

22nd TF-CSIRT meeting

20-21 September 2007

Porto, Portugal

Author: Cătălin Meiroşu – Issue 1

1. Welcome and apologies

Gorazd Božič welcomed the participants to the 22nd TF-CSIRT meeting. The list of attendees that registered through the TF-CSIRT website is attached at the end of this document.

Welcome address – Prof. Dr. Carlos Costa, FEUP President

Professor Costa said that for a university, ICT security is important in terms of services offered by the university computing centre. As FEUP is a technical university that teaches computer science curricula, security is also important for them from the academic and research points of view. The perception should be that security was not about making life difficult to users. It was concerned with giving access to the right items for the right people. He hoped the entire meeting will be fruitful for us and the attendees will enjoy Porto and the local specialties.

Welcome address – Tito Vieira, director of CICA

Tito Vieira is the director of services at the Centro de Informática Prof. Correia Araújo (CICA), the FEUP Computing Centre. The mission is to maintain and manage to ICT infrastructure of the university. The services cover several areas, such as network connectivity, firewall, information systems, etc. The ICT infrastructure in FEUP supports 6000 (...check number...), 6000 students and 1000` staff. Many services are targeting the students. An authentication infrastructure based on OpenLDAP and Active Directory was deployed for all students. The Computing Centre developed an identity management tool to ease the account management. Since 2005, students may change the password via an sms message. The main categories of services include wired and wireless access, antivirus, antispam, blog space, scientific software. A terminal server farm allowed users to run applications without installing software on their computers. The campus network offered wireless access on all public zones. Faculty has 27 computer labs having about 600 PCs, dual boot Linux-Windows. The labs were open 24h/day, 365 days/year. The FEUP Computing Centre has 20 employees. The security team covered handling of this type of incidents. Recently they have been accredited by the Trusted Introducer (July 2007). There is a clear need to create a security culture in the university, in particular for the end users.

3. Antonio Marques – Introduction to FEUP security activities

Antonio Marques started by thanking CERT-PT and IRIS-CERT for their help in the TI accreditation process. The security team is part of the networking department of the IT services at the Computing Centre. They are an academic CSIRT. The networking department also took care of projects such as the VoIP deployment. The teams for network and system admin needed to work together for handling incidents. The teams developed a system that creates extensive logs of all activities on the network. The Computing Centre also had a direct user support team, with team members assigned to each one of the computer labs. The HPC department takes care of the FEUP grids and clusters.

The FEUP-CSIRT maintained a portal about vulnerabilities and support tools (available through the team's webpage at <http://csirt.fe.up.pt/>). The vulnerability tracking system was developed to filter and present only the ones that were meaningful to the particular software deployments in the university infrastructure.

Jacques Schuurman asked what sources of information were used for dissemination of vulnerabilities and who the intended audience was. Antonio Marques answered that the audience was made of all the students and staff of the university. Sources included BugTraq, facert, etc. Only critical vulnerabilities were tracked because of the amount of information available on all sources was too large if all categories were included.

Jacques Schuurman what happened if there was a small number of users using eccentric platforms. Antonio Marques answered that the team was already in dialogue with such users. The team was not going to monitor these platforms. Antonio Marques remarked that the most difficult part of the vulnerability tool development was to find a way to globally catalogue or describe software platforms. For a while, they worked with someone in Siemens-CERT on this.

Another question from the audience was asked for more details on how the scanning services were implemented. Antonio Marques reported that a nessus server is contacted through a web interface and then runs the scan. This approach was good for a first step in interacting with students, as they were able to request scans of their own computers.

Gorazd Božič asked whether statistics on how many of the systems scanned were found vulnerable. Antonio Marques answered that the main area to be addressed was statistics. The team was working on it, but for now statistics were not available.

More details on the live CD were requested by the audience. Antonio Marques answered that it was based on Ubuntu, customised for the FEUP environment. The team needed to update it each time the distribution changes. As a more general remark, Antonio Marques noted that the computers on the FEUP infrastructure were booted over the network, so the patching takes place centrally at the level of the bootable operating system images stored on servers.

4. Hillar Aareleid and Kauto Huopio – Update on the Estonian network incidents

Hillar Aarelaid started his presentation with a brief incursion in history in order to give a background to the incidents. WWII for Russians meant defending their country. They had lots of losses during the war, and May 8 became very important in significance. Every Estonian had some relative that were deported to Siberia during the Stalin times. The Russian soldiers were regarded as occupants by the Estonians. Conflicts around the statue in the centre of the city escalated every year on the 8th of May between Estonians and Russians. At the end of April 2007, there were riots (maybe around 2000 people in the street) against the move of the statue. The attacks on the Estonian Internet started on the 27th of April. A campaign propaganda on Russian websites called for attacking Estonian Internet servers. Hillar Aarelaid thought this was the only way for Russians not living in Estonia to attack Estonians. The first peak was about 400kbps to a government sites, finally ended up with about 4 millions packets per second on the 5th of May. Lots of targets, state and private owned, were attacked in many different communities, including the educational community. Many different types of attacks were performed on all these targets. The CERT-EE team had to work with many players in order to address these incidents. In general, they could solve quite easy one incident a day. But for a large number (actually unknown) of incidents taking place during 4 weeks, their procedures were ineffective. For zombie networks with large number of nodes it was virtually impossible to get in touch with all the ISPs on whom networks these machines were located.

Kauto Huopio said CERT-FI had to tools to process all such cases automatically. They did this for about 160 ASs in Finland regularly. It was simply getting the data from Hillar Aarelaid, running their scripts on it and perhaps some phone calls for the AS-es where automatic messages could not be sent. CERT-FI developed a method for setting up a private IRC server where people could communicate in a trusted environment. Gorazd Božič, Hillar Aarelaid, Kauto Huopio and people in Germany met in such environment. CERT-FI provided neutral information to the media and the community on the incidents.

Karel Vietsch reported that newspapers in The Netherlands reported that NATO put 10 people on a plane, sent them to Tallin and they solved all the problems. Hillar answered that he met with two people from NATO. CERT-EE handed over a lot of raw material to NATO site. Even though not that much feedback came back, this was considered as normal practice in the field. The headlines in the media helped them a lot, he thought. Kauto Huopio remarked that this situation was a big eye opener on what can be done with DDOS-es. But he thought the real threats are not DDOS. The people behind these attacks want the internet to work so they can carry out profitable criminal activities.

The audience asked how many systems were affected. Hillar Aarelaid answered that Estonia was a small country with 1.5 million people. Only the smallest one of the banks was not attacked. They targeted mostly two of the banks that were the biggest market players. The attackers targeted the online banking systems. They did not attack to deface the webpages.

The participants asked whether the government put out warnings for the computer users related to these incidents. Hillar Aarelaid answered that this was done only to ask for

people to be calm. Several means of communication were used, including sending SMS messages to all the mobile phone users.

Kauto Huopio thought that it was to be expected that media went into overdrive on such events. Training the staff on duty to have skills and even the permission to talk to the press would be good, but then they had to know how the press works.

The audience wanted more details about the extent of the problem. For example, whether ATM machines were affected and what was that made peoples lives difficult. Hillar Aarelaid explained that in Estonia 99% of the banking transactions were made electronically. This made the difference, even though POSes and ATMs were mainly unaffected.

5. Andrea Kropáčová - Building National CERT of the Czech Republic

Andrea Kropáčová presented a new project entitled “Building National CSIRT of the Czech Republic”. She started by introducing the members of the project team present in Porto that were new to the TF-CSIRT community: Robert Malý (NESS), Martin Kult (NESS), Václav Jirovský (Charles University, Prague). The project was funded by the Ministry of Interior of the Czech Republic for the interval 2007-2010 and is lead by Václav Jirovský.

Andrea Kropáčová outlined the activities of the Centre for Combating Cyber-Threats, an agency established by the Czech government. The agency became the entity responsible for Cyber Security in the Czech Republic. Part of its activities was to support security research and development projects and act as a liaison between the public sphere and the academic world. The activity of the agency was supported by six organisational divisions. The Czech national CSIRT was supposed to form one of these divisions. The project finally mandated to organise these activity started in May 2007, after many years of political debates.

Andrea Kropáčová announced that the domain www.csirt.cz was registered by the project. A first milestone, to be reached during Autumn 2007, consists in signing Memorandums of Understanding regarding the cooperation with the most important Czech ISPs. The incident handling will be based on procedures, policies and tools provided by CESNET-CERTS. The team aims to start a pilot service in January 2008.

Andrea Kropáčová asked the participants to send any reports on incidents involving computers connected to Czech network to the address abuse@csirt.cz

6. Wilfried Wöber – update on RIPE database activities and the IRT object

Wilfried Wöber reported that an abuse-mailbox field was added to the IRT object in the RIPE database. This would be the place for the contact details of a dedicated abuse handling team. A major re-writing of the IRT object documentation was triggered as result of the input from the TF-CSIRT community.

Issues on data protection were high on the agenda of the last RIPE meeting. It was concluded that the RIPE database was not compliant with Dutch and European regulations in this area. A task force was created by RIPE-NCC to address these issues. More details on these activities may be found at <http://www.ripe.net/ripe/tf/dp/index.html>.

Several changes to the IRT object were proposed and are still under discussion. Removing orphaned objects (person) from the database and requiring a maintainer for all objects in the database were options being considered in the working group. Several other areas, such as the NRTM service, creating mntr objects and dealing with legacy stuff were also on the agenda.

Gorazd Božič asked Wilfried Wöber whether he would be willing to re-run the IRT workshop if there would be interest in the community. Wilfried Wöber answered that he would be happy to do it.

Kauto Huopio asked whether there were any discussions in the working group regarding the availability of the data in the database. Wilfried Wöber remarked that such discussions took place almost every other year. Most of them originated from people that have little knowledge about enforceability. Wilfried Wöber asked the audience if anyone having ideas, expectations, or suggestions relating to the IRT object to get in touch with him.

7. Jacques Schuurman – Brief report on the visit to APCERT

Jacques Schuurman was invited to Malaysia at the APCERT conference as the TF-CSIRT liaison to APAN. Jacques witnessed the elections which he thought were a bit more formal than in TF-CSIRT. Also, there are more functions for people to be elected in. APCERT were going to setup an out-of-band system of communication that would span many timezones. They would be interested to include some of the teams in our community in the pilot. The project was to be lead by AuCERT. Volunteers from the TF-CSIRT community interested to contribute could contact Jacques Schuurman.

Action item 22-1: Jacques Schuurman asked Hillar Aarelaid if he could get in touch with the APCERT people regarding the incidents in Estonia.

Gorazd Božič asked whether more details could be provided on what would involved by the volunteering.

Action item 22-2: Jacques Schuurman to check with AuCERT (and perhaps JPCERT) who was already involved in the project and what would be required from potential volunteer European teams.

8. Jacques Schuurman – JRA2 update

Presentation prepared by Christoph. GN2 is the EU project funded by the EC, 37 NREN members in Europe, for a next-gen backbone. JRA2 is about security. There are 12 partners that work in JRA2.

9. Karel Vietsch – TRANSITS update

Karel Vietsch started his presentation with a short history of the TRANSITS courses. He announced TERENA's decision to continue running twice-yearly workshops as long as there is interest from the community and sponsorships could be secured in order to keep the fees low. Karel Vietsch mentioned that if TF-CSIRT members wanted to use the materials for national workshops, they were welcome to contact the address on the website and TERENA will send the latest version of the materials.

Karel Vietsch reminded the audience that an agreement with FIRST stated that any time FIRST organises a workshop outside Europe they will pay TERENA 600 euro for the maintenance of the course materials. However, FIRST asked TERENA to charge everybody else that wanted to organise workshops outside Europe a similar fee of 600 euro. Karel Vietsch did not commit TERENA to do this, but the situation was a bit unclear. In June, IRIS-CERT and UNAM-CERT (Mexico) organised a workshop in Mexico. This workshop was not related to FIRST, but they asked FIRST permission to use the material. FIRST pointed to TERENA for the material, but also asked them to pay the 600 euro. As well as another initiative for a workshop in Peru, the organisers could not afford paying the fee. Karel Vietsch found it not good that courses were not allowed to take place (or even running illegally perhaps) on these grounds. Karel hoped this issue of the contribution will be raised in the FIRST steering committee.

Karel Vietsch announced the next training course to take place in Kannach, Luxembourg. The government of Luxembourg provided a generous sponsorship, together with ENISA. The formula will be the usual one. Karel Vietsch reminded the audience that the deadline for registration was 28 of September.

Serge Droz noted that in the application for prospective participants there was a demand for recommendations from two well-known teams. He thought this was difficult, especially for new members. He suggested that perhaps one recommendation could be enough.

Jacques Schuurman asked how the 600 euro for the fee was calculated. Karel Vietsch answered that the amount paid for maintaining the material was divided by an estimate of

the amount of workshops organised annually outside Europe. Jacques Schuurman suggested we keep our own policy for fee-free availability of the materials or charging small prices only when this could not be avoided.

10. Gorazd Božič – Questionnaire on TF-CSIRT future activities

Gorazd Božič announced that the three meetings in 2008 were planned already, although some question marks remained on some of them. The purpose of having this discussion now was related to the decreasing number of action items and discussion groups within the Task Force. A lot of feedback was needed on how the future of TF-CSIRT was seen by the community. Maybe everybody was happy just meeting three times a year, listened to presentations and then talked to people. Also, there may be areas where people had common interests and problems to solve. Therefore, the feedback of the community was needed. Gorazd Božič noted that just a few answers were received to the message sent on the mailing list and asked the participants for suggestions.

Andrew Cormack said that with respect to the meeting in May 2008, if it took place later than the Tuesday before the TNC (May 19-22, 2008) he and perhaps other members would have problems attending. Gorazd Božič reminded the audience that the place of the meeting was Oslo. One possibility would be to move it one week ahead of the TNC on the Monday. However, Saturday the 17th of May is the Independence Day and a national holiday in Norway. Another possibility was 12-13 May.

Action point 22-3: Gorazd Božič to coordinate with the local organisers the dates for the May 2008 TF-CSIRT meeting.

Gorazd Božič announced that for the meeting in September 2008 an offer was received from the Russian colleagues. Gorazd had exploratory discussions with them for some time now. One issue would be the visas. The Russian team was in communication with the Ministry of Foreign Affairs in a try to streamline the visa application procedure. Gorazd Božič would like a broader feedback on this. He invited the participants to discuss this with him either in public or in private. He pointed out that a wider feedback on this issue was really needed.

Jacques Schuurman reminded the participants that SURFNET-CERT we were the ones that accredited RUS-CERT with FIRST. He thought it would be worth considering their invitation. We want them to be part of the community. He would be in favour to going to Russia for this meeting. Don Stikvoort fully supported what Jacques Schuurman. Serge Droz said that if our visit strengthens that team and the IT security in the country, then it would be worth doing.

Dan Bailey wanted to know in more details how would this meeting be organised. He noted that from his business perspective Russia was probably not one of the safest environments to walk around. Gorazd Božič promised to discuss this with Mikhail

Ganev. He announced that part of the solution could be that the organisers take care of the transportation to and from the airport, for example.

Regarding the next meeting in January, the proposed location was Prague. Derek Scholl confirmed to Gorazd Božič that Sun Microsystems has facilities in Prague (easily reachable by metro) that could be used for a meeting of 120+ people. Gorazd Božič was still waiting for a confirmation that these facilities would be available on the proposed dates, 28-30 January 2008. The participants agreed with these dates.

There was no time left for a detailed discussion on the questionnaire regarding future TF-CSIRT activities. Gorazd Božič thanked the few that sent feedback by email, and ask the participants to the meeting to send their opinions to him and the TF-CSIRT secretary.

Action item 22-4: Gorazd Božič and the TF-CSIRT secretary to schedule the discussion at the top of the agenda for the TF-CSIRT meeting in January.

Annex 1. List of the attendees registered on the TF-CSIRT website

First name	Last name	Organisation
Alexander	Talos	Univie / AConet
Andrea	Kropacova	CESNET
Andreas	Bunten	DFN-CERT
Andrew	Cormack	JANET(UK)
Antonio	Sanchez	CCN-CERT
António	Sacramento	CC-CRISI FA
Anukool	Lakhina	Guavus, Inc.
Arturs	Medenis	LATNET-CERT
Baiba	Kaskina	LATNET
Barbara	Monticini	GARR
Bernhard	Tellenbach	ETH Zurich
Carlos	Simões	CC-CRISI FA
Carlos	Abad	CCN-CERT
Carlos	Fuentes	IRIS-CERT/RedIRIS
Carol	Overes	GOVCERT.NL
Chelo	Malagon	IRIS-CERT/RedIRIS
Christoph	Graf	SWITCH
Christoph	Sprongl	iT-AUSTRIA
Claudio	Allocchio	GARR
Cyril	Gayet	CERTA
Cătălin	Meiroşu	TERENA
Damijan	Marinsek	Ministry of Public Administration
Dan	Bailey	GovCertUK
Daniel	Eriksson	TS-CERT subCERT CSIRT-TSS
David	Penedo	CERT.PT
Demos	Panagopoulos	FORTH-ICS
Derek	Simpson	BT CERT CC
Dmitry	Avramenko	RU-CERT
Don	Stikvoort	Trusted Introducer DDIRV (State Information Network Agency - CSIRT)
Egils	Sturmanis	
Elena	Galvan	esCERT-UPC
Emin	Akhundov	AzNET Project
Francisco A.	Lago	INTECO
Gorazd	Božič	SI-CERT (ARNES)
Hillar	Aarelaid	CERT-EE
Igor	Karpenko	RU-CERT
Jacques	Schuurman	SURFcert
Janos	Mohacsi	NIIF/HUNGARNET
Jason	Rafail	CERT/CC
Jimmy	Arvidsson	TS-CERT CC
Karel	Vietsch	TERENA
Kauto	Huopio	FICORA / CERT-FI
Krešimir	Nesek	CARNet CERT
Ladislav	Lhotka	CESNET
Leila	Pohjolainen	Funet CERT

Lino	Santos	CERT.PT
Lionel	Ferette	BELNET CERT
Marco	Thorbruegge	ENISA
Marius	Urkis	LITNET CERT
Martijn	de Hamer	GOVCERT.NL
Martin	Camilleri	mtCERT
Martin	Kult	NESS
Maurizio	Molina	DANTE
Mehis	Hakkaja	ENISA
Michelle	Danho	CERT RENATER
Mike	Andersen	NorCERT
Nino	Jogun	CARNet CERT
Orod	Badjelan	DK-CERT
Otmar	Lendl	nic.at
Pascal	Steichen	Ministry of the Economy and Foreign Trade
Paulo	Alves	CC-CRISI FA
Pavel	Traian	SIE Romania
Peter	Haag	SWITCH-CERT
Przemek	Jaroszewski	NASK/CERT Polska
Raymond	Azzopardi	mtCERT
Robert	Maly	NESS
Robert	Schischka	nic.at
Rudolf	Schraml	Bundeskanzleramt
Salih	Gönüllü	SWITCH
Serge	Droz	SWITCH
Shehzad	Ahmad	DK-CERT
Simona	Venuti	GARR-CERT
Stefan S.	Stefansson	PTA
Stelios	Maistros	GRNET-CERT State Agency for Information Technology and Communications
Tanya	Nikolova-Kotseva	
Thorben	Jändling	JANET CSIRT
Torsten	Voss	DFN-CERT
Varis	Teivans	LATNET-CERT
Victor	Sant'Anna	Ericsson PSIRT
Vladimir	Bobor	TS-CERT CC
Václav	Jirovský	CUNI, guest of CESNET-CERTS
Werner	Schram	SURFnet
Wilfried	Woeber	ACOnet-CERT
Wim	Biemolt	SURFnet

Annex 2. Summary of the action items

18-1. Wilfried Wöber reported he needed to contact Ulrich Kiermayr and ask him to run the script again. Wilfried Wöber would then distribute the results via the tfcsirt mailing list. Wilfried Wöber asked the TF-CSIRT secretary to remind him of this action item between the TF-CSIRT meetings. The action item is still open.

18-2. Wilfried Wöber reported progress. The whois v3 client was available from sourceforge. He thought that convincing the Linux distributions to include it would not be easy, but he will discuss this issue during RIPE NCC meeting in Tallinn. The action item is still open.

18-3. Wilfried Wöber reported that there was quite a lot of progress in this area, but further details were included in the IRT presentation.

21-1: Christoph Graf to check the public flag on the GN2 JRA2 deliverables on the toolset and announce on the tf-csirt mailing list when they will be available.

22-1: Jacques Schuurman asked Hillar Aarelaid if he could get in touch with the APCERT people regarding the incidents in Estonia.

22-2: Jacques Schuurman to check with AuCERT (and perhaps JPCERT) who was already involved in the project and what would be required from potential volunteer European teams.

22-3: Gorazd Božič to coordinate with the local organisers the dates for the May 2008 TF-CSIRT meeting.

22-4: Gorazd Božič and the TF-CSIRT secretary to schedule the discussion at the top of the agenda for the TF-CSIRT meeting in January.