

**Minutes of the 17th TF-CSIRT meeting
Amsterdam, 23 January 2006**

[Please note that a seminar was held the next day. Presentations from the seminar and the meeting can be found at <http://www.terena.nl/activities/tf-csirt/meeting17/>]

1. Welcome and apologies

Gorazd Božič welcomed the participants of the first joint TF-CSIRT and FIRST event. The list of those present is available on-line: <http://www.terena.nl/activities/tf-csirt/meeting17/registrations.php>

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

The minutes of the last meeting held on 16 September 2005 were approved.

Action items:

16-01 Gorazd Božič – to inform APCERT that Jacques Schuurman from SURFnet-CERT has been appointed as the liaison from the TF-CSIRT side.

Done.

16-02 Gorazd Božič – to ask on the mailing list for volunteers to review the CERT-CC CSIRT Development Team documents and to inform Robin Ruefle about the results.

Superseded. Gorazd Božič asked whether it would be better to form a committee or to find volunteers on case by case basis for reviewing CERT-CC documents. It was agreed to look for volunteers on case by case basis. Klaus-Peter Kossakowski agreed to be a point of contact for reviewing requests.

16-03 Gorazd Božič – to investigate the possibilities for communication channel among the initiatives before the next TF-CSIRT meeting.

Done. It was agreed to subscribe liaisons from other initiatives to the TF-CSIRT mailing list. If a need arise a separate mailing list could be created.

16-04 Christoph Graf – to inform the TF-CSIRT group when the GN2 JRA2 deliverables are publicly available.

Ongoing.

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

Done.

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

Done. The e-coat forum workshop was held on 12 January 2006 in Amsterdam, the Netherlands.

15-01 Don Stikvoort – to give a presentation about the issues e-coat is working on in one of the following TF-CSIRT seminars.

Done. See agenda item 5.

3. Compulsory Data Retention: Issues for CSIRTs

Andrew Cormack spoke about the Compulsory Data Retention and issues for CSIRTs. He gave an overview on the Data Retention directive and institutions that were in favour or against it. He emphasised that the directive should ensure the same obligations for ISPs in the whole European Union.

The potential directive would concern traffic data, e.g. user real-world identities and addresses, login times and DHCP logs, source and destination information of packets, but not the content of packets. The data collection would be compulsory for specified types of network, for data about specific services and regardless if data would be needed for the ISP itself or not. The compulsory data retention

period would be 6 months to 2 years depending on the country. ISPs should also log and report access requests. These regulations would apply to public networks, but not to the private ones. Most of the NRENs could claim their networks to be private.

Andrew Cormack explained which data should be retained for which services and emphasised definition problems. Legislation containing so specific technical details would get outdated very soon.

The directive (when accepted) should be transposed into national laws. That would give a lot of flexibility and ambiguity for the individual governments to improve the market situation for ISPs in their country. Andrew Cormack predicted a lot of uncertainty in the short term and significant differences in the long term.

It was not clear who could have access to the data – only anti-terrorism units or any police department. CSIRTs would be affected by this directive indirectly to a great extent. There would be more log files available, but CSIRTs might not have access to them. Log files might get accessed also by hackers and others parties which can increase the workload of CSIRTs. In any case, implementation of this directive would reduce privacy in Internet.

Suggested actions for CSIRTs would be to clarify if their organisation would get affected by this law, to advise on secure and safe ways to store and access data, to ensure that requests for disclosure are verified. It would be advisable to work together with legislators to produce practical and effective law and to work together with enforcers to ensure they would not make a network that CSIRTs would not be able to use.

It was asked whether the rejected spam messages would have to be logged as well. Andrew Cormack said that indeed they should be logged. He gave as an example that even unanswered phone calls have to be logged.

Wilfried Wöber asked about the encrypted packets. Andrew Cormack agreed that this issue was not clarified. Also conflicts with human rights and data privacy issues were not solved. The group discussed the proposed directive. Andrew Cormack thought that it will be passed soon. Gorazd Božič summarised that the discussion should be continued in the next meeting.

4. ENISA update

Marco Thorbrügge gave an update about ENISA. He has been appointed as senior expert in CERTs in ENISA. He explained the structure of ENISA and its tasks. The ENISA office has been moved to Heraklion in September 2005. In the second half of 2005, ENISA started establishing contacts with relevant stakeholders, designing the work programme 2006 and participating in many conferences and events.

According to the work programme 2005, in the CERT area a CERT Cooperation and Support working group (WG) was created, an inventory of CERTs in Europe was produced and a CERTs workshop organised. CERT WG consisted of 9 experts from 8 countries and they met two times in 2005. The WG terms of reference consisted of many tasks, but not all of them were completed.

The Inventory of CERTs was the most visible outcome in 2005. The map of CERTs had even become very popular in Greek newspapers. Marco Thorbrügge asked everyone to review the inventory and provide him with comments.

The CERTs workshop was organised in December 2005 in Brussels. Government representatives from all member states participated in the workshop. TRANSITs training courses, Trusted Introducer, TF-CSIRT, e-coat, WARPs, legal handbook, CSIRTs and other issues were presented.

The work programme 2006 would focus on setting up CERTs, facilitating staff and management training, promoting the CERT concept and handling requests from member states. The work programme 2006 will be discussed by the management board of ENISA in March 2006. Marco Thorbrügge would prepare the work programme 2007. It would focus on issues related to “running a CERT”, including advanced training, audits, certification.

Gorazd Božič asked to clarify what kind of requests ENISA would work with. Marco Thorbrügge gave as an example that he had received a request to help setting up a Lithuanian governmental CERT. In the framework of that request, ENISA would sponsor the next TRANISTS training course in Vilnius, Lithuania in March 2006. Other requests might be European Commission requests for input and review of papers, requests to carry out studies, e.g. a study about European Early Warning systems, to audit European data protection agency, etc. Stelios Maistros asked whether ENISA would involve local CERTs in processing requests. Marco Thorbrügge said that it would depend on the request and he would certainly involve local CERTs if that could be useful.

Andrew Cormack spoke about the ENISA Permanent Stakeholders Group (PSG). The PSG meets three times per year with the ENISA director and staff. The purpose of these meetings is to maintain dialogue with external stakeholders and to advise ENISA on outputs useful to the stakeholders. The last PSG meeting was held in December 2005 in Heraklion, Greece. It provided initial input to the work programme 2007 and discussed technical issues and future challenges.

Bernd Grobauer asked whether ENISA was involved in the development of the 7th Framework Programme of the EU. Marco Thorbrügge replied that they had not received requests for input from the EC so far. Gorazd Božič thought that ENISA would be involved in that in future.

5. e-coat update

Don Stikvoort gave an update on the European co-operation of abuse fighting teams (e-coat) activities.

He pointed out problems with blacklists and whitelists as well as the huge scale of abuse in general. It might be very easy to get onto blacklists, but sometimes it was very hard to find the responsible person to get out of the blacklist. As other problems he mentioned the increase of phishing and botnets.

There were several organisations fighting different types of incidents and abuse, i.e. TF-CSIRT and FIRST focused on classical CERT issues, ETNO and FIINA focused on higher level issues, MAAWG focused on messaging. E-coat activity was created to discuss pragmatic abuse handling issues. E-coat consisted mainly of ISPs' abuse teams and had some overlap with TF-CSIRT participants. The 5th e-coat workshop was held on 12 January 2006 in Amsterdam.

E-coat goals were discussion of shared problems, sharing of solutions, establishing best practices and common standards. E-coat participants were interested in fighting massive abuse together, having direct NOC-to-NOC contacts, working on whitelists and blacklists, and dealing with other issues initiated by members. Several projects have been started to achieve the goals, to develop tools and to raise awareness by collaborating with ENISA and other bodies. An IRT server has been installed and used by the participants for on-line discussions.

Don Stikvoort described the working mechanisms of the forum and announced that the next e-coat workshop will be organised on 20 September 2006 in Helsinki, Finland, before the TF-CSIRT event. E-coat participants would be interested to create a FIRST SIG; the discussions with representatives from the Asia-Pacific region have started already. He hoped to have a BoF about creating the SIG during the next FIRST conference in Baltimore. It was not mandatory to be a FIRST member to participate in a SIG.

6. Update on EC funded projects: GN2/JRA2 update

Jacques Schuurman gave an update on the GN2/JRA2 activities. He summarised the GN2 project and all the JRA2 work items. A general JRAs meeting was held in Cambridge in January 2006, the JRA2 evaluation there was reasonably good.

Jacques Schuurman 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. Jacques Schuurman discussed the risks that GEANT2 community was facing including insecure partners.

As success factors for increasing overall GEANT2 security, Jacques Schuurman mentioned management commitment to invest in security, separating applied research and operations, as well as involving the affected less-developed partners and raising the community spirit.

7. CSIRT training courses

Karel Vietsch spoke about the CSIRT training courses. He gave details about the TRANSITS project and 7 training courses which have been held during the lifetime of the project, including number of participants, represented countries, sectors, etc. The course material consisted of five modules. The TRANSITS project ended in September 2005.

Karel Vietsch spoke about the Memorandum of Understanding between TERENA and FIRST, stating that FIRST would continue organising training workshops in the Latin American 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.

The technical module of the courses was updated by SWITCH people in December 2005. Karel Vietsch emphasised that volunteers would be needed to update other TRANSITS modules.

The first joint TERENA-FIRST "post TRANSITS" TRANSITS workshop was held in Vienna, Austria on 21-22 November 2005 and was sponsored by ISPA. In total in all the training courses there have been 181 trainees from 33 countries.

The next joint TERENA-FIRST CSIRT training course will take place in Vilnius, Lithuania on 29-30 March 2006 and will be sponsored by ENISA. The application deadline for the courses will be 14 February 2006.

Regarding the future plans Karel Vietsch said that TERENA would organise at least one more workshop in year 2006. The MoU with FIRST would be reviewed in the autumn of 2006. He raised concerns about collaboration with FIRST. Gorazd Božič hoped that these issues would be discussed and resolved in a meeting between TERENA and FIRST representatives.

Yuri Demchenko asked if the TRANSITS courses have been translated into other languages, e.g. Spanish, Russian, and Chinese. The course materials have been translated into Spanish and partly into Chinese. Some materials have been translated into Russian as well. Yuri Demchenko said that NATO could support full translation into Russian. Karel Vietsch emphasised the importance of the central repository of the materials kept by Don Stikvoort and better communication among involved parties. All the translations should be submitted to the repository. Klaus-Peter Kossakowski asked about the copyright issues of the translations. Karel Vietsch explained that TERENA copy rights holds also for the translated materials, i.e. they are available for non-commercial usage.

8. IRT object

Wilfried Wöber presented some background about the IRT objects in the RIPE database and gave an update about the latest developments. He explained the idea behind the IRT object and the way it was implemented in the RIPE database.

Since the last update several things have been implemented. General queries were returning less email addresses, references to X.509 objects were supported, and IRT object information was included in the simple whois queries. Also security provisions protecting the database have been improved; the crypt-pw authentication mechanism will be phased out. For authentication crypt-md5, PGP and X.509 mechanisms will be available.

Wilfried Wöber asked the participants how many of them were aware of the IRT objects and had their constituencies linked. The show of hands proved that there was room for improvement.

It was asked whether the data retrieving from the RIPE database could be automated. Wilfried Wöber replied that it was technically possible, but he asked to warn the RIPE NCC about such plans in advance. It was possible to mirror the RIPE database; the hosting organisation would only have to sign

an AUP with the RIPE NCC. Mirror sites were updated from the main server with a few minutes' delay.

Wilfried Wöber wanted to know if any follow-up was needed for the community, for example, training. There was no support for his idea.

Teun Nijssen asked about implementation of IRT objects in other world regions. Wilfried Wöber explained that there was something similar already implemented in the ARIN region. He could start again discussions with APNIC region people by presenting the subject in the annual APNIC conference. Gorazd Božič suggested him to discuss that with Yurie Ito. Also the liaison person could help with arranging a slot in the conference.

ACTION 17.01: Wilfried Wöber – to ask Yuri Ito about possibilities to present the IRT object in the next APNIC conference.

9. Update on RTIR working group

Carlos Fuentes 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. The contract was signed on 6 September 2005 and project started on 6 October 2005. The first milestone will be delivered on 6 April 2006. Carlos Fuentes pointed out that 51% of the requirements for the 1st milestone were done already, so he thought that everything would be delivered in time.

A RTIR WG meeting would be held on the evening after the TF-CSIRT meeting. Carlos Fuentes mentioned that the testing scenario and environment for the 1st milestone would be discussed there.

RTIR was presented at the 5th e-coat workshop. WG participants hoped to get more teams to use RTIR. The image of RTIR was available for download from the RedIRIS FTP server. Carlos Fuentes also mentioned a wiki for the WG for exchanging information.

10. Update from the TTC

Andrew Cormack informed the group that he has been appointed as member of the TERENA Technical Committee (TTC), taking care of the security area. As the member of the TTC he was more aware about other TERENA initiatives, for example about the “NRENs and Grids” workshop. He would try to inform TF-CSIRT people interested in Grids about the activities of that initiative. He asked the group to inform him in case they have any suggestions or proposals for the TTC.

11. Status of the ToR and other TF-CSIRT work items / deliverables

Gorazd Božič summarised that the progress of the work items and deliverables had been discussed during the meeting and there was no need to review the Terms of Reference. The current TF-CSIRT ToR mandate will end in September 2006, so in the next meeting the group should review all the work items and deliverables.

ACTION 17.02: Gorazd Božič – to initiate discussion about the work items and deliverables of the task force before the next meeting.

12. Date of the next meetings

The next meeting will be held on 25-26 May 2006 in Vilnius, Lithuania (hosted by LITNET CERT).

The subsequent TF-CSIRT meeting will be hosted by FUNET CERT and CERT-FI in Espoo, Finland on 21-22 September 2006.

13. Any Other Business

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

Baiba Kaškina announced that she will be leaving TERENA and thanked all the participants of the task force.

RESULTING ACTION ITEMS

17-01	Wilfried Wöber	Ask Yuri Ito about possibilities to present the IRT object in the next APNIC conference.
17-02	Gorazd Božič	Initiate discussion about the work items and deliverables of the task force before the next meeting.
16-04	Christoph Graf	Inform the TF-CSIRT group when the GN2 JRA2 deliverables are publicly available.