

**Minutes of the 10th TF-CSIRT meeting
Amsterdam, 26 September 2003**

[Please note that a seminar was held the previous day. Presentations can be found at <http://www.terena.nl/tech/task-forces/tf-csirt/meeting10/programme.html>]

1. Welcome and apologies

Gorazd Bozic welcomed the participants. The list of those present is below at the end of these minutes.

Apologies had been received from Suleyman Anil (NATO (NCIRC CC)), Ralf Dörrie (Telekom-CERT), Chelo Malagón (IRIS-CERT/RedIRIS), Vlado Pribolsan (CARNet CERT), Damir Rajnovic (Cisco Systems), Krzysztof Silicki (CERT Polska / NASK), and Han van Thoor (nl.tree / KCSIRT).

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

The minutes from the last meeting held on 30 May 2003 were approved.

Action items:

07-03 Wilfried Wöber/Ulrich Kiermayr - to produce the documentation on how to use the IRT object in the RIPE database.

Ongoing; see agenda item 9.

07-07 All - to send to Baiba Kaskina the URLs of the projects that are relevant to CSIRTs, to be listed on the TF-CSIRT webpages.

Done.

07-11 Don Stikvoort and BCP WG - to finalise his document on the BCP in CSIRTs.

Ongoing; Don Stikvoort promised to finalise the document by 15 October 2003.

08-03 Andy Bone - to discuss with John Green his responsibility for the work item C.

Done; Jan Meijer is a deputy at IETF Inch WG Liason (IODEF).

09-01. Jan Meijer - to create a questionnaire regarding the Incident Handling System requirements and send it to the mailing list.

Ongoing; Jan Meijer promised to send the questionnaire by 15 October 2003.

09-02. Wilfried Wöber - to organise a meeting on the issue of documentation and a users' guide for the use of the IRT object in the RIPE database.

Done; the meeting was held on 29 August 2003 in Amsterdam; see agenda item 9.

09-03. Klaus-Peter Kossakowski - to create a link from the TI website to the RIPE IRT objects.

Done; see agenda item 3.1.

09-04. TI - to put a discussion about certification issues on the agenda of the next meeting of the accredited teams.

Done.

09-05. Gorazd Bozic - to devise draft rules for admission to the TF-CSIRT mailing list and meetings.

Done; see agenda item 15.

09-06. Jacques Schuurman - to write a formal and final report on the work of TF-RI and present that to the Steering Committee.

Done. Jacques Schuurman reported that there was no reaction to the report and no resulting activities. If the TF-CSIRT wants some actions, it has to initiate them.

09-07. Karel Vietsch- to summarise all the proposals from the TF-C SIRT community about the NISA and send a letter to the EC, Mr.Santucci before mid-July.

Done; see agenda item 7.

09-08. Baiba Kaskina - to send a test message to the TF-CSIRT mailing list and a reminder of subscription to the cert-coord mailing list.

Done.

09-09. Baiba Kaskina - to send a reminder to the mailing list to visit the archive of the links.

Done.

09-10. Gorazd Bozic and Baiba Kaskina - to devise a questionnaire regarding the opinion of participants about seminars.

Done.

09-11. Andrew Cormack and Przemek Jaroszewski - to initiate a discussion regarding ideas how to involve more teams.

Ongoing; Andrew Cormack presented the slide show about the TF-CSIRT (see agenda item 12.), but Gorazd Bozic proposed keeping the action item and Przemek Jaroszewski promised to initiate the discussion.

3. Trusted Introducer Service

3.1. Status Report and feedback from the meeting of accredited CSIRTs

Don Stikvoort gave the TI status report and feedback from the meeting of accredited CSIRTs that was held on the previous day. He emphasized 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. A “health warning” recently had been added to the listed teams. It has been decided in the meeting of accredited CSIRTs to form a group which would define “code of ethics / conduct” for the accredited teams and devise future steps towards certification.

Don Stikvoort spoke about the TI organization, mentioning the maintenance fee for accredited teams of 720 EUR per year, TERENA’s role as a clearing-house and contracting party and the current contractor S-CURE of the Netherlands. The TI has a TI review board which is chosen by the accredited teams and oversees the TI operations and takes decisions in special cases. He reported that it was decided to organise meetings of the accredited teams more than once, and perhaps up to three times, per year, with a possibility to call special meetings. He also presented charts with the number of CSIRTs in the TI repository and accredited CSIRTs.

A number of services were provided for accredited CSIRTs, including a restricted website, four-monthly active maintenance, an up-to-date PGP key ring and formal signing of keys, the contact information in CSV format, trusted mailing lists for information exchange and discussion, CSV files with contact data for PDA’s and laptops, and the automatic registration and maintenance of IRT objects in the RIPE database. He mentioned the new services and information which would be added to the website, i.e. IRT-object related info and query tool, PR-info, IRT-object links, Globalsign server certificate, using a unique domain name for the TI. It was also planned to refine the ti-accr-sharing use policy and to define new services for abuse teams as well as services built on the eCSIRT.net infrastructure.

Don Stikvoort introduced the TI team members present and thanked for the trust of the community.

3.2. Report from the TI Review Board

Karel Vietsch reported on the meeting of the TI Review Board that was held on the previous day. He mentioned that TI review board is based on the contract between TERENA and S-CURE. He listed the tasks of the TI Review board, i.e. to receive 4 monthly reports by the TI, to review the overall performance of the TI and handle complaints about the TI, to sign PGP keys of the TI, to set and if necessary change operational framework for the TI, to decide about the special issues regarding

CSIRTs with “accredited” and “accredited candidate” status, including making exceptions to the TI standard procedure. He emphasized that more generally it was the role of the Board to be a sounding board for the TI team and a body providing advice and assistance.

Marco Thorbrügge had been elected as a member of the TI review board, replacing Andrew Cormack. The current composition of the TI review board is: Jacques Schuurman, Jimmy Arvidsson, Marco Thorbrügge, Gorazd Bozic, and Karel Vietsch. Jacques Schuurman is the elected chairman for the period from September 2003 until September 2004.

The TI Review Board took the decision to delete from the list of listed CSIRTs 5 CSIRTs that did not respond to the attempts to re-establish contacts. They also discussed the last TI status report and ideas for the future development of the TI service.

The TI Review Board reviewed the meeting of accredited CSIRTs and were positive about it because of the adequate preparations. Karel Vietsch thanked the TI team.

4. Update on the EC funded projects

4.1. eCSIRT.net

Klaus-Peter Kossakowski reported on the eCSIRT.net project, which aims to develop a standardised way for exchanging incident-related information. His presentation addressed statistics and the alert function.

He explained the rules and terms of participation, e.g. it was restricted to teams that are either partners or liaisons of the eCSIRT.net project, which included TI accredited teams and any other team admitted by decision of the project partners. The participants should sign the code-of-conduct and related policies, which are accessible on the public website.

Klaus-Peter Kossakowski presented three forms of statistics, i.e. CSIRT workload, information on incidents, and events on the Internet. Information on CSIRTs' workload could be obtained from the participating teams via a web form or from the tracking data.

The second form of statistics was information on incidents handled by CERTs. The participating teams should submit monthly information about closed incidents, based on the IODEF classification scheme. Klaus-Peter Kossakowski presented statistical results on various types of data, i.e. all reports vs. opened incidents, closed incidents and spent time, closed incidents vs. opened incidents, types of incidents.

Information on events on the Internet should not necessarily be handled by CERTs and it should not necessarily reflect the information on successful intrusions. These forms of statistics were collected from special sensors, which were located on not otherwise usable systems reachable over the Internet and equipped with particular software. These sensors were accessible via https and user certificates. Klaus-Peter Kossakowski told the group that they had installed 6 sensors during a two-week period and they worked fine. He presented the first statistics obtained from these sensors. The installation of sensors would continue.

He emphasized the importance of the authenticity and confidentiality of reporting for all the forms of statistics. The participating teams had access to aggregated data and a subset of aggregated data should be publicly available as statistics.

In the second part of his presentation Klaus-Peter Kossakowski spoke about the alert function. To perform this function a cryptographic secure mailing list had been created. This list supported S/MIME and PGP and was based on a commercial SMTP proxy. The mailing list used the secret key for receiving emails and public keys of subscribers for sending emails. The alert function should be used whenever there is a legitimate interest of the participating CSIRTs and if the impact can be foreseen and represents a widespread threat. The alerts could be sent in two formats, i.e. ASCII or IODEF (in XML). The IODEF format could be more convenient to interact with the existing systems. Klaus-Peter Kossakowski presented alert input forms and examples of ASCII and IODEF format alerts.

If email is not available for alerting, then the telephone system should be used instead. In the future the support of SMS and automatic fax distribution to allow transfer of large documents would be implemented. The eCSIRT.net team would like to involve teams from the other regions as well to receive early warnings during out-of-hours in Europe and live reports from the other time zones.

Gilles André asked Klaus-Peter Kossakowski about the future of the project and whether the produced software would be accessible on-line and the status of the data collection. Klaus-Peter Kossakowski replied that all the software should be accessible on-line and also the data available after the end of the project. Regarding the data collection he said that data are not normalised and it is difficult to gather them, so this issue is still in process.

The follow-up of the project was still uncertain and Gorazd Bozic proposed that the teams who participate in the eCSIRT.net project put down their future visions. The document about the eCSIRT.net future should be sent to the TF-CSIRT mailing list and discussed in the next TF-CSIRT meeting, in Madrid.

ACTION 10-01: Klaus-Peter Kossakowski - to devise a proposal for the eCSIRT.net project follow-up, send it to the TF-CSIRT mailing list and lead the discussion about it in the next TF-CSIRT meeting.

4.2. EISPP

Philippe Bourgeois gave a short report on the EISPP project. This started in June 2002 with the aim of establishing a European CSIRT network of expertise, and setting up the framework to provide SMEs with adequate security services. The project ends in January 2004. He spoke about two issues: CERT cooperation on security advisories, and providing security advisories and related services for SMEs.

Philippe Bourgeois reported that the document resulting from the Warsaw CERT workshop was available on-line on the EISPP web site. There were three areas where the EISPP team was working, i.e. common advisory format, cooperation, CEISNE.

The common advisory format was ready and being used by EISPP CERTs for advisory production. The new version of the advisory format was under development and improvements would be based on the feedback they had collected. The EISPP project team would like to encourage cooperation to obtain workload sharing and better accuracy.

In terms of cooperation the project was preparing the environment for CEISNE – Co-operative European Information Security Network of Expertise. CEISNE would be an informal co-operation based on a code of conduct. It would elaborate on creating a central site for sharing advisory data. That network of expertise would be the continuation of the EISPP project. CEISNE requirements were under discussion, but requirements could range from a “discussion forum” dedicated to security advisories to a central repository for sharing advisories.

Philippe Bourgeois spoke about services for SMEs. Security advisories dissemination activities have reached over 350 SMEs, including 23 direct subscribers and over 300 indirect subscribers through CoC and ISP. In the framework of the value added services 5 pilots were running, i.e. vulnerability scanners, firewalls, remote update systems, IDS, antivirus. Currently EISPP was collecting feedback from the users. As the future plans Philippe Bourgeois mentioned SME workshops which will take place in France, Italy, Spain and Sweden during October and November 2003. He also proposed participants to join CEISNE.

Ian Bryant said that he knew at least 5 different initiatives about common advisory formats and asked Philippe Bourgeois whether there is any collaboration among them. Philippe replied that he is aware of 3 formats, but there is no collaboration among the different initiatives. Ian Bryant suggested having an Internet draft for that.

4.3. TRANSITS

Karel Vietsch gave an overview of the TRANSITS project. This project, whose formal partners are TERENA and UKERNA, runs from July 2002 until June 2005.

The project is contracted to produce the training course materials (initially by mid-2002, with a revision by early-2004) and to run six training workshops (in spring and autumn each year). There is also some budget to partly cover the expenses of participants from the “poorer” European countries. Karel Vietsch (TERENA) is the project manager; Andrew Cormack (UKERNA) is responsible for the course materials and the workshop programmes, whilst Carol de Groot and Dick Visser (TERENA) are handling the workshop logistics.

The training course material was completed in September 2002. It remains the copyright of TERENA, but it may be used for non-commercial training courses, provided permission is sought and both TF-CSIRT and the European Commission’s IST programme are credited.

Two workshops have been held so far; Karel Vietsch gave some statistics about the trainees. There were 41 trainees from 23 different countries, 26 came from the existing CSIRTs and 15 from the organisations planning to set up a CSIRT.

The next training workshop will be held on 30-31 October 2003 at San Gaudenzio, Northern Italy. 22 applications were received and Karel Vietsch thought it would be possible to accept all of them. The lecturers in this workshop would be Andrew Cormack, Klaus Möller, David Parker, Jacques Schuurman and Don Stikvoort.

As the next milestones he mentioned revision of the materials in early 2004 and the 4th TRANSITS workshop in May 2004 near Hamburg, Germany.

5. Update on FIRST

David Crochemore gave an update on the latest activities in FIRST. The FIRST conference 2003 took place in Ottawa; the next conference will be held in Budapest in June 2004. In this year’s conference 80% of the tutorial speakers were from Northern America. In contrast, 35% of the paper speakers were from Europe. David Crochemore encouraged everyone to submit tutorials. The next chairman of the steering committee has been elected – Klaus-Peter Kossakowski. In the old steering committee there were 3 people (37.5%) from Europe, but in the new steering committee there are 4 people (50%) from Europe. David Crochemore presented the new composition of the committee and upcoming projects, i.e. web site restructuring, Microsoft and UNIX FIRST Responders toolkits, best practice guides.

Another issue presented and discussed in the framework of FIRST was the specific interest groups (SIGs). David Crochemore told the group about the definition of a SIG, the motion adopted by FIRST, support from FIRST to the SIGs and commitment from the SIGs to the FIRST membership. When a SIG is recognized by FIRST, it has committed itself to encourage its members to apply for FIRST membership and to present its work, projects and deliverables to the FIRST community during the conferences and / or TCs.

David Crochemore also spoke about the World Summit on Information Society (WSIS). It would be organized by the International Telecommunication Union (ITU) on behalf of the United Nations. The WSIS would have two conferences, in Geneva December 2003 and Tunis November 2005. The participants in the WSIS would be governments, private sector, and civil society. FIRST would probably also participate and could bring some message from TF-CSIRT as well.

Andrew Cormack encouraged everyone to look at the WSIS web site (www.wsis.org) which contains very comprehensive information. David Crochemore promised to send more information to the TF-CSIRT mailing list as soon as he would have it.

ACTION 10-02: David Crochemore - to send information about the World Summit on Information Society to the TF-CSIRT mailing list.

Dave Parker asked David Crochemore whether TF-CSIRT should consider becoming a FIRST recognized SIG. He agreed that the FIRST proposal was quite asymmetric. Gorazd Bozic proposed initiating a discussion on the TF-CSIRT mailing list about this issue and discussing it in detail in the next TF-CSIRT meeting. He also thought that a discussion on FIRST should always be on the agenda for the TF-CSIRT meetings.

ACTION 10-03: Gorazd Bozic - to initiate a discussion on the TF-CSIRT mailing list on TF-CSIRT becoming a registered SIG of FIRST.

Yurie Ito reminded the participants about the Technical Colloquium (TC) which would take place in Tokyo, Japan, in October 2003. It was still possible to register for the TC, but the participation was limited to FIRST members only.

6. APCERT Update: Regional Initiative within Asia Pacific

Yurie Ito from JPCERT/CC presented the regional initiative within the Asia Pacific region, the APCERT activities and possibilities for collaboration. 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 AP for incident handling. APCERT helps to contact victims and involved sites via point of contact (POC) CSIRTs. As languages and character sets are a very critical issue in the AP region, POC helps with translating the information about incidents.

To illustrate their model of collaboration Yurie Ito presented their activities during the Blaster worm attack, which started on 12 August 2003.

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. APCERT and APNIC share the same regional boundaries. There are 15 full members of APCERT.

Activities of APCERT included organizing the annual conference APSIRC and an annual general meeting together with the APRICOT conference and various working group (WG) activities, i.e. accreditation WG, training and communication WG, finance WG. Yurie Ito invited those present to participate in the next APSIRC conference which will take place in Kuala Lumpur, Malaysia, on 21 February 2004. Their WG activities were focused on the creation of a similar service as the TI. Yurie Ito was very positive about Don Stikvoort's presentation on the TI and hoped to adopt some of the TI concepts. Problem in the AP region would be the membership fee; therefore they would have to devise their own mechanism for participation and accreditation. Yurie Ito told the group that she liked the eCSIRT.net workshop that was held on Wednesday. She thought of starting to use their standard and thus make it international.

Jungu Kang from KISA/CERTCC-KR presented communication technologies within APCERT. He spoke about the APCERT encrypted mailing list principles and usage and secure web site.

Yurie Ito emphasized that the main issues in the AP region were not technical but more related to policy and procedures. Therefore they would like to collaborate with other regional initiatives including TF-CSIRT. They would be particularly interested in the TI and eCSIRT.net project outcomes. Time zone differences could also be beneficial for both organizations, it would allow to send early warnings and exchange information on time based attacks. APCERT is involved in the IODEF standard development, particularly in the issues related to special character sets.

Wilfried Wöber asked Yurie Ito whether APCERT would be the right organization to report about the incidents from the AP region countries. She replied that it is one of their main functions to act as a point of contact for incident information, to send it to the appropriate CERTs in a particular country and to help with translations if necessary. She promised to give TF-CSIRT members access to post information on their mailing list or to access the website.

Gorazd Bozic summarized that liaisons between TF-CSIRT and APCERT. Collaboration on time based attacks and sharing of traffic information for the eCSIRT.net project would be very valuable outcomes from this meeting. He hoped that liaisons would be established and everyone would gain from that.

7. Update on Inter-disciplinary working group for the European Network and Information Security Agency (ENISA)

Andrew Cormack reported on the latest activities regarding ENISA. He gave a short historic overview and details of the current Commission's proposal. He spoke about proposed objectives and tasks of the agency including gathering and analysing data on information security, establishing a centre of expertise for technical matters, contributing to cooperation in the field, providing support to the Member States, identifying relevant standardization needs, supporting contacts with countries outside the EU. Contributing to cooperation in the field and providing support tasks had very poor performance so far.

Andrew Cormack spoke about the Inter-Disciplinary working group (IDWG) which had been created to advise on the formation of ENISA. The working group consists of delegations from the Member States including governmental, academic and commercial sectors, participants from the accession states and the EEA. Andrew Cormack was an academic representative from the UK. Unfortunately only few people in the working group had CSIRT experience. This group had a meeting in July 2003. The participants in the meeting were almost unanimous in their view on the purpose of the agency, i.e. it would not be operational, not a CSIRT, it would identify and share best current practice in the Member States, help small business and end-users. Most of the first year's effort would be needed to get established. The IDWG planned two preparatory studies.

The next steps in this area would be a Ministerial Council Meeting in November 2003, an IDWG meeting in December 2003 and the creation of ENISA in early 2004. As activities in ENISA would be controlled by the Member States, Andrew Cormack encouraged people to talk to the representatives from their countries as soon as possible.

Karel Vietsch asked Andrew Cormack whether he has a list of IDWG representatives. Andrew replied that as soon as the mailing list would be created he would have the list of the email addresses. He was quite pessimistic about the fact that representatives are not experts in the security area, but rather people who are usual representatives of their country at the Commission.

Karel Vietsch reminded the participants about the visit of the TF-CSIRT delegation to Brussels in March 2003. He summarized the developments that happened after the visit. The latest of them was the reply from Mr. Gerald Santucci, which has been forwarded to the TF-CSIRT mailing list. The problem was that the TF-CSIRT talked to the Commission people who are responsible for research, not for the agency. A other problem for the TF-CSIRT community was the frequent rotation of the personnel in the Commission. Therefore it was very problematic to establish good relationships with appropriate officials. Ms Anne Bucher, who is the head of the unit responsible for ENISA was invited to participate in this TF-CSIRT meeting, but she did not reply.

Mr. Santucci proposed organizing another meeting with a TF-CSIRT delegation and promised to invite Ms. Bucher as well. Karel Vietsch asked the opinion of the group whether TF-CSIRT should have another meeting with the Commission. Andrew Cormack thought that a meeting should be organised because two IST projects are about to end and their future would be very uncertain. Dave Parker agreed that in case of a rejected invitation TF-CSIRT would risk to loose contact. Karel Vietsch also agreed and asked the participants what topics should be discussed in this meeting. eTEN activities and the Legal Handbook project were mentioned.

The following people volunteered to participate in a meeting with the Commission – Jacques Schuurman, Gilles André, Dave Parker, Andy Bone, Klaus-Peter Kossakowski, Andrew Cormack, and Wilfried Wöber, although eventually the date that would be fixed for the meeting could make some changes in this list. Karel Vietsch proposed postponing the meeting till November after the Council Meeting. He will contact Mr. Santucci and suggest having a meeting between a TF-CSIRT delegation and the Commission in November 2003.

ACTION 10-04: Karel Vietsch - to contact Mr. Santucci and suggest having a meeting between a TF-CSIRT delegation and the EC in November 2003.

The only activity until then could be contacting the countries' representatives.

8. Launch of the Legislative Handbook for CSIRTs

Andrew Cormack informed those present about the launch of Legislative Handbook for CSIRTs on 16 September 2003 in Brussels. He was representing the TF-CISRT community in that meeting and gave a short presentation about the history of CSIRTs and their needs.

RAND Corporation had been contracted for producing the handbook; it is available in paper format now. It contains information about the 15 Member States. Information about the accession states was not included. Andrew Cormack told the group that there was a draft version of the handbook available on-line in PDF format some time ago. The current paper version could be considered as the final draft and comments still could be submitted to Neil Robinson from RAND.

RAND would like to create a searchable on-line database, but they would need additional finances for that. Andrew Cormack felt that putting the database on-line, constant updating it and adding other countries should be the responsibility of ENISA. So far the future of the Legislative handbook was not clear.

Karel Vietsch asked Andrew Cormack whether there were any proposals on how to keep the database up-to-date. Andrew replied that RAND suggested an electronic version with upload possibilities, but there was no money for that. Wilfried Wöber added that maintenance and extension of the handbook should be mandatory and that it should be done by some institution with appropriate credentials. About the content of the handbook Karel Vietsch added that it is still incomprehensive and lacks information on what evidence could be needed as well as appropriate contact information.

Henk Bronk added that GOVCERT.NL had another handbook which is on CD, both in English and Dutch. They had distributed some copies of that handbook. Andrew Cormack suggested visiting the web site of the National Hi-The Crime Unit (www.nhtcu.org).

9. Results and outcomes from the meeting on documentation and the use of the IRT object

Wilfried Wöber presented outcomes from the meeting on documentation and use of the IRT object that was held on 29 August 2003 in Amsterdam.

He gave an overview on the history of the IRT object, format, functions and authorization requirements. The IRT objects could be attached to both IPv4 and IPv6 address space objects. He also showed "whois" command usage with and without parameter "-c". There were two ways of creating an IRT object – by way of the RIPE NCC (ripe-254) or by a well-known trusted body, recognized by the RIPE NCC. So far it has been done by the Trusted Introducer, but in the future ISP associations and NRENs could do that as well. There were 39 registered IRT objects, which were connected to the IP address range, in the RIPE database on 25 September 2003.

Wilfried Wöber spoke about the future developments of the IRT project, i.e. extension of the IRT mechanism to AS numbers, offering similar facilities to other regional Internet Registries (APNIC, ARIN), deployment, development of the tools for easy retrieval of the information, maintenance of the data, documentation.

The TF-CSIRT "interim" meeting contributed to the development of documentation and other issues about the IRT object. There were 10-14 participants from different areas, e.g. government, NRENs, TI, RIPE NCC, ISP associations, etc. Wilfried Wöber was very positive about the outcomes of the meeting. He thanked Marco Thorbrügge for taking the minutes and putting them on-line at <http://www.dfn-cert.de/team/matho/irt-object/>.

The meeting had decided to pay more attention to the marketing issues and to inform as wide a community as possible. RIPE meetings, the FIRST 2004 conference in Budapest and regional initiatives were mentioned as potential places for informing people. It has been decided to create technical how-to and FAQ documentation, to continue working with the RIPE-NCC on improving access to the information, continue using the TF-CSIRT mailing list, etc. As the last issue Wilfried Wöber mentioned that discussion has started on a more general approach to manage authentication when referencing the protected object in the database.

Jacques Schuurman proposed discussing with the APCERT people the possibility to introduce the IRT object in the APNIC database. Yurie Ito said that there is an initiative APRIFE, which would be presented in more detail in the APRICOT conference in February 2004.

Wilfried Wöber encouraged everyone to check the IRT objects web page, to read and comment on the FAQ. He promised to give an update on this issue in the next TF-CSIRT meeting.

10. Update on the CHIHT

Marco Thorbrügge reported on the latest activities within the CHIHT. CHIHT is a pilot project to compile a collection of tools and guidelines of their use, intended for incident handling teams. He told the group that usage statistics of the CHIHT website were available on-line at <http://chiht.dfn-cert.de/statistics>. The CHIHT webpage has been used on a daily basis. He promised to get the information about major users excluding internal scripts and mirrors for the next TF-CSIRT meeting.

ACTION 10-05: Marco Thorbrügge - to prepare statistical information on the CHIHT website and present it in the next TF-CSIRT meeting.

As a future improvement Marco Thorbrügge proposed to include graphics with the CSIRT -workflow descriptions as an HTML image map on the clearinghouse-webpage. Single parts of the workflow could be made clickable and would redirect the user to the appropriate tools to fulfil that step/task. A functioning prototype will be made available before the next meeting. Gorazd Bozic accepted Marco's proposal to present the prototype in the next TF-CSIRT meeting.

ACTION 10-06: Marco Thorbrügge - to include a sample CSIRT-workflow description as a prototype to the clearinghouse webpage and present it in the next TF-CSIRT meeting.

11. Report on the Conference on regional cybersecurity cooperation for South-Eastern Europe

Gorazd Bozic reported on the Conference on regional cyber-crime cooperation for South-Eastern Europe which took place in Bulgaria. The conference was organized jointly by the US Department of State and the Government of Bulgaria. The audience of the conference was mainly government officials from ministries, agencies and policy makers. The programme of the conference was dominated by speakers from the US. There were only few speakers from Europe, some presentations about local Bulgarian issues and the TF-CSIRT presentation by Gorazd Bozic. This was reflected at the closing session when several participants expressed their wish to have a more balanced approach and hear more about the European perspectives if there would be another conference for SE Europe.

The program itself dealt with the legislative and regulatory issues and also included a "how to start a CSIRT" talk from CERT/CC. As time was limited, Gorazd Bozic had given an overall presentation of TF-CSIRT and the history of European collaboration efforts, but concentrated on the Trusted Introducer and TRANSITS in the second half of his presentation. After his presentation, several participants expressed interest in TF-CSIRT and establishing contacts; most notably from Bulgaria, Hungary and Serbia.

The question on how to proceed was left unanswered at the end, but the Croatian colleagues (Natasja Glavor and Suzana Stojakovic-Celustka, who was previously also involved in the Croatian CARnet-CERT) mentioned that it is possible that they would try to organize a similar event next year in Croatia. Gorazd Bozic had also been told that another event is planned at the beginning of December in Belgrade with more emphasis on the data protection. There was no more particular information about this event available.

Miroslaw Maj asked Gorazd Bozic whether it would be possible to use this forum to popularize the TF-CSIRT activities. Gorazd replied that there was no forum, but if he gets all the email addresses of the participants, he would send some information about TF-CSIRT.

12. TF-CSIRT slide show presentation

Andrew Cormack informed the participants that a common slide show about the TF-CSIRT activities has been created. He thanked to all who contributed, particularly Jacques Schuurman and David Crochemore.

He said that he would like to have slides about all the TF-CSIRT activities. Then if somebody has to present something, he/she could choose the appropriate subset of slides. Andrew Cormack would like to suggest some subsets for the particular cases as well.

He encouraged everyone to contribute to these slides by adding missing information and checking the correctness of the existing information. The terms of usage for these slides would be similar to the TRANSITS training materials.

Baiba Kaskina would be in charge of keeping the latest version of the slide show and distributing it upon request. She would also collect some statistics, where people have used the TF-CSIRT slide show.

13. Election of the TFCSIRT deputy leader

Gorazd Bozic and Karel Vietsch explained the participants why the TF-CSIRT task force would need a deputy leader. The deputy leader function would chair the meeting of the task force in case the chairman cannot participate.

Gorazd Bozic asked the group for the nominations. Przemyslaw Jaroszewski nominated Andy Bone and he accepted the nomination. Jimmy Arvidsson nominated Andrew Cormack and he also accepted the nomination.

Karel Vietsch suggested that both nominees would leave the room and others would vote. This proposal was accepted.

Andy Bone and Andrew Cormack left the room and those present voted for the deputy task force leader. Andy Bone received 21 votes and Andrew Cormack 19 votes.

Gorazd Bozic congratulated Andy Bone as the deputy task force leader.

14. Results of the seminar sessions, ideas for the future sessions

Gorazd Bozic summarized that this seminar had gathered a very large number of participants. Unfortunately that caused problems with the meeting space and registration for the meeting had been closed one week before the event. He proposed organizing more spacious rooms in the future, but in case of a similar situation to limit the number of attendees to the meeting, i.e. only 2 persons from one team would be allowed. Others agreed that these would be reasonable conditions, but they should be implemented only as an emergency measure.

Karel Vietsch proposed implementing separate registrations for the seminar day and for the meeting day; the majority of the participants agreed.

Andy Bone felt that his presentation of yesterday could be considered a great success, because around 20 teams wanted to participate in trials of the RTIR system. He would think of possible ways how to continue this project and would inform the others. Andy Bone would give another update on the RTIR in the next TF-CSIRT seminar.

Jacques Schuurman asked the group whether anybody would like to participate in the trials of the NERD software. The following organisations volunteered – JANET, DANTE, SWITCH, DFN, CERT Polska (NASK), RedIRIS and UPC from Barcelona.

15. Status of the other TF-CSIRT work items / deliverables

Gorazd Bozic proposed discussing the rules for participation in TF-CSIRT. Until now subscription to the TF-CSIRT mailing list was approved by the TF-CSIRT chair. But in the last TF-CSIRT meeting in Warsaw it was decided to devise the rules for participation.

In Gorazd Bozic' view, subscription to the mailing list implies access to the TF-CSIRT meetings, but not necessarily the other way around. Attendance at TF-CSIRT meetings of people who are not subscribed to the mailing list is fully at the discretion of the chairman.

Gorazd Bozic proposed the following rules:

"In order to subscribe to the list, one of the following requirements must be met:

- A. the candidate works for a CSIRT that has acquired "TI accredited team" status (see <http://ti.terena.nl/> for details)
- B. the candidate works for a CSIRT that has a "TI listed" status and has established contacts with a CSIRT that is already participating in the TF-CSIRT.
- C. the candidate works for an institution which is forming its own CSIRT and has established contacts with at least one CSIRT that is already participating in the TF-CSIRT
- D. when the candidate is not a member of an existing European CSIRT but her/his work is closely tied to activities of European CSIRTs; the candidate has to be introduced by a CSIRT that is already participating in the TF-CSIRT

In all cases except A., the decision on whether a candidate can participate in the TF-CSIRT, as well as termination of subscription, is left to the TF-CSIRT Chair. Any complaints about this decision should be addressed to the TF-CSIRT Secretary: TERENA will then give a final ruling following discussion, if necessary, with the Chair, Task Force members, and other relevant parties."

The participants discussed to whom the complaints should be sent and who would take the final decision.. It was first suggested that the complaints committee should include TF Secretary, TF Deputy Chair and two persons nominated by the TF participants. Since this could result in deadlocks, it was decided that it is more reasonable to have three people in the committee: TF Deputy Chair, TF Secretary and an elected person. This proposal was accepted and Klaus-Peter Kossakowski volunteered for a one-year term to be in the complaints committee. He was unanimously elected.

ACTION 10-07: Gorazd Bozic - to finalise the new rules for participation in the TF-CSIRT and send them to the TF-CSIRT mailing list.

16. Date of the next meetings

The next meeting will be held on 15-16 January 2004 in Madrid, Spain (hosted by IRIS-CERT).

The subsequent TF-CSIRT meetings will be hosted by DFN-CERT in Hamburg on 27-28 May 2004 and mtCERT in Malta on 23-24 September 2004 .

17. Any Other Business

Jan Meijer proposed organizing a working group for IODEF exchange protocol. The eCSIRT.net project will end in December 2003, but the task would not be finished. The working group would consist of the people who were active in the eCSIRT.net project and would like to contribute in the future. He offered to prepare a charter and list of deliverables for the next TF-CSIRT meeting. All participants could discuss whether to add new deliverables to the TF-CSIRT charter.

ACTION 10-08: Jan Meijer - to prepare a charter and list of deliverables for the IODEF exchange protocol working group and present them in the next TF-CSIRT meeting.

Jacques Schuurman announced that CERT.NL will change name: from 1 January 2004 it will be SURFNET.CERT.

Ian Bryant proposed creating a working group on the possible unified Vulnerability and Exploit Description and Exchange Format (VEDEF). He would also prepare a charter and list of deliverables for the next TF-CSIRT meeting.

ACTION 10-09: Ian Bryant - to prepare a charter and list of deliverables for the working group on a possible unified Vulnerability and Exploit Description and Exchange Format and present them in the next TF-CSIRT meeting.

The meeting expressed its thanks to CERT.NL and the University of Amsterdam for organising a perfect meeting.

List of meeting participants

<i>Name</i>	<i>Organisation</i>	<i>Country</i>
1. Gilles André	CERTA	France
2. Jani Arnell	FICORA / CERT-FI	Finland
3. Jimmy Arvidsson	TeliaCERT	Sweden
4. Andy Bone	JANET-CERT	United Kingdom
5. Philippe Bourgeois	Cert-IST	France
6. Gorazd Bozic (Chair)	SI-CERT	Slovenia
7. Henk Bronk	GOVCERT.NL	The Netherlands
8. Ian Bryant	NISCC R&D	United kingdom
9. Andreas Bunten	DFN-CERT	Germany
10. Martin Camilleri	mtCERT	Malta
11. Roberto Cecchini	GARR-CERT	Italy
12. Andrew Cormack	UKERNA	United Kingdom
13. David Crochemore	CERTA	France
14. Daniel Cruz	esCERT-UPC	Spain
15. Michelle Danho	Renater CERT	France
16. Jan Drömer	Philips	Germany
17. Michel Dupuy	CERTA	France
18. Julian Field	University of Southampton	United Kingdom
19. Mikhail Ganev	RU-CERT	Russia
20. Rolf Gartmann	SWITCH	Switzerland
21. Natasa Glavor	CARNet	Croatia
22. Gema Gomez	esCERT	Spain
23. Manuel Gracia-Cervigón	esCERT	Spain
24. Christoph Graf	SWITCH-CERT	Switzerland
25. John Green	JANET-CERT	United Kingdom
26. Pege Gustafsson	TeliaCERT	Sweden
27. Kauto Huopio	FICORA / CERT-FI	Finland
28. Yurie Ito	JPCERT/CC	Japan
29. Przemyslaw Jaroszewski	CERT Polska / NASK	Poland
30. Jungu Kang	KISA/CERTCC-KR	Korea
31. Baiba Kaskina (Secretary)	TERENA	-
32. Hiroyuki Kido	JPCERT/CC	Japan
33. Ulrich Kiermayr	ACOnet-IRT	Austria
34. Piotr Kijewski	CERT Polska / NASK	Poland
35. Mark Koek	Stelvio	The Netherlands
36. Klaus-Peter Kossakowski	PRESECURE	Germany
37. Gilbert Laanen	Philips CERT	The Netherlands
38. Huw Langford	BT-CERT	United Kingdom
39. Sergey Linde	RU-CERT	Russia
40. Antonio Liu	PRESECURE / TI Team	The Netherlands
41. Iñaki Lopez	esCERT	Spain
42. Stelios Maistros	GRNET-CERT	Greece
43. Mirosław Maj	CERT Polska	Poland
44. Klaus Möller	DFN-CERT	Germany
45. Jan Meijer	SURFnet / CERT-NL	The Netherlands
46. Francisco Jesus Monserrat Coll	IRIS-CERT, RedIRIS	Spain
47. Gustavo Neves	FCCN (CERT.PT)	Portugal
48. Tomasz Nowocien	POL34-CERT	Poland
49. João Pagaiame	FCCN (CERT.PT)	Portugal
50. David Parker	UNIRAS/NISCC	United Kingdom

51. Leila Pohjolainen	Funet CERT	Finland
52. Jacques Schuurman	SURFnet / CERT-NL	The Netherlands
53. Mikel Stamm	DK-CERT	Denmark
54. Ilker Temir	Cisco PSIRT	Belgium
55. Marco Thorbrügge	DFN-CERT	Germany
56. Vincent Thiele	CERT-RO	The Netherlands
57. Yozo Toda	JPCERT/CC	Japan
58. Maris Urkis	LITNET CERT	Lithuania
59. Thomas Veit	BSI / CERT-Bund	Germany
60. Karel Vietsch	TERENA	-
61. Robert Walton	DANTE (Dancert)	United Kingdom
62. Torbjörn Victorin	SUNet-CERT	Sweden
63. Wilfried Wöber	ACOnet-IRT	Austria
64. Jörg Zemke	Philips	The Netherlands

Apologies were received from:

Suleyman Anil	NATO (NCIRC CC)	Belgium
Ralf Dörrie	Telekom-CERT	Germany
Chelo Malagón	IRIS-CERT/RedIRIS	Spain
Vlado Pribolsan	CARNet CERT	Croatia
Damir Rajnovic	Cisco Systems	Belgium
Krzysztof Silicki	CERT Polska / NASK	Poland
Han van Thoor	nl.tree / KCSIRT	the Netherlands

RESULTING ACTION ITEMS

07-03	Wilfried Wöber / Ulrich Kiermayr	Produce the documentation on how to use the IRT object in the RIPE database.
07-11	Don Stikvoort, BCP WG	Finalise Don Stikvoort's document on the BCP in CSIRTs.
09-01	Jan Meijer	Create a questionnaire regarding the Incident Handling System requirements and send it to the mailing list.
09-11	Andrew Cormack / Przemek Jaroszewski	Initiate a discussion regarding ideas how to involve more teams.
10-01	Klaus-Peter Kossakowski	Devise a proposal for the eCSIRT.net project follow-up, send it to the TF-CSIRT mailing list and lead the discussion about it in the next TF-CSIRT meeting.
10-02	David Crochemore	Send information about the World Summit on Information Society to the TF-CSIRT mailing list.
10-03	Gorazd Bozic	Initiate a discussion on the TF-CSIRT mailing list on TF-CSIRT becoming a registered SIG of FIRST.
10-04	Karel Vietsch	Contact Mr. Santucci and suggest having a meeting between a TF-CSIRT delegation and the EC in November 2003.
10-05	Marco Thorbrügge	Prepare statistical information on the CHIHT website and present it in the next TF-CSIRT meeting.
10-06	Marco Thorbrügge	Include a sample CSIRT-workflow description as a prototype to the clearinghouse webpage and present it in the next TF-CSIRT meeting.
10-07	Gorazd Bozic	Finalise the new rules for participation in the TF-CSIRT and send them to the TF-CSIRT mailing list.
10-08	Jan Meijer	Prepare a charter and list of deliverables for the IODEF exchange protocol working group and present them in the next TF-C SIRT meeting.
10-09	Ian Bryant	Prepare a charter and list of deliverables for the working group on a possible unified Vulnerability and Exploit Description and Exchange Format and present them in the next TF-CSIRT meeting.