



SUBJECT

Approved minutes of the 33rd TF-CSIRT meeting
2 June 2011, Malahide, Ireland
Version 1.2

Page 1/9

33rd TF-CSIRT meeting

2 June 2011

Grand Hotel, Malahide, Ireland

Please note that a seminar was held the following day. The presentations can be found at <http://www.terena.org/tf-csirt/meeting33/>

1. Approval of Minutes

The minutes of the last meeting held on 1 February 2011 were approved.

2. Actions from last meeting

- 31.1 TI Review Board to discuss how to deal with Spamhaus problems and what further action to take.
Ongoing.
- 31.2 CERT NIC.LV to document specific problems they had experienced with Spamhaus.
Done.
- 32.1 André Oosterwijk to check whether CERT Academy materials could be made available to other CSIRTs.
Done. An CSIRT employee profile was available in Dutch, but this could be translated and shared if there was enough interest.
- 32.2 Marco Thorbrügge to send pointer to information about Article 13a to the mailing list.
Ongoing.

3. Team Cymru presentation

Ian Cook gave a presentation about Team Cymru. This was a geographically-dispersed group of security professionals who provided a variety of commercial and community services, and who collaborated with a number of governmental and industrial bodies.

Team Cymru was a non-profit organization with US 503(c)3 status that essentially gave it charitable status, and had its main office in the Chicago area. However, there were also researchers located in New York, Washington D.C, Arizona, California and Missouri; as well as in Australia, New Zealand, Poland, and UK.

Kauto Huopio asked about Team Cymru's plans for the future. Ian replied they might expand a bit further, but they wanted to maintain their unique working environment and did not wish to become just another security vendor.

4. BTCERT presentation

Derek Simpson gave a presentation about BTCERT (see <http://www.terena.org/tf-csirt/>)

[meeting33/simpson-btcert.pdf](#)). This was an investigatory team that coordinated internal computer and network security incidents across the BT enterprise, raised security awareness across the business, and liaised with other CSIRTs and law enforcement agencies.

The team provided 24x7x365 response and had a network of sub-CERTs to support key areas of BT that were vulnerable to external and malicious attacks. As sub-CERTs received priority incident handling, full sub-CERT status was only granted after a site obtains high levels of security practice in accordance with FIRST regulations.

BTCERT was also considered an important element in the UK government's national security strategy, which included hostile attacks on UK cyberspace. However, the UK did not currently have a national CSIRT and there appeared to be very little coordination between other UK-based CSIRTs on a regular basis.

Andrew Cormack asked whether law enforcement agencies had become more technically aware. Derek replied they were a lot more technically savvy these days, although this had taken a lot of training.

Kauto Huopio asked about incidents originating from BT customers. Derek replied virus and malware infections were a particular problem, although they planned to deploy an automated detection system in the near future.

5. SI-CERT presentation

Matej Breznik gave a presentation about SI-CERT. This was the Slovenian national and government CSIRT that provided the main contact point for reporting network security incidents in the country. It was operated as a service of ARNES, the Slovenian NREN.

6. AbuseHelper Developments

Christian Van Heurck reported on the feedback from the first AbuseHelper workshop (see <http://www.terena.org/tf-csirt/meeting33/vanheurck-abusehelper.pdf>). This had been held on 2-4 May 2011 at the BELNET offices in Brussels, and had involved representatives of several CSIRTs.

The workshop aimed to identify which aspects of the AbuseHelper automated incident report framework needed improving, which sources of information could be used, and how the statistical analysis should be implemented. A number of inputs and tools were identified, with a view to developing a demonstration system. However, there were a number of legal issues to investigate around the use of data that could be used to identify individuals.

Andrew Cormack mentioned that he had written a paper on incident response and data protection, along with worked examples (see <http://www.terena.org/tf-csirt/publications/data-protection.pdf>). Christian added they were also compiling links to applicable data retention legislation and would be interested in sharing this, but wondered whether other teams could do something similar. Dave Monnier replied this was a good idea and might be something Team Cymru would be interested in undertaking.

7. Phishing at your own risk

Jan Vykopal gave a presentation on the phishing awareness initiative that was being

trialled at Masaryk University (see <http://www.terena.org/tf-csirt/meeting33/vykopal-phishing.pdf>). Spear phishing was a growing problem at the university, with an increasing number of e-mails being sent from compromised accounts in trusted domains. This meant they were not trapped by anti-spam and anti-phishing filters, and therefore user education acquired a lot of significance.

To this end, approximately 250 users volunteered to be exposed to three different e-mail traps based on real attacks. E-mails were sent randomly over a 30 day period, and user actions were logged and evaluated.

With the generic phishing e-mail, 80% of the recipients did not respond, 14% clicked on the included link, whilst another 6% revealed their credentials. With the more targeted e-mail, 68% of the recipients did not respond, 20% opened the attachment, whilst 12% revealed their credentials. These results were discussed with the administrators in the affected departments, with a view to improving user awareness of these sort of attacks.

Alexander Zen-Talos said they had undertaken something along similar lines, but to check whether users accepted invalid SSL certificates. Around 50% of users had actually done this.

8. Building a phishing net

Bente Christine Åsgård gave a presentation on an phishing e-mail filtering system they had developed at the University of Oslo (see <http://www.terena.org/tf-csirt/meeting33/aasgaard-phishing.pdf>). Whilst they had dramatically decreased volumes of spam over the past year thanks to effective filtering, the number of phishing e-mails remained the same. They received an average of around 75 complaints per month from users, with up to 4 accounts being compromised.

They therefore considered that if spam can be identified, then why not phishing e-mails as well? Closer investigation revealed there were probably less than 10 basic layouts, and these were used to build custom filters for their mail system that worked by scanning for known patterns.

Even though a working prototype only took five hours to develop, it did appear to be quite effective in preventing phishes reaching users. There were some false positives, but these were mostly related to automated messages that users probably wouldn't notice had not been delivered. Indeed the number of complaints had dropped to around 15 per month (12 of which were reporting new attacks) and there had only been one compromised account since.

Further work was needed to develop a framework for quarantining messages for further inspection (e.g. in case of false positives), but it had been demonstrated that it was feasible to build custom filters for little time and money that were as effective as proprietary solutions.

Dave Monnier observed that the University of Oslo appeared to have less compromised accounts than those who had identified e-mails as phishes. It was usually the other way around, so was it the case that the university had more educated users? Bente replied they had run an awareness raising campaign for a long time, so this might explain it.

James Davis asked whether they were aware of an outbound e-mail filtering product called Kochi (see <http://oss.lboro.ac.uk/kochi1.html>).

9. CENTR Security Activities

Serge Droz reported on recent security developments within the European ccTLD community (see <http://www.terena.org/tf-csirt/meeting33/droz-centr.pdf>).

ccTLD registries were normally heavily regulated and therefore security understanding seemed to follow similar lines, in particular ISO 27001. CENTR (the European ccTLD Association) was increasingly interested in incident handling and coordination though, and was now planning to hold regular security meetings. The first of these would be held on 7 June 2011 in Trondheim and Serge had been invited to participate. However, he did not feel that another security community was desirable, and asked whether there was anything that TF-CSIRT could do to better involve ccTLDs.

Wilfried Wöber asked whether the ccTLD registries' interest in security was related to the ICANN DNS-CERT initiative. This did not appear to have made much progress, but perhaps there were developments behind the scenes. Some CSIRTs already had close relationships with ccTLD registries as they belonged to the same parent organisation, so it made sense to try to involve them in TF-CSIRT.

Andrew Cormack said that some countries already blocked domains to prevent the spread of botnets and other malware, so there were certainly common issues to discuss. He added that Paul Vixie and others had written an interesting paper about the US PROTECT IP Act, which aimed to implement DNS filtering (see <http://www.shinkuro.com/PROTECT%20IP%20Technical%20Whitepaper%20Final.pdf>).

Kauto Huopio however, thought that DNS was a specialist service with its own unique issues. Whilst it was important to establish good relations, he felt it was more appropriate for them to have their own forum.

Kevin Meynell added that TERENA had previously been approached by CENTR to enquire about the use of Trusted Introducer for incident coordination in the ccTLD community. Some information had been provided, but there had not yet been any follow-up.

It was agreed that Serge should discuss TF-CSIRT and TI in Trondheim, and invite CENTR to participate in the next TF-CSIRT meeting.

Action 33.1 – Serge Droz to invite CENTR to participate in TF-CSIRT meeting in Luxembourg.

10. TRANSITS I/TRANSITS II update

Don Stikvoort reported on the recent TRANSITS II course, and provided an update on developments (see <http://www.terena.org/tf-csirt/meeting33/stikvoort-transits.pdf>).

The first TRANSITS II workshop had been held on 6-8 April 2011 in Zürich, following on from the trial workshop in October 2010 in Amsterdam. This focused on advanced topics for experienced CSIRT members, including NetFlow, forensics, communications skills and practical exercises. The second workshop was planned for Spring 2012, possibly in Prague.

The TRANSITS I material was currently in the process of being updated, with the operational module nearly completed. The technical module was planned to be next, in order to align the material with that in TRANSITS II. The advisories module had been dropped as these were less important these days, whilst the roleplay now used the ENISA

exercises.

The next TRANSITS I workshop was planned for early-September in Dublin, although offers for workshops after this were welcomed.

11. Restructuring TF-CSIRT and TI

Kevin Meynell presented some ideas about restructuring TF-CSIRT and Trusted Introducer (see <http://www.terena.org/tf-csirt/meeting33/meynell-tf-csirt.pdf>).

TF-CSIRT was created in 2000 and over the past 11 years had established itself as one of the main forums where CSIRTs could discuss and exchange experiences and knowledge. It had also established a number of spin-off activities such as Trusted Introducer (TI), TRANSITS and RTIR upgrades.

The average attendance at TF-CSIRT meetings was between 60 and 70 participants, although this rose to approximately 120 participants at the meetings held jointly with FIRST. In the past year, around 60% of participants had come from academic CSIRTs, 20% came from government CSIRTs, 15% came from commercial CSIRTs, and 5% came from other types of organisations.

Allied to this, the TI service had been established in 2001 as an accreditation and listing service that was financed by the CSIRTs and provided under contract by a third-party supplier (currently S-CURE, but PRESECURE from 1 September 2011). There were currently 80 accredited teams of whom 44% were academic, 28% were governmental, and 28% were commercial; as well as 143 listed teams of whom 39% were academic, 24% were governmental, and 37% were commercial. The average attendance at each TI meeting was around 50 participants.

It could therefore be seen that the group had moved well beyond its origins as a forum for academic CSIRTs, and was increasingly seen as a representative body by external organisations. However, the group's mandate and terms of reference technically needed to be renewed by TERENA every two years, which was increasingly incongruous for a group that had become indispensable.

There were a number of other reasons why change was necessary. TF-CSIRT had no formal notion of membership which was increasingly expected by external organisations, and there was confusing overlap between TF-CSIRT and TI, with (often) different Chairs and Secretaries. This led to duplication of functions and awkward coordination, whilst not permitting common use of staff resources. TI was also now well established and should therefore be considered an essential element of the European CSIRT community rather than an 'add on'.

More importantly though, TF-CSIRT had started to drift away from its former cooperative approach and there was increasingly less input from participants. There was also a feeling that the CSIRT community had become a bit disconnected from the leadership, which was even more of a concern now that non-academic CSIRTs (who were not represented in TERENA) constituted a majority.

The proposal was therefore to amalgamate TF-CSIRT and TI, with the new entity becoming a standing body of TERENA rather than having to be biennially renewed. The plan would be to retain the name 'TF-CSIRT' as that is more descriptive and better known than 'Trusted Introducer'.

A formal membership would then be defined based on existing TI categories and

qualifications – namely accredited members, listed members and associate members (who are individuals). All members would have the right to attend TF-CSIRT meetings, although a closed session for just accredited members would still be held. This would formalise the current ad-hoc and largely unwritten arrangements with respect to who is allowed to attend meetings, although the TF-CSIRT Chair would still have the possibility to invite non-members as necessary.

The plan was also to have an elected Chair (probably for 3 year periods), with the existing TI Review Board becoming a TF-CSIRT Advisory Board. This would be comprised of the TF-CSIRT Chair, the TF-CSIRT Secretary, and 3 other members elected by accredited teams on a 3-year cycle (i.e. 1 member elected per year). In addition to their TI responsibilities, this board would advise on the direction of TF-CSIRT as whole, act as a programme committee for the meetings, and deputise for the Chair in his/her absence.

The TI services as defined by TERENA in consultation with the Advisory Board would be continue to be provided by the TI supplier (PRESECURE from 1 September 2011) under the TF-CSIRT umbrella. Accreditation fees would continue to be collected to cover the costs of these.

The benefits would be that TF-CSIRT and TI would be streamlined and simplified without any radical change, but would establish a unified regional group with a recognisable membership. It would also improve coordination and use of staff resources, as well as establish a more direct relationship between teams and the leadership.

Wilfried Woeber expressed concern at the lack of transparency with how TERENA had handled the recent TI re-procurement, and how much influence the TI Review Board representatives actually had over the process. Kevin replied that the announcement of the TI fees followed by the announcement of the TI re-procurement could have been better handled, but TERENA had legal and financial responsibilities with respect to the contract so ultimately had to make the final decision. In addition, procurements by necessity have to be confidential, so there is only so much information that can be made public. Nevertheless, he believed that TERENA saw the advice and recommendations of the TI Review Board as being important, and it would have an expanded role under the new proposals.

Kauto Huopio asked whether the new entity would adopt policies or positions on particular issues. Kevin replied that was entirely a matter for the group to decide when any new charter was being formulated, and indeed such matters could even be decided at a subsequent date.

The question was asked whether TERENA would continue to support TF-CSIRT. Kevin replied that TERENA considered TF-CSIRT to be a very important and useful activity, and planned to continue its support as well as provide the necessary legal framework for contracting and/or operating the support services.

There were a number of comments that the proposals appeared to be a positive development, so a show of hands was called to determine whether to formulate a more detailed proposal. Nearly all participants were in favour, with no objections. Those who abstained were asked for their opinions and the consensus was that they wished to have more detail before making a decision.

It was proposed that a working group should be formed to develop a proposal before the next meeting. This was agreed and Serge Droz, Lionel Ferette, Przemek Jaroszewski, Baiba Kaskina, Jacques Schuurman, Don Stikvoort, Erika Stockinger, Toomas Lepik and Wilfried Woeber volunteered to participate in this. Kevin was then asked whether he could produce an initial draft for discussion.

Action 33.2 – Kevin Meynell to draft proposal for new TF-CSIRT group and circulate to TF-CSIRTng Working Group.

The issue of meeting costs was also raised, and whether there were plans to introduce registration fees or cover the costs of these in some other way. Kevin replied that the size of the meetings and expectations of facilities meant it had become more difficult to find organisations willing to host. This was especially the case with the Joint FIRST/TF-CSIRT event which was now attracting 150 or more participants.

At the present time, the plan was to try to keep meetings free and there were probably enough hosts for the next couple of years. Some small charge would probably need to be made for the next FIRST/TF-CSIRT event as this was being organised by TERENA (with logistical help from GARR), but this would be on a strict cost recovery basis.

12. Date of next meeting

Lionel Ferette thanked Jumper CSIRT for hosting TF-CSIRT in Malahide.

The next meeting will be held on 22-23 September 2011 in Luxembourg City, Luxembourg (hosted by RESTENA-CSIRT and CIRCL).

The following meeting was planned to be a Joint FIRST/TF-CSIRT Technical Colloquium. It would probably be held on 30 January – 1 February 2012 in Rome, Italy; although this still needed to be confirmed.

Open Actions

- 31.1 TI Review Board to discuss how to deal with Spamhaus problems and what further action to take.
- 32.2 Marco Thorbrügge to send pointer to information about Article 13a to the mailing list.
- 33.1 Serge Droz to invite CENTR to participate in TF-CSIRT meeting in Luxembourg.
- 33.2 Kevin Meynell to draft proposal for new TF-CSIRT group and circulate to TF-CSIRTng Working Group

SUBJECT

Approved minutes of the 33rd TF-CSIRT meeting
2 June 2011, Malahide, Ireland

Participants

<i>Name</i>	<i>Organisation</i>	<i>Country</i>
Shehzad Ahmed	DK-CERT (UNI-C)	Denmark
Mateo Araque	CCN-CERT	Spain
Kristian Borryd	CERT-SE	Sweden
Matej Breznik	SI-CERT (ARNES)	Slovenia
Aidan Carty	HEAnet	Ireland
Jorge Chinaea	INTECO-CERT	Spain
Ian Cook	Team Cymru	United Kingdom
Andrew Cormack	JANET(UK)	United Kingdom
Michelle Danho	CERT-RENATER	France
James Davis	JANET CSIRT	United Kingdom
Serge Droz	SWITCH-CERT	Switzerland
Shane Duigan	Jumper CSIRT	Ireland
Lionel Ferette (Chair)	-	Belgium
Umberto Grigolini	Jumper CSIRT	Ireland
Tomasz Grudziecki	CERT Polska (NASK)	Poland
Tilman Haak	DFN-CERT	Germany
Mikko Halin	CERT-FI (FICORA)	Finland
Michael Hanna	IRISSCERT	Ireland
Brian Honan	IRISSCERT	Ireland
Kauto Huopio	CERT-FI (FICORA)	Finland
Przemek Jaroszewski	CERT Polska (NASK)	Poland
Sigitas Jurkevicius	CERT-LT	Lithuania
Baiba Kaskina	CERT.LV	Latvia
Andrea Kropacova	CZ.NIC	Czech Republic
Toomas Lepik	CERT-EE	Estonia
Antonio Liu	Trusted Introducer	Germany
Peter Magula	CSIRT.SK	Slovakia
Chelo Malagon	RedIRIS	Spain
Branko Mazar	CARNet	Croatia
Kristians Melins	CERT.LV	Latvia
Stephen Meyer	Jumper CSIRT	Ireland
Kevin Meynell (Secretary)	TERENA	-
Dave Monnier	Team Cymru	United States
Thomas Nguyen Van	Jumper	Ireland
Triin Nigul	CERT-EE	Estonia
Theodoros Nikolakopoulos	Jumper CSIRT	Ireland
Tomasz Nowocień	PIONIER-CERT	Poland
Patrick O'Callaghan	Unity	Ireland
André Oosterwijk	GOVCERT.NL	The Netherlands
Maurice Paudice	Erika C & T	Italy
Martin Peterka	CZ.NIC	Czech Republic
Leila Pohjolainen	FUNET CERT	Finland
Timo Porjamo	FUNET CERT	Finland
Juan Quintanilla	DANTE	-
Margrete Raaum	UiO-CERT	Norway
Dennis Rand	DK-CERT (UNI-C)	Denmark
Daniel Röthlisberger	SWITCH	Switzerland
Wayne Routly	DANTE	-
Jorge Ruão Pinheiro	Universidade do Porto	Portugal
Sandra Salán	INTECO-CERT	Spain
Jacques Schuurman	XS4ALL Internet	The Netherlands
Derek Simpson	BT	United Kingdom
Jan Soukal	CSIRT-MU	Czech Republic

SUBJECT

Approved minutes of the 33rd TF-CSIRT meeting
2 June 2011, Malahide, Ireland

Don Stikvoort	S-CURE	The Netherlands
Erika Stockinger	CERT-SE	Sweden
Marius Urkis	LITNET CERT	Lithuania
Christian Van Heurck	BELNET CERT	Belgium
Han Van Thoor	Jumper CSIRT	Ireland
Tito Vieira	Universidade do Porto	Portugal
Srdjan Vukovojac	CARNet	Croatia
Jan Vykopal	CSIRT-MU	Czech Republic
Wilfried Wöber	ACOnet-CERT	Austria
Bente Christine Åsgård	UiO-CERT	Norway

Apologies were received from:

Mikael Ganev	RU-CERT	Russia
Vincent Hinderer	CERT-LEXSI	France
Klaus-Peter Kossakowski	PRESECURE	Germany
Stelios Maistros	GRNET-CERT	Greece
Marc Stiefer	RESTENA CSIRT	Luxembourg
Thomas Stridh	SUNET CERT	Sweden