunteers for reviewing would be needed or the documents could be simply sent to the TF-CSIRT

mailing list. Robin Ruefle replied that a list of volunteers could assure that their opinion would be taken into consideration. Gorazd Božič agreed to collect the names of the volunteers and to send them to Robin Ruefle. She said that a document for review could be expected before summer 2006. Each document would be announced on the list and reviewed by volunteers.

ACTION 16.02: Gorazd Božič – to ask in the mailing list for volunteers to review the CERT CSIRT Development Team documents and to inform Robin Ruefle about the results.

Urpo Kaila asked about the anonymisation issues regarding the CSIRT stories. Robin Ruefle said that usually the information was not sensitive, but they have done already anonymisation for some stories changing all data that could lead to a particular team.

The group discussed the legal issues, whether a lawyer should be invited to a TF-CSIRT event, and what kind of legal information could be shared as best practices. Andrew Cormack said that the incident response process should be documented to find balance between privacy and needs for incident response. He proposed to share the JANET's process. Damir Rajnovic proposed to invite their lawyer to the TF-CSIRT event to talk about these issues.

Gorazd Božič suggested establishing a communication channel between TF-CSIRT and CERT/CC. Damir Rajnovic suggested subscribing liaisons from APCERT and CERT/CC to the TF-CSIRT mailing list. Another suggestion was to create a separate mailing list as a communication channel among the different initiatives. Gorazd Božič would investigate this issue.

ACTION 16.03: Gorazd Božič – to investigate the possibilities for communication channel among the initiatives before the next TF-CSIRT meeting.

Regarding the CSIRT case studies Gorazd Božič said that people know many examples about different teams, they just should be written down. Also information from the TI website could be useful.

7. FIRST update

Yurie Ito spoke about the latest FIRST developments. She introduced the new Steering Committee (SC) members and their roles. A lot of positive changes were planned, i.e. the website and the conference would be improved, the members would be better informed. So far FIRST has not been conducting organisational liaisons, but now Yurie Ito has been appointed as the liaison and outreach member of the SC. She would meet involved organisations; keep dialogue with TF-CSIRT, APCERT and other regional initiatives to ensure that all the efforts are joined. She would also participate in conferences and meet the law enforcement people to open new communication channels.

Two new special interest groups (SIG) have been formed, i.e. Common Vulnerability Scoring System (CVSS) SIG and Vendor SIG. Yurie Ito spoke about the background and plans of the SIGs. The Vendor SIG will organise a meeting on 16 November 2005 in California, hosted by Oracle. Damir Rajnovic was the moderator of both working groups, he should be contacted for more information.

Other upcoming FIRST events were presented as well, i.e. the FIRST TCs and the next FIRST conference. Yurie Ito encouraged people to submit papers for the next FIRST conference and to attend it. She proposed to organise a Regional Initiatives Joint Workshop at the Baltimore conference in 2006 to discuss how FIRST could support the regional frameworks. TF-CSIRT participants were very positive about this proposal.

8. Update on RTIR working group

Carol Overes gave an update about the RTIR WG and project with Best Practical (BP). In the framework of this project, BP would produce the features required by the RTIR WG in three milestones. The RTIR WG would test and evaluate the deliverables.

TERENA has received money from all the WG partners, the contract with BP was signed and development will start on 6 October 2005. The point of contact for BP would be Carlos Fuentes Bermejo. The WG would be chaired by Robert Morgan. The deadlines for the deliverables would be 6 April 2006, 6 October 2005 and 6 April 2007. Carol Overes presented the test and evaluation process

that has been discussed by the WG and would be finalised soon. The test group would consist of 4 core members and other volunteers.

Gorazd Božič asked if it was planned to improve the API documentation. Carol Overes said that improvement of documentation would be one of the BP tasks. It was asked if the RTIR WG would consider incorporating some features from the AIRT software. Carol Overes said that it could be considered in the future. Teun Nijssen added that AIRT software has only one year of production experience, they had started to present it only one month ago. He agreed that in future some collaboration could be done.

9. Update on the EC funded projects

9.1. TRANSITS – the final report

Karel Vietsch spoke about the TRANSITS project. He gave details about the 7 training courses which have been held during the lifetime of the project, including number of participants, represented countries, sectors, etc. The project's final review was on 14 September 2005 in Brussels, it went very well. The course material consisted of five modules. Additional evening sessions have been added as well, e.g. incident handling scenarios, PGP key signing. Those were highly rated by students.

Karel Vietsch spoke about the agreement between TRANSITS and FIRST that FIRST would use the TRANSITS materials for courses in Latin America and the Asia-Pacific region during the lifetime of the TRANSITS project. FIRST had organised two "train the trainers" workshops and three FIRST/TRANSITS courses in different world regions.

A Memorandum of Understanding was signed by TERENA and FIRST in June-July 2005, stating that FIRST would continue organising training workshops in the Latin America and Asia-Pacific regions. FIRST would also provide funding for the FIRST secretariat (Don Stikvoort) to be the editor-in-chief and the repository for updating the TRANSITS materials. Between mid-2005 and mid-2006 FIRST and TERENA would jointly organise two training courses in Europe where participants would have to cover the real costs of the course. The agreement would be reviewed in mid-2006.

Karel Vietsch emphasised that volunteers would be needed to update all five TRANSITS modules (approximately 3 people per module) as well as trainers for the upcoming TRANSITS courses in Europe. SWITCH has volunteered to update the technical module by November 2005, material translations to Chinese, Spanish and French were in progress. There were also plans to develop regional variants of modules (e.g. legal).

The following events have been planned – "train the trainers" workshop in Baltimore, USA, June 2006, a FIRST-organised course in Buenos Aires, Argentina, October 2005, and a TERENA/FIRST-organised course in Vienna, Austria, 21-22 November 2005. The Vienna workshop will be sponsored by ISPA. Karel Vietsch announced the details for this workshop. The deadline for applications was 11 October 2005. The registration fee would be 500 EUR, without the ISPA sponsorship it would have been 750 EUR.

In summary, the project has been very successful, all the objectives were achieved and arrangements have been made for the continuance of activities after the completion of the project.

Yurie Ito congratulated to project team with the great success of this project. The ENISA involvement in the future workshops was discussed. Andrew Cormack suggested that ENISA could encourage the member states to use the course material. The funding issue should be discussed with the ENISA again later.

9.2. GN2/JRA2 update

Christoph Graf gave an update on the GN2/JRA2 activities. He summarised the GN2 project and all the JRA2 work items. The first year of the project was finished; Christoph Graf outlined the objectives and achievements of the JRA2. The main achievements were having identified, tested and assessed sets of tools, having designed and tested co-ordination infrastructure, and having traffic cleaning capability proposed to GEANT2 backbone. The toolset elements and conducted surveys were presented.

Christoph Graf spoke about the evaluation of objectives for the second year of the GN2 project. The group would focus more on identifying missing tools, developing them, as well as on providing services and training. He summarised the achievements which could not happen or would have to happen much later without the GN2 project.

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

Andrew Cormack asked if the JRA2 deliverables were available on-line. Christoph Graf said that they were not publicly available yet, but might become later, after the project review and approvals. He promised to inform the group when the JRA2 deliverables are publicly available. Karel Vietsch reported that all public GN2 deliverables will be published at www.geant2.net/server/show/nav.00d00b002001

ACTION 16.04: Christoph Graf – to inform the TF-CSIRT group when the GN2 JRA2 deliverables are publicly available.

10. Update on VEDEF WG

Oliver Göbel gave an overview of the VEDEF working group. The WG would aim to create "the best breed" from candidates, e.g. EISPP/CMSI, CAIF, VulDEF, etc. He recalled the background of this working group and spoke about the relationship to other initiatives. The road map, current activities and plans of the WG were presented. The BoF at the FIRST Conference did not take place, but other meetings have been organised, e.g.a meeting in Stuttgart on CAIF. The new website (www.secdef.org) would be on-line soon and would provide information on security related DEF activities.

11. CSIRT mentoring scheme

Andrew Cormack spoke about the CSIRT mentoring scheme. It has been discussed, approved and put on-line. He emphasised that the whole CERT community would benefit from having more CERTs established. He also reminded the group about valuable help many CERTs had already received from their more experienced colleagues.

Andrew Cormack was disappointed about the low number of responses to the request to act as a mentoring team. Due to this reason the CSIRT mentoring scheme has not been announced yet. He encouraged more teams to consider volunteering to be a mentor team. All information on how to participate was available on-line.

Damir Rajnovic asked how many requests have been received to get mentorship. Andrew Cormack replied that so far there was none, because the scheme has not been advertised. It was agreed to advertise the scheme in the tf-csirt mailing list and then see how many requests will be received. The next step would be to advertise it in the TRANSITS training course lists.

ACTION 16-05: Andrew Cormack - to advertise the CSIRT mentoring scheme in the tf-csirt mailing list.

12. Result of yesterday's seminar sessions, ideas for future sessions, including schedule for the next TF-CSIRT event together with the FIRST TC

Baiba Kaškina presented the proposed schedule for the next TF-CSIRT event in Amsterdam, which will be organised together with the FIRST TC. The event will start on Monday (23 January2006) with the TF-CSIRT meeting and meeting of the TI accredited teams. It was decided that the TI meeting will be in the morning, followed by the TF-CSIRT meeting and then by the TI Review Board meeting.

On Tuesday (24 January 2006) a whole-day seminar will be organised together by TF-CSIRT and FIRST. On Wednesday (25 January 2006) the FIRST hands-on classes will take place as well as other meetings (e.g. RTIR WG, e-coat, GN2 JRA2 meetings). Two meeting rooms have been reserved for the TF-CSIRT needs. Damir Rajnovic said that more meeting rooms can be allocated if necessary.

Gorazd Božič was worried to have other meetings in parallel with the FIRST hands-on classes. A solution could be to hold other meetings in the evening. Christoph Graf said that there will not be a GN2/JRA2 meeting, because they will hold a workshop earlier. Baiba Kaškina will check with e-coat people if they are going to organise a workshop in Amsterdam.

ACTION 16-06: Baiba Kaškina – to ask Don Stikvoort if the e-coat forum would organise a workshop in Amsterdam in January 2006.

13. Status of the ToR and other TF-CSIRT work items / deliverables; appointing the deputy chair

Gorazd Božič nominated Kauto Huopio from CERT-FI as the deputy chair. Kauto Huopio was not present in the meeting, but he had agreed to fill this position. The participants unanimously approved the proposal.

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.

14. Date of the next meetings

The next meeting will be held on 23-25 January 2006 in Amsterdam, the Netherlands (hosted by Cisco) together with the FIRST TC.

The subsequent TF-CSIRT meetings will be hosted by LITNET CERT in Vilnius, Lithuania on 25-26 May 2006 and by FUNET CERT and CERT-FI in Helsinki or Espoo, Finland on 21-22 September 2006.

15. Any Other Business

Gorazd Božič and the group expressed their thanks to FCCN for organising the meeting.

Andrew Cormack encouraged participants to submit security related papers for the next TERENA Networking Conference TNC2006 which will take place in Catania, Italy on 15-18 May 2006. He gave a short overview about the usual TNC format and content. The Call for Papers will be issued in autumn 2006; only extended abstracts will be needed for submission.

List of meeting participants

	Name	*Organisation*	*Country*
1.	Antti Alinen	Ericsson	Sweden
2.	Claudio Allocchio	GARR-CERT	Italy
3.	Preben Andersen	DK-CERT	Denmark
4.	Gilles André	CERTA	France
5.	Jimmy Arvidsson	TeliaSoneraCERT CC	Sweden
6.	Dmitry Avramenko	RU-CERT	Russia
7.	Raymond Azzopardi	mtCERT	Malta
8.	Dan Bailey	NISCC	United Kingdom
9.	Wim Biemolt	SURFnet	Netherlands
10.	Gorazd Božič (Chair)	SI-CERT	Slovenia
11.	Andreas Bunten	DFN-CERT	Germany
12.	Roberto Cecchini	GARR-CERT	Italy
13.	Andrew Cormack	UKERNA	United Kingdom
14.	David Crochemore	CERTA	France
15.	Michelle Danho	RENATER CERT	France
16.	Lionel Ferette	BELNET	Belgium
17.	Mikhail Ganev	RU-CERT	Russia
18.	Christoph Graf	SWITCH-CERT	Switzerland
19.	Oliver Göbel	RUS-CERT	Germany
20.	Uldis Grunde	State Information Network Agency	Latvia
21.	Peter Haag	SWITCH-CERT	Switzerland

22.	Lars Hedensjö	SITIC	Sweden
23.	Jeroen Hoppenbrouwers	SURFnet-CERT	Netherlands
24.	Przemek Jaroszewski	CERT Polska / NASK	Poland
25.	Rick Jones	BT-SBS	United Kingdom
26.	Sigitas Jurkevicius	Communications Regulatory Authority	Lithuania
27.	Yurie Ito	JP-CERT	Japan
28.	Urpo Kaila	Funet CERT	Finland
29.	Baiba Kaškina (Secretary)	TERENA	-
30.	Ulrich Kiermayr	ACOnet-IRT	Austria
31.	Andrea Kropacova	CESNET z.s.p.o.	Czech Republic
32.	Ladislav Lhotka	CESNET	Czech Republic
33.	Sergey Linde	RU-CERT	Russia
34.	Antonio Liu	PRESECURE	Germany
35.	Mika Müller	Ericsson	Sweden
36.	Stelios Maistros	GRNET-CERT	Greece
37.	Chelo Malagón	IRIS-CERT, RedIRIS	Spain
38.	Jan Meijer	SURFnet / CERT-NL	The Netherlands
39.	John Millar	BT CERT	United Kingdom
40.	Maciej Milostan	PIONIER-CERT / PSNC	Poland
41.	Milda Mimiene	LITNET CERT	Lithuania
42.	Martin Mogensen	DANTE	United Kingdom
43.	Maurizio Molina	DANTE	United Kingdom
44.	Barbara Monticini	GARR-CERT	Italy
45.	Claudia Natanson	Diageo	United Kingdom
46.	Gustavo Neves	CERT.PT	Portugal
47.	Teun Nijssen	SURFnet-CERT	Netherlands
48.	Jiri Novotny	CESNET	Czech Republic
49.	Tomasz Nowocien	PIONIER-CERT	Poland
50.	Niclas Olsson	TeliaSoneraCERT CC	Sweden
51.	Carol Overes	GOVCERT.NL	the Netherlands
52.	Daven Patel	Diageo	United Kingdom
53.	Leila Pohjolainen	Funet CERT	Finland
54.	Jason Rafail	CERT/CC, SEI, Carnegie Mellon University	USA
55.	Damir Rajnovic	Cisco Systems	United Kingdom
56.	Robin Ruefle	CERT Program, SEI, Carnegie Mellon University	USA
57.	Jacques Schuurman	SURFnet / CERT-NL	The Netherlands
58.	Erika Stockinger	SITIC	Sweden
59.	Ferenc Suba	Ministry of Informatics and Communication	Hungary
60.	Balazs Szekeres	CERT-Hungary	Hungary
61.	Alexander Talos	ACOnet CERT	Austria
62.	Marco Thorbrügge	DFN-CERT	Germany
63.	Peteris Treijs	VAS VITA	Latvia
64.	Maris Urkis	LITNET CERT	Lithuania
65.	Juan Vazquez	EsCERT-UPC	Spain
66.	Karel Vietsch	TERENA	-
67.	Torbjörn Wictorin	SUNet CERT	Sweden
68.	Wilfried Wöber	ACOnet-IRT	Austria
69.	Martin Zadnik	CESNET	Czech Republic

Apologies were received from:

Ian Bryant	NISCC	United Kingdom
Martin Camilleri	mtCERT	Malta
Ralf Dörrie	Telekom-CERT	Germany
Per Arne Enstad	UNINETT CERT	Norway
David Freeman	ITsafe	United Kingdom
Natasa Glavor	CARNet CERT	Croatia
Mirosław Maj	CERT Polska / NASK	Poland
Janos Mohacsi	NIIF/HUNGARNET	Hungary
David Parker	UNIRAS/NISCC	United Kingdom

Peter Quick	Deutsche telekom AG, T-Com	Germany
Sharon Sciberras	mtCERT	Malta

RESULTING ACTION ITEMS

16-01	Gorazd Božič	Inform APCERT that Jacques Schuurman from SURFnet-CERT has been appointed as the liaison from the TF-CSIRT side.
16-02	Gorazd Božič	Ask in the mailing list for volunteers to review the CERT CSIRT Development Team documents and to inform Robin Ruefle about the results.
16-03	Gorazd Božič	Investigate the possibilities for communication channel among the initiatives before the next TF-CSIRT meeting.
16-04	Christoph Graf	Inform the TF-CSIRT group when the GN2 JRA2 deliverables are publicly available.
16-05	Andrew Cormack	Advertise the CSIRT mentoring scheme in the tf-csirt mailing list.
16-06	Baiba Kaškina	Ask Don Stikvoort if the e-coat forum would organise a workshop in Amsterdam in January 2006.
15-01	Don Stikvoort	Give a presentation about the issues e-coat is working on in one of the following TF-CSIRT seminars.