20th TF-CSIRT meeting
January 29-31, 2007
Budapest, Hungary

Author: Cătălin Meiroşu – Issue 2

1. Welcome and apologies

Gorazd Božič welcomed the participants to the 20th TF-CSIRT meeting. The list of attendees that registered through the TF-CSIRT website is attached at the end of this document.

2. Introduction to Hungarian CSIRT activities

Ferenc Suba presented the activities of the CERT-Hungary team. The team was established in 2006. The activity is mainly government-oriented. The collaboration with the police is very good and CERT-Hungary is training the cybercrime task force of the police. CERT-Hungary was organised within the framework of the Theodore Puskás foundation, a special type of foundation that was established by the government in 1993. The supervisory bodies of the foundation are the Prime Minister's office and the Communications Authority. The team is accredited by FIRST and a founding member of the International Watch and Warn association. CERT-Hungary represents the government in the relationship with ENISA and OECD. Current plans include developing an early warning system and fostering collaboration in Eastern Europe.

Tamás Tiszai introduced the MTA-Sztaki team. The constituency is made of a network of research institutes and ISPs. However, the team only mediates between ISPs. The service is provided only during regular office hours (no 24/7 service). The main areas of interest for the team were development and deployment of security tools. They were also working on the security of mobile networks and have a project running a sensor network.

János Mohácsi spoke about the security activities at NIIF-Hungarnet. NIIF-Hungarnet was responsible for the development of Internet infrastructure dedicated to research and development in Hungary. They connected more than 500 institutes and served more than 600000 users. The activities were supported by the work of 39 employees, out of which 27 were technical staff. János Mohácsi asked the audience what was the average response time for incidents when it was required to block systems. Andrew Cormack answered that, in the case of UKERNA, the policy allows for blocking immediately if needed. János Mohácsi said that at NIIF the default policy recommended blocking after two days, but this could also be done immediately if the risk to the infrastructure was considered very high. Jacques Schuurman asked whether NIIF had a relationship with the NREN of Serbia. János Mohácsi answered that NIIF acquired cross border dark fibre and was providing services to the Serbian NREN. Scott McIntyre asked what the ASN number of

NIIF was. János Mohácsi answered that NIIF had several ASNs, and that the mean number was 155.

3. Update on ENISA activities

Marco Thorbrügge presented recent activities at ENISA. The agency was established as a centre of expertise for governments in the EU. The first mandate will end on March 2009. The mid-term review was finished and the results were expected in April 2007. Marco Thorbrügge reported that ENISA had two deliverables in 2006: The CSIRT setting up guide (available online since October 2006). The second deliverable was briefly presented during this meeting, and was made available online at the end of January 2007. Together with the colleagues from CERT-Polska, ENISA made an informal study for an European alerting system.

Marco Thorbrügge announced that ENISA built a section on their website dedicated to CSIRT cooperation. It can be accessed at http://www.enisa.europe.eu/csirt_cooperation The website includes description of the models and legal bases of collaboration, models of trust, past and present of cooperation examples, analysis of the status quo in the field and conclusion on how to further foster cooperation. ENISA would appreciate the feedback of the community with respect to this website.

Marco Thorbrügge stated that the legal document that would allow ENISA to host the Clearinghouse for Security Tools was signed by TERENA and will be signed by ENISA's director general. Therefore, he expected to have a mandate to work on the Clearinghouse shortly. Marco Thorbrügge announced his intention to update the information currently in the Clearinghouse. He will prepare a questionnaire and send it to the community. Marco Thorbrügge asked DFN-CERT to continue hosting the Clearinghouse website until the required infrastructure will be setup at ENISA's premises.

Kauto Huopio asked whether ENISA was aware of new CSIRT teams from Romania or Bulgaria. Marco Thorbrügge reported that they were not aware of new teams. However, ENISA's director visited the new member states a few weeks before the TF-CSIRT meeting, so first contacts were established at governmental level. Gorazd Božič announced that Bulgaria appointed a representative in the ENISA management board.

Klaus Möller – Update on CSIRTs and Grids

Klaus Möller started his presentation by briefly summarising the developments since the BoF session held at the January 2006 TF-CSIRT meeting. Activities related to interactions with the Grid community were added to the new TF-CSIRT Terms of Reference document approved in June 2006. The website that was promised was still in the planning stage. Klaus Möller noted that lots of expressions of interest were received, but very little concrete responses or ideas for projects. One of the reasons may have been

that these activities remained often in very early planning phases. No definitive answer could be provided to the question whether a Grid-CERT is needed. However, the consensus was that CSIRTs should answer Grid incidents. There was also agreement in the community that Grids have many things to learn about CSIRTs.

Klaus Möller continued by giving the example of the DGrid project in Germany. This is a Grid integration project centred on six communities: high-energy physics, astronomy, climate change, InGrid = engineering, Medigrid = protein research, large scale immunological research, Textgrid = comparing large amounts of text related to social sciences and linguistics. Klaus Möller thought CSIRTs could provide pro-active services to these communities, in addition to incident response. In order to tailor these services to specific Grid needs, the CSIRTs community would need to increase the awareness and setup points of contact in a more formal way.

Through their participation in DGrid, DFN-CERT was building up knowledge for a Grid CSIRT in all aspects. Penetration testing could be performed on Grid sites. Also, Grid sites on the net could be identified using standard open source tools. Klaus Möller demonstrated how a specific Grid could be identified by looking into the webservices and the service certificate. DFN-CERT accumulated nmap fingerprints for certain Grid services, but they need to keep them private for the time being. Intrusion detection could be performed via neighbourhood watch. Someone from InGrid asked whether DFN-CERT could deploy Grid honeypots. Klaus Möller mentioned that honeyd could be setup to fake Grid ports. CSIRTs need to know about the Grid software and their vulnerabilities. In this respect, audits were performed within the Grid community (especially EGEE) and outside. Klaus Möller reported observing a slowly growing interest in the grid vulnerabilities – mainly because Grid sites were seen as “cool” to play with.

One of the problems to be addressed when handling Grid incidents is to determine, as a CSIRT, whether a particular IP address belonged to a Grid, and which user ran software at the time of the incident. The Planetlab addressed this issue by building a webpage that allowed submitting an IP address and then the project tracked the usage internally. Klaus Möller reported that this worked for him twice. Andrew Cormack mentioned that another interesting issue would be to know in advance what type of traffic would be expected expected. Carlos Fuentes reported that he is the Security Officer for South-Western European region in EGEE, and as such was involved in handling Grid incidents.

Carlos Fuentes – Update on RTIR

Carlos Fuentes reported that in October 2006 the group received the 2nd release of the software. Since then, a testing phase covered the workflow and overall functionality. The workgroup was planning to buy the rtir.org domain and create a community of users on this website. Carlos Fuentes reported that they were planning for a v3 of the software, if enough money could be raised from the participating organisations. He also reported on plans to have a dedicated online test system.

Sławomir Górniak - Examining the feasibility of an European Information Sharing and Alert System

Sławomir Górniak announced that the European Commission asked ENISA to examine the feasibility of an Information Sharing and Alerting System at a European scale. This request is included in the Communication COM(2006)-251, entitled Strategy for Secure Information Society. Sławomir Górniak briefly reviewed the generic categories of information sharing and alert systems. Passive systems are made by best practice documents. Active systems include advisories on new exploits or patches available for various operating systems. Short-term systems target the dissemination of warnings and countermeasures. This study will build on the role of ENISA in fostering a culture of security in Europe. As such, it is part of the overall effort in raising the awareness on network and information security with the citizens and the SMEs. As indicated in the Communication, an important feature of the system would be multilingualism, thus allowing information in the native language to be disseminated in the member countries. Sławomir Górniak reported that ENISA assembled a voluntary experts group to examine the feasibility of such system. The work was concentrating on analysing the resources already available in various countries and producing a description of possible use scenarios. The next steps will be concentrated on assessing the added value of a European-wide Information Sharing and Alert System, by determining a series of indicators that could be used to analyse the impact on the overall security culture.

Karel Vietsch – Update on TRANSITS

Karel Vietsch briefly explained what the TRANSITS courses are about and the history behind them. The courses started as a project funded by the European Commission. The training material covered five areas and is delivered during two full days. A training session usually gathers from twenty to thirty attendees. The course material was originally developed as a volunteer effort by members of the TF-CSIRT community during 2001. Seven training workshops were organised during the TRANSITS project lifetime. The materials were also made available to organisations that wanted to arrange their own workshops. The courses developed something of an introduction to the TF-CSIRT community. Karel Vietsch thanked again the teachers of the courses, all volunteers. At the end of the EU-funded interval, the workshops continued with sponsorships from several organisations, notably ENISA and ISPA.

Karel Vietsch announced that the Memorandum of Understanding with FIRST for organising TRANSITS courses outside of Europe came to an end in Oct 2006. The FIRST Board of Directors decided to discontinue the collaboration with TERENA on TRANSITS. The motivation of the decision was unclear to Karel Vietsch. He announced that TERENA plan to continue organising the courses three times a year as long as there is interest in the community. Sponsorship for future workshops would be even more important, in order not to raise the registration fees and be able keep the workshop

participation affordable. Karel Vietsch announced that JP-CERT is translating the TRANSITS material in Japanese and intends to use it for courses in Japan.

Marco Thorbrügge asked whether more details would be available on the planned training session in Bulgaria. Karel Vietsch answered that he was in contact with the people appointed to run a government CSIRT there. TERENA could not be more precise on the date, but there were hopes of organising the training before the summer.

Wilfried Wöber – RIPE IRT Database update

Wilfried Wöber reported that there was little progress on this topic from the previous TF-CSIRT meeting. Most IP address space registered in the database still needs to be linked to IRT objects. He asked the opinion of the audience with respect to these issues. Margrete Raaum thought that, for a particular organisation, it may not be clear whose responsibility is to register an IRT object in the database. Also, the amount of work required to actually register IRT objects is difficult to estimate. Wilfried Wöber answered that the RIPE working group was aware of these potential issues. He showed the ENISA webpage containing the CERT activities in Europe as an example of coverage. Jacques Schuurman mentioned that his team was asked by a CERT team of a SURFnet client whether they need to register their own IRT object or whether SURFnet CERT would prefer to have that IP address block registered under their own name.

Wilfried Wöber proposed to develop a Cookbook that would complement the FAQ on the IRT object existing on the RIPE site. Gorazd Božič asked whether this Cookbook would be aimed at the users (CERTs) or at the maintainers of the database. Wilfried Wöber felt that both parts would need to collaborate, but the actual focus of the Cookbook would need to be determined. He thought the document should be developed within TF-CSIRT. Marco Thorbrügge reminded the audience that he wrote such a document in 2003. Gorazd Božič noted that in this case the community should perhaps better disseminate this document and re-evaluate the need for a new Cookbook.

Action item 20.1. Wilfried Wöber, Don Stikvoort and Gorazd Božič will review the existing documents (FAQ, how-to, other guides) on the RIPE IRT object.

Wilfried Wöber announced the formation of a Data Protection Task Force at RIPE. The reason for forming this task force is that the RIPE database was found to be non-compliant to the European and Dutch data protection regulations. He invited people from the TF-CSIRT community with an interest in this subject to join the task force. More details on the task force could be found on the website at http://www.ripe.net/ripe/tf/dp/index.html.

Jacques Schuurman – GN2 JRA2 Update

Jacques Schuurman presented a brief update on the JRA2 activities in the GN2 project. He reported that the project was proceeding into the 3rd year of activities. The toolset developed by the contributors in the activity consisted in both hardware and software tools. An important part of the activities were now aimed at determining how netflow data could be analysed in more sophisticated ways. An equally important aim of the activities in JRA2 was to raise the overall security metric of GN2 project participants. The metric was yet to be defined, but Jacques Schuurman thought that it should be defined in such way that the JRA2 community as a whole would feel comfortable with it. Andrew Cormack asked whether the project planned to document the various choices that were considered for the elements composing the metric. He exemplified with the case of the accreditation system for the teams. Jacques Schuurman answered that it was the intention of the collaborators in JRA2 to provide such documentation.

Ian Bryant – Information Security Metadata

Ian Bryant presented the wider context under which these activities took place, namely the "cooperation with information security metadata activities" from the TF-CSIRT Terms of Reference document. He identified two large categories of metadata that CSIRT teams should have an interest in: Description and Exchange Formats and Reusable Name Spaces. The category of description and exchange formats includes Forensic Investigation data, Incident Objects, secure configuration metadata, security event descriptions, susceptibility and flaw descriptions, and vulnerability and exploit metadata. The Incident Object Data Exchange Format (IODEF) which originated in work of a TF-CSIRT subgroup is now available as RFC 3067. Several directions of development were pursued through IETF in the Extended Incident Handling (INCH) working group. The Forensic Investigation Data Exchange Format (FIDEF) could be implemented as an extension of IODEF. The Secure Configuration Data Exchange Format (SCDEF) had to approach three scenarios, including installation, new and ad-hoc connections and flaw remediation. However, the "standard configurations" would need to be extended for taking into account local policies and countermeasure elements. As a Security Event Data Exchange Format (SEDEF), it was thought that the IETF-lead IDMEF would provide 90% of the solution. However, subsequent analysis found that a wider scope needed to be addressed in order to support firewall logs, malware checkers, content monitors, etc. Ian Bryant reported that NC3a-NL, Mitre and the UK government were all investigating various options for addressing these issues. The Vulnerability and Exploit Data Exchange Format (VEDEF) was defined within a TF-CSIRT working group lead by NISCC. Ian Bryant reported he was aware of three formats being used in practice: CAIF, DAF and IVDF. He then continued by providing an overview on the work on metadata for ICT-Namespaces and Events and Incidents Namespaces. Ian Bryant announced that the study entitled Exploiting Metadata for Information Assurance was completed. Also, as result of a reorganisation within the UK government, the effort he could devote to this area will be greatly reduced. Therefore, Ian Bryant called for a new TF-CSIRT voluntary rapporteur in this area. Andrew Cormack observed that the review presented was comprehensive and suggested that perhaps this activity in TF-CSIRT could be considered completed as well.

Gorazd Božič asked Ian Bryant to summarise the issues in an email and send it to the tf-csirt list. Gorazd Božič thanked Ian Bryant for his involvement in this activity.

Action item 20.2. Ian Bryant to send an email to the tf-csirt mailing list, summarising the issues in the metadata formats area.

Amendment adopted as proposed by Jan Meijer, at the 21st TF-CSIRT meeting in Prague, May 4th

RFC3067 documents the requirements for IODEF, IODEF itself has not yet received a RFC number, it is currently on its way to IETF last call.

Any other Business

Scott McIntyre noted that the activity within E-CoAT slowed down in the last months. He announced that E-CoAT was looking onto ways to improve this, and invited TF-CSIRT members to contact him or someone else in E-CoAT with ideas on how to improve the activity. Gorazd Božič asked the participants to contact their colleagues doing abuse handling and remind them about E-CoAT. Raymond Azzopardi noted that the E-CoAT webpage was not updated for a while. Scott McIntyre answered that E-CoAT were still investigating on the right combination of people and topics for the web page. Gorazd Božič suggested that perhaps E-CoAT could become a regular item on the agenda of the TF-CSIRT meetings.

Dates and venue for the next meeting: May 3rd, Prague, hosted by CESNET-CERT. A host would still be needed for the September meeting. The dates of the September meeting were agreed to be 20 and 21st.

Summary of Action Items

Action item 18.1 – Wilfried Wöber – Report on the number of teams that connected inetnum objects to their IRT object in the RIPE database.

Action item 18.2 – Wilfried Wöber – Contact RIPE NCC regarding the plans to include the RIPE NCC whois client in Linux distributions.

Action item 20.1. Wilfried Wöber, Don Stikvoort and Gorazd Božič will review the existing documents (FAQ, how-to, other guides) on the RIPE IRT object.

Action item 20.2. Ian Bryant to send an email to the tf-csirt mailing list, summarising the issues in the metadata formats area.

Annex – List of attendees (registered through the TF-CSIRT website)

Alexei	Altuhov	RENAM Association
Andre	Oosterwijk	GOVCERT.NL
Andrea	Kropacova	CESNET
Andrew	Cormack	UKERNA
Andás	Kabai	CERT-Hungary
Antonio	Liu	TI Team
António	Marques	FEUP-Faculdade de Engenharia da Universidade do Porto
Ari	Husa	FICORA / CERT-FI
Arjen	De Landgraaf	E-Secure-IT
Arturs	Medenis	LATNET CERT
Axa	Rojas	LUZ
Balazs	Szekeres	CERT-Hungary
Beatrix	Tóth	MTA SZTAKI
Bence	Birkas	CERT-Hungary
Branko	Mažar	CARNet CERT
Brian	Honan	BH Consulting
Carlos	Fuentes	IRIS-CERT/RedIRIS
Carlos	Doce	EsCERT-UPC
Carol	Overes	GOVCERT.NL
Claudia	Natanson	Diageo
Cătălin	Meiroşu	TERENA
David	Pybus	Diageo plc
Derek	Simpson	BT CERT CC
Don	Stikvoort	Trusted Introducer
Elena	Galván	EsCERT-UPC
Enikő	Becske	CERT-Hungary
Erika	Suortti	FICORA / CERT-FI
Ferenc	Suba	CERT-Hungary
Francisco	Monserrat	IRIS-CERT /RedIRIS
Gabor	Roczei	NIIF/HUNGARNET - NIIF CSIRT
Gilles	ANDRE	CERTA
Gorazd	Božič	SI-CERT (ARNES)
Gustavo	Neves	CERT.PT
Harri	Sylvander	Funet CERT / CSC - Scientific Computing Ltd.
Ian	Bryant	CSIA
Ian	Cook	Pentest Ltd
Jacques	Schuurman	SURFnet-CERT
Jane	Bondur	State Service for Special Communication and Information Protection
Janos	Mohacsi	NIIF/HUNGARNET
Jonas	Juknius	Communications Regulatory Authority
Juergen	Sander	PRESECURE
József	Komli	CERT-Hungary
Karel	Vietsch	TERENA
Kauto	Huopio	FICORA / CERT-FI
Klaus	Möller	DFN-CERT

Klaus-Peter	Kossakowski	PRESECURE
Ladislav	Lhotka	CESNET
Lionel	Ferette	BELNET CERT
Lorincz Dr	Istvan	ASSOCIATOR Ltd. (CERT-Hungary)
Maciej	Milostan	PIONIER CERT, PSNC
Maksym	Smetana	State Service for Special Communication and Information protection of Ukraine
Marco	Thorbruegge	ENISA
Margrete	Raaum	UiO-CERT
Marius	Urkis	LITNET CERT
Mark	Rowe	Pentest Ltd
Martin	Zadnik	CESNET
Masaki	Kubo	JPCERT Coordination Center
Mirosław	Maj	CERT Polska
Nino	Jogun	CARNet CERT
Orod	Badjelan	DK-CERT
Pascal	MERCIER	CERTA
Pavel	CELEDA	CESNET
Per Arne	Enstad	UNINETT CERT
Peter	Haag	SWITCH-CERT
Peter	Quick	T-Com CERT / Telekom CERT
Piotr	Kijewski	CERT Polska/NASK
Rafael	Calzada	Carlos III University
Rafal	Tarlowski	CERT Polska
Ralf	Dörrie	Telekom-CERT
Raymond	Azzopardi	mtCERT
Reijo	Matinmikko	Ericsson
Serge	Droz	SWITCH
Sigurd	Mytting	University of Oslo
Simen	Stovland	NorCERT
Spiros	Antonatos	Institute of Computer Science, FORTH
Stelios	Maistros	GRNET-CERT
Sławomir	Górniak	ENISA
Tadej	Hren	SI-CERT (ARNES)
Tamás	Becz	MTA-SZTAKI
Tim	Hurman	Pentest Ltd
Varis	Teivans	LATNET CERT
Victor	Sant'Anna	Ericsson PSIRT
Vytautas	Krakauskas	LITNET CERT
Werner	Schram	SURFnet
Wilfried	Woeber	ACOnet CERT
Zoltan	Györkő	Balabit Ltd. (CERT-Hungary)

-- amend the minutes with comment from Jan.