Minutes of 40th TF-CISRT Meeting
26th – 27th September 2013
London, United Kingdom.
The meeting was hosted by BT.

Table of Contents

1. Welcome and Apologies

Lionel Ferette welcomed attendees to the open session of the 40th meeting of TF-CSIRT. Apologies were received from Matthew Cook (Janet ESISS), Serge Droz (SWITCH), Mikhail Ganev (RU-CERT), Andre Oosterwijk (NCSC-NL), and Margrete Raum (UiO-CERT).

2. Approval of Agenda

The agenda was approved as circulated.

3. Minutes of Last Meeting and Update of Action List

- Minutes

The minutes of the last meeting were approved as circulated.

- Actions from Previous Meetings

Reference	Who	Action	Status
20130523-01	Nicole Harris	Circulate the revised terms of reference and ask Full Members to vote on its acceptance.	Closed – action complete
20130523-02	Don Stikvoort	Circulate Alerts, Warnings and Announcements Survey to the TF-CSIRT list.	Closed – action complete
20130523-03	Don Stikvoort	Circulate classification documentation to the TF-CSIRT list.	Closed – action complete
20130523-04	Nicole Harris	Coordinate a 'test run' of the Security Monitoring working group for the September 2013 meeting.	Closed – action complete

4. Update from CERT Hungary - Tamás Gyebrovszki

Hungary has gone through significant changes in terms of government structure and ministry management. CERT Hungary has been re-established under a new department with a new legal structure. Although the name for CERT Hungary remains the same, the group members have changed. As such CERT Hungary will need to go through accreditation once more.

CERT-Estonia commented that is a similar process is underway in Estonia. Dave Parker from Bournemouth University asked if this was connected to the ENISA changes or if it was a national issue. Tamás replied that it was a specific reaction to cyber security issues within Hungary.

5. Team Cymru Update – Ian Cook

Ian gave an overview of useful monitoring tools currently being used by Team Cymru. Tools and sites recommended are:

- Website Watcher: a simple RSS feed reader.
- Feed Demon: has RSS reader abilities but allows you to have an active watch on keywords.
- Copernic Agent: metdata search agent.
- Twendy: monitors twitter feeds for security professionals.
- The Tweeted Times: aggregates twitter streams that have been flagged for monitoring and creates newspapers.
- Paper.li: processes mored than 250 million social media posts, extracting and analysing articles.
- News Now: news aggregation services, but very UK centric.
- CERT-LatestNews: specific RSS feed.
- CyberWire: **www.thecyberwire.com**. Top security stories.
- SILOBreaker: news.silobreaker.com.
- News360 for the iPad: news360.com.
- Prismatic for the iPad: learns what you like and tailors information.
- Pulse for the iPad: **www.pulse.me**.
- Copernic Summarizer: creates concise documents summaries of any text files or web page.

Twitter has really changed the experience of searching for information and it has focused attention on trending topics. The removal of RSS feeds from twitter.

Members of the audience recommended Taranis as a useful tool: **http://www.govcert.nl/english/service-provision/ICT+risk+alert/taranis**. There was an attempt to make it open source but this has currently stalled.

6. Recent and Upcoming Developments - ICANN47 and RIPE67. Wilfred Woeber.

"whois" currently has no precise definition. There are some old RFCs but they do not contain enough information concerning syntax, semantics or schemas. ICANN is now permitting a change in domain names and how they can be used worldwide. ICANN has a set of commitments describing responsibilities and mandatory review and the effectiveness and implementation of commitments for "whois" are now under review. 2 reports from this group have been made available proposing some changes – including the establishment of an Expert Working Group with a broad overview for "whois". Some of the recommendations from the group are:

- Adoption of new language and concept for registration data and directory services when a domain is registered.
- Focus on changes for new gTLDs becoming operational soon.
- Ongoing conversation around privacy of data for who registers domains and why / when data might be kept private.

Areas that are still unclear in relation to this group:

- (Possible) alignment with IRTF's WEIRDS working group?
- Proposal to require a central data repository? This is a very controversial topic, with questions of political control, data protection, legal registration etc.
- Concept of 'profiles' for access to registration data – what might this definition be? Resellers? Marketing? Governments? Security teams? Law enforcement? Will this access be monetised?

Similar issues exist for the Numbers Registry. Traditionally this was ASCII as default, but there are no semantics for signalling code tables, causing problems when using Latin, Cyrillic, Greek etc. RIPE66 initiated an action to investigate the software system for the Numbers Registry, including user interfaces and APIs. This will in turn create the need for new policy processes to be put in place. This should be addressed in the working group agenda for the next RIPE meeting in Athens (specifically the Database WG and Services WG). Wilfred also recommended following the WEIRDS WG in IETF.

Andrew Cormack commented that ICANN have just issued a report on privacy and proxy services for domain registrations, which suggested that all uses of such services were inappropriate. This does not reflect the reality of how these services are used.

7. Trusted Introducer. Klaus-Peter Kossakowski.

Klaus-Peter gave an update on the membership of Trusted Introducer, noting that TI is nearly close to 200 listed teams. A current trend sees a significant increase in the number of government CERTS joining, as well as more commercial CERTS. NREN numbers are stabilising as most research and education CERTS are now members. 4 new members have been accredited since the last meeting: CERT-EU, COSDEF-CERT, Panasonic PSIRT and Malware.lu. UNINETT CERT and CERT.PT are currently candidates for certification.

The website has been updated, and TI are asking teams to help them put information up in native languages for each CERT. TI has provided a template to make this possible and is asking CERTS to help with this translation. TI are also now publishing events of interest on the TI website – these should have a broad level of interest beyond a national focus. An encrypted IRC server is also being introduced to support collaboration between teams.

TI is also looking to provide X.509 certificates to all listed teams as well as accredited teams to help with the distribution of information and ease of use of the TI website.

8. Transits Update. Don Stikvoort.

The TRANSITS team is considering introducing more exercises to the TRANSITS courses. Both TRANSITS models use the ENISA exercises to support role-play scenarios. All of the models have recently be renewed to ensure they remain relevant.

TERENA and FIRST have recently signed a new MoU for TRANSITS materials use outside of Europe. The aim of TRANSITS is to be used as widely as possible and further

9. 4GH. Don Stikvoort.

4GH is an event for hard-core technical people. It is a trusted meeting of peers to allow people to talk openly. Everyone comes 'armed' with issues for discussion and anyone can be chosen to talk at the event. The next meeting will be 8th – 10th November 2013 in Egmond aa Zee in the Netherlands. The website is: http://www.4gh-con.org.

10. Sharing Data / Information – Ian Bryant

Ian started by explaining the D - I – K – W principle (data, information, knowledge, wisdom). TF-CSIRT has always had an interest in data and information sharing, including the IODEF (Incident Object Description Exchange Framework) which moved in to the IETF as well as the Request Tracker for Incident Response (RT-IR).

Ian works for the UK Trustworthy Software Initiative (TSI), which aims to improve the quality and trustworthiness of software outputs. TSI focus on looking at issues around safety, reliability, availability, resilience, and security. Software problems are high cost to the economy – a NIST study indicated that around $60 billion a year was lost due to software problems. Ian state d that most principles and techniques needed for Trustworthy Software have existed for many years, we just need to get people to use them – with a specific focus on due diligence.

TSI have a Trustworthy Software Framework structure that they use to help focus practise in software development. This helps describe standards and processes in a logical and understandable way and then links through to a repository of information from standards bodies. Ian went on to describe a 'bowtie lifecycle', showing proactive treatment vs reactive measures around events.

One of the biggest challenges is sharing information across boundaries – including language and protocol barriers. Communities are not necessarily aligned to natural circles of trust and communities may not share either a common language or processes. By creating "boundary objects" we can define mutually recognised means of sharing information.

Ian recommended ISO/IEC 27010:2012 Information Security Management of inter-sector and inter-organisational communications" as a useful resource for standardisation of data sharing processes. This helps to rationalise the many different data sharing formats that are available (currently over 50 different frameworks and formats).

Multinational Alliance for Collaborative Cyber Situation Awareness (MACCSA) are creating an Information Sharing Framework with an aim to increase organisations cyber situational awareness enabled by sharing information across a trusted community of interest. This may be an initiative work tracking.

11. Shibboleth / Single Sign On with/out Single Sign Off. Alexander Talos-Zens

Alexander started with an overview of Aconet's progression and use of SSO. This is base around SAML2 and is widely deployed in Austria. One of the main complaints that has been

received from users is the lack of a logout button for the services using the Aconet federation.

Alexander pointed out that this was not something that had been overlooked, but was a problem with the way that web browsers currently handle sessions. It is almost impossible to truly implement single logout due to these issues, so the only possible approach is to consider a partial logout approach, but this in itself is greatly problematic for the user.

Aconet are looking to implement logout where feasible, and to provide clear user instructions for both possible logout and where not available. This includes warnings where users are on public computers.

12. Voting on new ToR and Steering Committee Members

Nicole outlined the minor changes made to the ToR to make them easier to read and more specific in terms of relationship between membership of TI and TF-CSIRT. Members voted to ACCEPT the changes by simple majority.

ACTION 20130926-01: Nicole Harris to implement the new ToR on the TERENA website.

Lionel Ferette explained that under the new Terms of Reference 2 members of the Steering Committee were being replaced at this meeting. There were 3 candidates for election: Wilfried Woeber, Baiba Kaskina and James Davis.

In the first ballot, Baiba Kaskina was elected to the Steering Committee. In the second ballot, Wilfried Woeber was elected to the Steering Committee.

13. NREN and ISP Security Working Group Report – Wayne Routly

Wayne presented an overview of the work undertaken by DANTE to focus on security audit via the NREN and ISP security working group. The group is trying to focus on credible future threats and hardening infrastructure in response. This includes working with commercial ISPs, external security specialists and involving groups such as ENISA to ensure that a broader picture than research and education is take in to account.

The core recommendations from the group are:

- To implement a firewall filer review process.
- To develop a service approach policy for BYOD.
- To develop a cloud services policy.
- To perform stress test on security systems.
- To perform targeted pen testing of critical systems.
- To perform annual security exercises.
- Review staffing levels / notification mechanism for staff leaving organisation.
- Implement Privacy Officer role.

14. Presentation on BT and the London Olympics. Mark Hughes.

Mark gave an overview of the measures that BT had to put in place to manage the threats

associated with providing the right support for the Olympics. This included over 80,000 connections over 94 locations in London. During the games itself, there were over 800 working on the ground to support the venues. BT were supporting the broadcast, voice and data networks as a digital hub – this was the first time this had been attempted at an Olympic event. During the games, london2012.com was the fifth busiest website in the world.

Support requirements had changed significantly. During Beijing, the iPad was not yet available demonstrating how quickly support requirements change. Rehearsals and 'war-games' prior to the event were key to the planning, but also BT had to deal with many temporary venues that only were only constructed at the last minute.

BT spent a lot of time working with other organisations in London to help them understand possible changes and threats due to the games and possible knock-on impacts. A key tool to support this was a list of 10 questions to use when assessing corporate risk. However most of the tools they used to help monitor and track were simplistic – twitter, IRC etc.

During the games there was at least 2 hacktivist campaign each day. On london2012.com there were over 11,000 malicious requests per second. On 'super Saturday' over 128 million events were detected. One of the main issues was dealing with journalists with their own devices using the games infrastructure.

The legacy is a new operational team at BT with core responsibility for protecting the network and systems from cyber attacks.

Andrew Cormack asked if there was impact on domestic broadband due to people being encouraged to stay home during the Olympics. There was a notable increase but this was built in to the planning. The real impact area was on streaming as events were being watched.

Andrew followed this up by asking if there was a fade in interest after the Olympics were over. The ongoing media attention and coverage of security attacks is actually doing a good job of keeping issues present on the agenda of senior management.

Wayne Routly asked what was the most significant lesson learnt from the experience. Mark replied that reliance on the skills and analytical abilities of staff supported by the right procedures was the most important factor. There is a skills shortage in this area.

David Byers asked if BT would be involved in Rio to pass on the experience gained. Mark confirmed that they were.

15. CERT la Poste Update. Frederic Le Bastard.

Le Groupe La Poste is one of the largest retail groups in France, with 17,000 points of sale across France. The group provides post and parcel delivery but is also a retail bank. The CERT's main role is surveillance and anticipation for security events. The team was put in place in 2008 after a massive worm infection. The team has been listed in TI since March 2012 and they are working towards accreditation.

Services that the CERT provide includes an internal security supervision service (SISO) across

the company – this monitors things like ensuring security patches are up to date. They also provide advice on legal requirements as well as focusing on internal infosec policies. They have some specific watch activities based on known issues and points of threat – particularly banking phishing. The team is also mapping the group's websites on the Internet so that they have a clear inventory of exposed websites.

CERT La Poste have created an internal tool called Malware Trap. The tool uses proxy logs and other trusted repositories to build up information. The trap redirects malicious domains to a different IP address. Automated scripts are then used to run antivirus software. The tool has reduced the number of compromised endpoints from 3000 to 50. Problems with this approach include the difficulties of performing automated semantic analysis of FQDNs and the fact the automated updates of internal DNS zones makes people nervous.

Alexander Talos-Zens asked if they provide support to end-users. This is typically passed back to the business units across the group. Although the CERT rarely gets feedback on how the issues are dealt with, monitoring allows them to see when the problem is resolved.

16. Update from JANET. James Davis.

James Davis gave an update on changes at Janet. Janet has now taken over the Education Shared Information Security Service to create Janet ESISS. ESISS has therefore been removed from Trusted Introducer. ESISS focus on manual penetration testing, vulnerability assessment and bespoke consultancy. The only real change has been to the branding, customer base and sales structure. Future developments include investigation around PCI services and collaborations with other NRENs.

17. Update from LiU IRT. David Byers.

David Byers introduced LiU IRT from Sweden: https://www.trusted-introducer.org/directory/teams/liu-irt.html. The unit is part of Networks, IRT and telephony at Linkoping University. The team's activities include blocking malware-infested computers, blocking open resolvers, managing firewall rule-sets, providing advice for procurements, and formulating security policy.

Jan Vykopal asked how many incidents LiU IRT handle per month. David replied that they do not handle very many, the focus. Wayne Routly asked about the relationship with the university audit team. This relationship is still evolving. The team is working on a regular audit process to be undertaken by the university audit team.

18. Update from LITNET CERT. Patrikas Kugrinas

Patrikas gave an update on LITNET CERT. LITNET is the academic research network in Lithuania. The team works on behalf of all the universities support by LITNET. Main work areas include investigation and coordination across the connected organisations.

Malware is the most common incident dealt with followed by spam cases. Crime and compromise cases are low.

A recent project included combining NFSen (a netflow sensor) and Hadoop to improve workflow

for the team. The code is available on github – see Patrikas slides for details. The team is also using AbuseHelper to help support automated incident notification.

Jan Vykopal asked Patrikas to attend the Network Security Monitoring WG meetings.

19. Poste Italiane CERT: strategy, mission and services. Stefano Grassi.

Poste Italiane CERT is exploring an integrated approach to cyber security and aim to take a leadership role in CERT activities in Italy. Post Italiane is a very large organisation within Italy and like La Poste it is involved in financial activities and digital communications as well as traditional logistics and postal operations.

Poste Italiane CERT is responding to EU Cyber Security Strategy and the proposed NIS directive alongside the strategy of the Italian government who have developed a new remit for cyber security issues. The team is working towards TI accreditation.

The team have an early warning service that aims to provide alerts to the PI CERT community. It provides information gathering, analysis and vulnerability alert functionality. This is supported by information sharing activities reporting on threat intelligence and incident investigation via a communication centre.

Post Italiane CERT are working with the Italian Ministry of Economic Development to support the set-up of an Italian National CERT.

20. Date of Next Meeting, AOB and Close

The next meeting will be in Switzerland in January 2014.

The attendees thanked BT and Martin Hathaway for hosting the meeting.

Action List

Reference	Who	Action	Status
20130926-01	NH	Implement the new ToR on the TERENA website	Initiated.

List of Participants

First Name	Last Name	Organisation
Aaron	Kaplan	CERT.at
Adam	Smutnicki	WCNS/EGI CSIRT
Aleksandre	Varadanidze	DATA EXCHANGE AGANCY
Alexander	Talos-Zens	ACOnet-CERT / Univie
Andrea	Kropacova	CESNET

Andrea	Dufkova	ENISA
Andrea	Volponi	PI-CERT
Andrew	Cormack	Janet
Anto	Veldre	CERT-EE/EISA
Baiba	Kaskina	CERT.LV
Bob	van der Kamp	NCSC-NL
Chelo	Malagon	IRIS-CERT
Claudio	Allocchio	GARR
Colin	Tomlinson	Trusted Introducer
Cynthia	Wagner	RESTENA Foundation
Daniel	Roethlisberger	SWITCH
Dave	Monnier	Team Cymru
David	Byers	LiU IRT
David	Willems	NCSC
David	Kvatadze	LEPL Data Exchange Agency (CERT-GOV-GE)
David	Parker	BU-CSIRT Bournemouth University
Don	Stikvoort	Trusted Introducer
Erika	Stockinger	CERT-SE
Frederic	Le Bastard	CERT La Poste
Gaus	Rajnovic	Panasonic
Goran	Culjak	ZSIS
Gorazd	Bozic	SI-CERT
Hillar	Leoste	Consilium of the European Union
Huw	Langford	BTCERTCC
Ian	Cook	Team Cymru
Ian	Bryant	UK TSI
Ingo	Chao	XING
Irakli	Lomidze	DEA (CERT.GOV.GE)
Jacques	Schuurman	XS4ALL
James	Davis	Janet
Jan	Vykopal	CSIRT-MU
Jean-Paul	Weber	GOVCERT.LU
Juan	Quintanilla	DANTE
Klaus-Peter	Kossakowski	Trusted Introducer

Lionel	Ferette	TF-CSIRT
Marc	Stiefer	Restena-CSIRT
Martin	Hathaway	BT
Martynas	Gintalas	SVDPT-CERT
Mateo	Araque	CCN-CERT
Matthias	Fraidl	CERT.at
Michael	Nowlan	TERENA
Michael	Dwucet	CERT-Bund (BSI)
Michael	Hausding	SWITCH
Miklos	Kiss	GovCERT-Hungary
Milda	Mimiene	LITNET CERT
Morten	Schioenning	TeliaSonera
Nicole	Harris	TERENA
Nelson	Cheuque	TeliaSonera
Noel	Comerford	IRISSCERT
Ossi	Kuosmanen	Funet CERT
Otto	Makela	Funet CERT
Paata	Sirbiladze	LEPL Data Ecchange Agency, Ministry of Justice
Patrick	Houtsch	GOVCERT.LU
Patrikas	Kugrinas	LITNET CERT
Pavel	Basta	CSIRT.CZ
Petra	Hochmannova	CSIRT.SK
Przemek	Jaroszewski	CERT Polska/NASK
Radim	Ostadal	GovCERT.CZ
Raphael	Vinot	CIRCL - National CERT Luxembourg
Rocco	Mammoliti	POSTE ITALIANE
Shehzad	Ahmad	DKCERT (DTU)
Simona	Venuti	GARR-CERT
Stefano	Grassi	POSTE ITALIANE
Sven	Gabriel	Nikhef/EGI CSIRT
Tamas	Gyebrovszki	GovCERT-Hungary
Thomas	Schreck	Siemens CERT
Tilmann	Haak	XING
Tomas	Lima	FCCN - CERT.PT

Tomasz	Nowocien	PionierCERT/PSNC
Toomas	Lepik	CERT-EE/EISA
Torsten	Voss	DFN-CERT Services GmbH
Ulrik	Haugen	LIU IRT
Wayne	Routly	DANTE
Wilfried	Woeber	UniVie / ACOnet-CERT
Alex	Zaharis	GRNET-CERT