

18th TF-CSIRT meeting

May 25-26, 2006

Vilnius, Lithuania

Author: Catalin Meirosu – Issue 2

1. Welcome and apologies

Gorazd Božič welcomed the participants to the 18th TF-CSIRT meeting. The list of registered attendees is attached at the end of these minutes..

2. Approval of the minutes and status of the Action Items from last meeting

The minutes of the last meeting held on the 23rd of January were approved.

17-1 – Wilfried Wöber - Ask Yuri Ito about possibilities to present the IRT object in the next APNIC conference.

Wilfried Wöber reported that this is still open. There will be an APNIC meeting in September, and this will be the new target date for this action item.

17-2 – Gorazd Božič - Initiate discussion about the work items and deliverables of the task force before the next meeting.

Gorazd Božič reported that he asked on the tf-csirt mailing list for suggestions for the new ToR, but he received no replies.

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

Christoph Graf announced that the deliverables are yet to be made available and therefore this action item will be maintained.

3. Update on ENISA – Andrew Cormack

Andrew Cormack reminded the audience that ENISA was formally setup in 2004. The organisation moved to Crete in September last year and became fully operational since. The Executive Director of the agency is advised on general issues, like the work program and directions that the agency should investigate, by a Permanent Stakeholders Group (PSG). The PSG is a collection of experts that was selected and appointed on the basis of the results of an open call for expression of interest. The PSG is composed of 30 individual members appointed until 2007. The members come from industry, users (for example, the head of security at BP) and academia (six of them). The PSG will have four meetings in 2006. The next ones are scheduled for June and October.

Three ad-hoc Working Groups were organised within ENISA and their respective Terms of Reference documents were agreed by the PSG. The areas covered by the Working Groups are CSIRTs, Risk Management and Awareness Raising. These groups are composed of well-known members of the community and pretty much independent of each other. ENISA has direct communication channels in each Member State and in the European Commission. Andrew noted that this has not happened before and he considered these channels as a very good step forward. The results of the Working Groups activity in 2005 were made available on ENISA's website.

The draft work programme for 2007 was first analysed at the meeting in Athens in May and will be approved in September. The split of domains was horizontal rather than vertical, and there is an increased focus on getting things done. The areas of interest under consideration include security tools (mainly commercial ones), how can one do authentication between organisations, metrics (tools for working out where you are in terms of information security) and new technologies – with security opportunities and threats that they bring. For example, peer-to-peer techniques that are good for distributing information could be used as well for spreading malware.

ENISA has a Management Board that stands between the Commission and the executive of the agency. The Management Board is composed of one representative from each member state, with three observers from the EEA member states. Representatives from the European Commission and consumers, academia and industry are also included in the Management Board. The Management Board formally approves the work programme of ENISA. The minutes of the Management Board minutes are made available on the ENISA website.

The first official request for advice was received by ENISA last autumn. It was related to a directive of the European Commission stating that the network providers had to assure the security and had to protect their users. Further inquiries from the ENISA staff revealed that the Commission had in mind the spam emails when this proposal was formulated.

All the ENISA publications are on the website, at the new URL:
<http://www.enisa.europa.eu>

4. JRA2 progress report – Christoph Graf

Christoph Graf started his talk by briefly introducing the Geant2 project started in September 2004 and scheduled to run for 4 years. The project encompasses several activity categories: Service Activities, Network Activities and Joint Research Activities (JRA). The JRAs have two major goals: to prepare the grounds for new services within the project (and its successors) and look forward to technology developments. JRA2 approaches the area of security, with the goal of improving the overall security for the Geant2 community. It tries to achieve its goal by involving existing security teams at the NRENs that contribute to the project. Twelve of the project partners are involved in

JRA2. The work is organised in 5 work items. The relationship with TF-CSIRT is formalised within Work Item 4.

An update to the policy document on securing Geant2 is currently under review. JRA2 developed “The Toolset”, a system composed of a flow probe, NERD and NFsen, that could be used for investigating security problems. The requirements for further development of the toolset were under discussion.

Christoph reported that the first case of formalised security advice from TF-CSIRT to Geant2 is pending. An official request was issued by Geant2. A team of volunteers from TF-CSIRT discussed the scenarios and were in the process of formulating an answer.

The NRENs involved in Geant2 had different levels of security expertise. The vision of the project calls for helping all the partners to achieve a minimum security level. The plan for the third year of the project shows a grouping of the activity in two categories, addressing distinct user types. The security services will be relevant for all the partners and the activities will be aimed at defining minimum requirements for a CSIRT. This activity will build on using existing initiatives like TF-CSIRT, FIRST, TRANSITS. It is envisaged to produce training material regarding The Toolset, and offering this training as a TRANSITS module could be discussed.

On the advanced services side, the participants plan to experiment with anomaly detection on the Geant2 backbone. The coordination infrastructure could be done by IODEF, but a decision on this should be taken during a JRA2 meeting.

5. Update on TRANSITS – Karel Vietsch

Karel Vietsch gave a brief status update on the TRANSITS courses, which were attended by most of the participants at the meeting. Initially, the material of the courses was developed by volunteers from the TF-CSIRT community and later the European Commission paid for the maintenance via the TRANSITS project. The funding ended last year, but the courses were considered very useful for the community so arrangements for longer term maintenance needed to be done. An agreement between FIRST and TERENA makes the long-term maintenance possible. The FIRST secretariat is the repository of the versions of the courses material. Volunteers from the community are encouraged to update each of the modules. The technical module was overhauled by the SWITCH-CERT people.

Two courses were organised after the end of the TRANSITS project, in Vienna (subsidised by ISPA) and Vilnius (sponsored by ENISA). Another CSIRT training event is planned later this year. Karel reported that GOVCERT.NL might be able to sponsor a workshop next year. TERENA and FIRST are currently looking for another sponsor for the last workshop of 2006. There are ongoing discussions for organising this workshop probably in November, so that an announcement could be sent to the mailing list after the summer holidays. ENISA might be able to sponsor it. They had a slight preference for

locating the workshop in Greece, and were discussing with GRNET CERT on the location. Karel promised keep the community informed on the progress of the discussions.

6. IRT object – Wilfried Wöber

Wilfried Wöber informed the audience about a decision taken at the 51st RIPE meeting to change the implementation in order to include IRT data on simple whois queries (in line with what the IRT group wanted from the beginning of the work). When RIPE NCC examined the implementation, they discovered a couple of corner cases when it was unclear what the original plan looked like. This was followed up by discussions on the mailing list and at the 52nd RIPE meeting in Istanbul.

The agreed solution involves several implementation phases. The first phase includes changing the behaviour of the answer to queries submitted via the web interface. Then, this change will be reviewed to see if it helped. The second phase of the implementation will change the default behaviour of the software. The minutes of the discussions will be made available on the official RIPE NCC web page.

Wilfried announced that a proposal for phasing out crypt-pw was under development. However, it was unclear how wide the spectrum of potentially affected people was - but this should be discussed before the end of June. He asked the participants to be prepared to use MD5 checksums and potentially X-500 or certificates for future interrogations of the RIPE database.

The NCC database predated European regulation (and national ones), so RIPE NCC started a review project to examine what will have to be done in order to comply with the regulations. They will setup a task force to help with the examination, so anybody on the database working group may receive an invitation to participate. There was also an idea of involving ENISA. Andrew said that the European Commission established a group known as the “Article 29 Working Party”. This group produced a good report on whois and this might help in the RIPE NCC examination. One of the recommendations from the report was to allow role details to be given as owning domains etc. rather than insisting on personal names and addresses. He asked everybody to try to get involved. People from CSIRTs should try to identify the address management entity in their constituency. This is because in case private persons can no longer be registered in the database (due to legislative constraints), the entire whois process would need to be changed.

In a short intervention before the coffee break, Til Döriges encouraged people who are FIRST members to step forward at the next conference for the positions in the Steering Committee. He also asked the audience if anybody was aware of someone considering to candidate for a position. Only one candidate was known so far: Francisco Jesus Monserrat (IRIS CERT).

7. Update on RTIR – Carlos Fuentes

Carlos Fuentes announced that the first milestone was reached on the 9th of March. The testing period covered workflow functionality and specific requirements (customer improvement, interface improvement). There were actually two rounds of testing, because so many bugs were discovered during the first round (more than 100) that the software was refused at first. The software was accepted after the second round of testing. Some minor bugs remained, but the producer promised to fix these bugs during 15 days. The second milestone should be reached in the second half of June. The RTIR working group advised all the new users of RTIR to only exercise the new version – RTIR 2.0 is stable. Carlos thought that the workflow would need to be refined in order to provide a more universal version. The RTIR working group intended to create a public website with the documentation.

Kauto Huopio asked about PGP integration. Carlos answered that PGP was part of the next milestone, with the deadline in about 6 months. Gorazd Božič asked how much has the database schema changed in RTIR 2.0 and whether migration tools were provided as part of the new distribution. Carlos answered that he will contact Best Practical and require a migration procedure. He has tried migrating the database, but the software crashed during the migration process. He concluded that in about 6 months he would expect a much smoother transition from version 1 to version 2.

8. Update on VEDEF – Ian Bryant

Ian Bryant started his talk by summarising the current situation in the Vulnerability and Exploit Definition and Exchange Format area. He considered that the main problem to be addressed is the proliferation of competing and incompatible formats for representing such information. Even though there is a de-facto standard for storing vulnerability data (Common Vulnerabilities and Exposures – CVE from Mitre), there are at least 8 proposals for vulnerability exchange formats. Ian exemplified by citing three formats in use with people from the TF-CSIRT community: DAF (Deutsches Advisory Format), CAIF (Common Advisory Information Format) and ITDF (Information Triage and Dissemination Format). Little support for a common format was noted throughout 2005 – especially during the BoF session at the FIRST meeting in Singapore and the informal discussions at W3C in the 4th quarter of 2005.

Ian described activities related to VEDEF, in the areas of trouble ticketing (the RTIR, OTRS and SIRIOS initiatives), remediation, ICT description and vulnerability scoring. He then reported on the meeting of the VEDEF working group hosted by Siemens CERT in April 2006. The participants belonged to six organisations from Germany and the UK. Ian reported that there was no obvious convergence path between the different formats used by the participants, and also noted that there was no pressing business case for such a convergence.

There seem to be little interest in the community for a common format for exchanging vulnerabilities and Ian partly reached to this conclusion before. There were 23-24 people who attended the working group over the years, but not much activity from the community. He felt very uncomfortable representing a one-person effort. He would be perfectly happy to wear his UK government metadata hat and update the community on developments in this area. Karel Vietsch suggested that VEDEF this could continue in TF-CSIRT as a liaison activity, with Ian being the liaison person.

8. Update on CSIRTs and Grids – Klaus Möller

Klaus Möller reported that the DFN-CERT performed a study and concluded that Grid incidents were not that different from standard security incidents. They are convinced that a CSIRT can do incident handling. When DFN-CERT examined in detail the Grid incidents they were called on to solve, it turned out that virtually all of them involved stolen authentication from the user workstation. Another conclusion of the study is that incident detection techniques that are specific to Grid environments need to be developed.

The DFN-CERT people found it difficult to track contact people for a particular IP address, especially in the context of a distributed system such as a Grid. Also, dealing with vulnerabilities was hard, as there were no public sources for vulnerability lists except those related to the Globus toolkit. Another problem exposed by the study was that Grid administrators and local CSIRTs co-exist in the same organisation, but the people in the different teams often did not know about each other.

Klaus Möller briefed the audience on the NREN-Grids workshop hold in Paris in April 2006. The conclusion of the workshop was that Grid security and incident handling could be approached by the existing NREN CSIRTs. However, a closer working relationship needs to be developed between all the actors – including the CSIRTs. To facilitate communication, a mailing list was established by DFN-CERT `grid-cert@grid-security.net`. The subscription process requires sending a message to the list, which will be handled by a human operator at the other end.

Klaus Möller announced that DFN-CERT tried to establish a meta directory for grid security documents, projects and expertise. The website will be at `www.grid-security.net` and was under development. He asked the audience for suggestions on what should go on this site.

Investigating vulnerabilities in Grid middleware was found to be difficult, in particular since there was no public list of vulnerabilities, with the exception of the Globus toolkit. Klaus Möller mentioned that at the NREN-Grids workshop Yuri Demchenko stated that EGEE had a closed group handling vulnerability issues. Klaus Möller expressed his hope that this information could be made available to CSIRTs.

Another problem identified by the DFN-CERT study was related to the software distribution process, for example the lack of PGP signing of packages. Klaus Möller thought CSIRTs could help the Grid developers in this process.

Andrew Cormack asked whether there further meetings on security and Grids will be organised in the future. Klaus Möller said that the workshop in Paris clearly indicated the need for more meetings. Catalin Meirosu announced that TERENA will organise another NREN-Grids workshop this year. The theme of the workshop is open to discussion, but the current proposal is to approach AAA issues.

Karel Vietsch thought that the turnout rate of the NREN-Grids workshop in April 2006 was a bit low, which would lead him to conclude that perhaps Grid people are not so much concerned about security. He pointed out that generally speaking it is non-trivial to find a European forum attended by more than one Grid project. Klaus Möller suggested that the CSIRT community could discuss with the national Grid initiatives – at least in the countries there had established contacts in this area.

9. Discussions on the Terms of Reference

Gorazd Božič started with the generic statements in the Terms of Reference document. The mandate of TERENA task forces was limited at two years. The participants may propose the extension of the task force, and the TERENA Technical Committee may approve or deny the extension. The current mandate of TF-CSIRT approaches the end of the lifetime. Therefore, a new Terms of Reference document needs to be discussed in order to extend the mandate for another two years.

There were no comments or objections to the text of the Point 2 of the ToR.

Referring to Point 3 of the ToR, Gorazd commented that there have not been any real problems in the past two years in relation to the participation to the mailing list. There were no objections to the content of Point 3 of the ToR.

The discussion related to Point 4 of the ToR was opened by Gorazd stating that Kauto Huopio was currently the deputy leader of the task force. Gorazd declared he would feel more comfortable if someone else would organise the election for a new chair. He asked the audience if there are ideas or possible nominations for different task for chair. Andrew Cormack asked whether it was permissible to nominate the same chairman. Gorazd replied that serving another mandate would not be a problem for him. The audience agreed to Gorazd Božič to continue as the task force chair, and also confirmed Kauto Huopio as deputy chair.

In relation to Point 5 of the ToR, Gorazd asked whether TERENA would be comfortable with continuing the work. Karel Vietsch answered that TERENA would be happy to do

that. He also mentioned that the costs of supporting the task force are currently reimbursed by the European Commission through the GN2 project.

The only issue with respect to Point 6 of the ToR is changing the dates to reflect the new mandate. Andrew Cormack asked the audience for suggestions or volunteers for the TNC Program Committee.

There were no comments or objections to the text of the Point 7 of the ToR.

There were no comments or objections to the text of the Point 8 of the ToR.

There were no comments or objections to the text of the Point 9 of the ToR.

The discussion continued to the work items. Work Items A and B will be maintained with the same text in the new ToR.

Gorazd asked whether there was still a need for maintaining Work Item C in the new ToR. Karel Vietsch asked what was the IODEF status within the IETF. Till Döriges answered that the IETF has issued a draft, but the changes are small and his thought there was not much going on in the area. Gorazd polled the audience on who would like to keep this work item in the new ToR, but there were no positive answers. In conclusion, work item C will be dropped from the new ToR.

There were no objections for work item D being maintained. Karel Vietsch asked Wilfried Wöber whether the formulation needs update. Wilfried replied that he found the text to be quite good and promised to think offline whether an update was needed.

Gorazd asked whether the clearinghouse for security incidents specified as work item E should be kept as a task force activity. Klaus Möller answered that, to his knowledge, Marco Thorbrügge said he was going to maintain it while working at ENISA. The decision was to keep the work item and contact Marco for clarifications on the status. Karel Vietsch suggested that in case Marco could not continue to maintain this website, perhaps someone from the community could take over.

Karel Vietsch remarked that the formulation of work item F is no longer up to date. He volunteered to draft a text and circulate it to the list for approval.

The effort covered by work item G was carried mainly by Andrew Cormack and Przemek Jaroszewski. Andrew said that it was very difficult to get feedback out of people on whether this was useful or not. ENISA will prepare a checklist for opening a new CSIRT. Gorazd asked whether Andrew expected any new effort in the area. Andrew replied that he would not expect any additional effort, until there is some feedback (perhaps also via ENISA). Andrew suggested changing the word “develop” to “maintain”. Robert Morgan also suggested changing the word “working” to reflect what TF-CSIRT would do to assist people. Robert and Andrew promised to circulate a new version of the text for approval on the mailing list.

It was decided that work item H will be kept in the new ToR. Gilles André suggested to include collaboration with e-coat (and pointed out that work item N refers to e-coat by the wrong name)

There were no comments or objections to the text of the Work Item I of the ToR.

Ian Bryant agreed to draft a new text for Work Item J and circulate it on the mailing list

Christoph Graf proposed to maintain the same text for the Work Item K in the new ToR.

Gorazd felt that little work has been done within Work Item L. He was sceptical that much additional work could be done. Andrew Cormack thought that the building blocks for an incident data exchange network were covered by JRA2. Christoph Graf thought that even within JRA2 there was not much incentive to automate it. The agreement was to drop this item from the new ToR.

Karel Vietsch volunteered to update the text of Work Item M and circulate the draft on the mailing list. The audience agreed delete the last phrase.

There was no real need for the second phrase in the current text of Work Item N. It was suggested add e-coat in brackets to clearly identify the reference.

Gorazd asked the audience whether new Work Items were needed. Andrew Cormack proposed a work item related to Grid and another one related to email whitelist information exchange. Gorazd felt that the whitelisting is more of the resort of the e-coat. There were no additional comments from the audience on this issue. Karel Vietsch expressed his agreement for including a Work Item on Grid-related security issues. Andrew Cormack and Klaus Möller agreed to propose a text on the mailing list.

10. Dates and venues for next meetings

Leila Pohjolainen and Kauto Huopio presented Espoo and Helsinki, the location of the next meeting TF-CSIRT on 21-22 September. The meeting will be co-hosted by CSC/FUNET and FICORA.

The TF-CSIRT meeting in January 2007 (a joint TF-CSIRT – FIRST technical colloquium) will take place in Budapest. It could be organised from Monday to Wednesday and the intervals 15th-17th, 22nd-24th, 29th-31st were proposed to the audience. It was noticed that the EGC meeting will be during week 3, and many people would participate to that meeting. The conclusion was to suggest the 29th-31st of January to the Hungarian organisers.

The meeting in May 2007 will be organised in Prague, but it was felt that is was too early to discuss about the actual dates.

Gorazd Božič thanked LITNET-CERT for hosting the 18th TF-CSIRT meeting, and everybody in the audience for attending.

List of Meeting Attendees

Adrian	King	SI-CERT
Aivar	Jaakson	CERT-EE
Alexander	Talos	ACOnet
Andrea	Kropacova	CESNET
Andrew	Cormack	UKERNA
Anukool	Lakhina	Boston University
Arturs	Medenis	LATNET
Baiba	Kaskina	LATNET
Carlos	Fuentes	IRIS-CERT/RedIRIS
Carlos	Doce Reyes	EsCERT
Carol	Overes	GOVCERT.NL
Chelo	Malagon	IRIS-CERT
Christoph	Graf	SWITCH
Claudio	Allocchio	GARR and TERENA
Cătălin	Meiroșu	TERENA
Darius	Janulevičius	TeliaSonera SubCERT CSIRT-Omnitel
Darko	Androcec	CARNet
David	Pybus	Diageo
Derek	Simpson	BT CERT CC
Don	Stikvoort	Trusted Introducer
Erika	Stockinger	SITIC
Filip	Gyllensvaan	SITIC
Gilles	ANDRE	CERTA
Gorazd	Bozic	SI-CERT
Gustavo	Neves	CERT.PT
Hillar	Aarelaid	CERT-EE
Ian	Bryant	CSIA / NISCC
Jaan	Priisalu	Hansabank
Jimmy	Arvidsson	TeliaSoneraCERT
Karel	Vietsch	TERENA
Kauto	Huopio	FICORA / CERT-FI
Klaus	Möller	DFN-CERT
Ladislav	Lhotka	CESNET
Leila	Pohjolainen	Funet CERT
Lionel	Ferette	BELNET CERT
Marius	Urkis	LITNET CERT
Martin	Camilleri	mtCERT
Michael	North	BT Secure Business Services
Milda	Mimiene	LITNET CERT
Nerijus	Slušnys	AB Lietuvos Energija
Nino	Jogun	CARNet CERT

Orod	Badjelan	DK-CERT
Pavel	Kácha	Cesnet, z. s. p. o.
Peter	Haag	SWITCH-CERT
Peter	Hammond	NISCC
Piotr	Kijewski	CERT Polska/NASK
Przemek	Jaroszewski	CERT Polska/NASK
Robert	Morgan	JANET-CERT
Rytis	Rainys	Communications Regulatory Authority
Sarunas	Talandis	SE Infostruktura
Serge	Droz	SWITCH-CERT
Sigitas	Jurkevicius	Communications Regulatory Authority
Till	Dörges	PRESECURE Consulting GmbH
Tomas	Beinaravičius	Hansabankas
Torvaldas	Česnulevičius	Ministry of Interior
Urpo	Kaila	Funet CERT
Vilius	Nakutis	Communications Regulatory Authority

Action List resulting from the meeting

17-01	Wilfried Wöber	Ask Yuri Ito about possibilities to present the IRT object in the next APNIC conference.
16-04	Christoph Graf	Inform the TF-CSIRT group when the GN2 JRA2 deliverables are publicly available.
18-01	Catalin Meirosu	Replace the name of the deputy chair in article 4 of the ToR, to reflect the fact that Kauto Huopio accepted this position
18-02	Catalin Meirosu	Change the date in article 6 of the ToR to reflect the new mandate of the task force
18-03	Wilfried Wöber	Send an updated text for Work Item D of the ToR
18-04	Gorazd Božič and Klaus Möller	Contact Marco Thorbrügge for clarifications on Work Item E
18-05	Karel Vietsch	Circulate an updated text for Work Item F
18-06	Robert Morgan and Andrew Cormack	Send an updated text for Work Item G
18-07	Ian Bryant	Send an updated text for Work Item J
18-08	Karel Vietsch	Send an updated text for Work Item M
18-09	Andrew Cormack and Klaus Möller	Send a text for a new Work Item on CSIRTs and Grids