



Report on Fifth Training Workshop

IST-2001-39118

Training of Network Security Incident Teams Staff

TRANSITS



Deliverable no. D9

Project Manager: Karel Vietsch

TERENA, Singel 468 D, 1017 AW Amsterdam, The Netherlands

Phone : +31 20 5304488
Fax: +31 20 5304499
Email: vietsch@terena.nl

Date: 24 November 2004

CONTENTS

Executive Summary	3
1. Workshop Objectives and Background	3
2. Workshop Preparations	4
2.1. Selection of Venue	4
2.2. Choice of Presenters	5
2.3. Workshop Announcements and Selection of Participants	5
2.4. Financial Arrangements	6
2.5. Workshop Materials	6
3. Workshop Delivery	7
3.1. Participants	7
3.2. Programme	8
3.3. Experiences of Presenters and Trainees	10
3.4. Results from Feedback Forms	11
4. Actions Arising	12

Annex I

Fifth TRANSITS Training Workshop materials

Executive Summary

The fifth TRANSITS training workshop was held at the Parkhotel in Průhonice near Prague, Czech Republic on November 11th and 12th, 2004. As with the previous workshops, a mailing list for the participants has been set up to help them communicate with each other in future. Students were a mix of members of existing CSIRTs whose colleagues had attended previous TRANSITS training workshops, members of new CSIRTs to whom the course had been personally recommended by national or international peers, and staff members from organisations that had received calling notices for the workshop through various mailing lists. The TRANSITS project therefore seems to be achieving its aims of both supporting the existing CSIRT community and expanding the CSIRT model into new organisations and countries.

The fifth TRANSITS workshop was very much oversubscribed, with more than 40 applications while the nature and structure of the course limit participation to two groups of about ten trainees. In the end it was decided to admit 23 trainees, thereby stretching the capacity of the venue to its limit. Besides the number of applications for this workshop, also other signals from the CSIRT community indicate that there is a substantial interest among new and existing European CSIRTs to send their staff to TRANSITS training courses. This raises the question how to meet these needs in the year 2005, and how to proceed after the end of the TRANSITS project.

Compared to earlier training courses, an extra session was added to the workshop programme, where students worked together in groups to address a scenario exercise. This was highly successful.

1. Workshop Objectives and Background

Increasing the proportion of European networks that have Computer Security Incident Response Team (CSIRT) services is a major part of improving the dependability of networks and promoting public confidence in the Internet. The objective of the TRANSITS project is to promote the creation of more, professional CSIRTs and the strengthening of existing CSIRTs.

Operating a CSIRT takes rare and specialist skills; currently there are only a few hundred experts in Europe who have the necessary knowledge and experience. The TRANSITS project addresses this problem by providing specialist training to staff members of new CSIRTs and new staff members of existing CSIRTs.

Before the start of the TRANSITS project, course materials had already been prepared, but these need to be edited, maintained and updated during the lifetime of the project. A try-out presentation of the course was made in January 2002 in a workshop hosted by Telia at its headquarters in Farsta near Stockholm, Sweden. After the start of the TRANSITS project in July 2002, the earlier material and the feedback from the try-out presentation of the course were taken as inputs for preparing the first edition of the course material. That work was completed in September 2002, and the result was submitted to the European Commission as TRANSITS deliverable no. D1. A major review of the course material was carried out early in

2004, which led to significant changes to all modules. This second edition of the course material was submitted to the European Commission in March 2004 as deliverable no. D6.

During the lifetime of the TRANSITS project the course materials will be presented six times, and it is intended to spread the locations of these six training workshops over various regions in Europe. The first training workshop took place in Oegstgeest, the Netherlands, on October 31st and November 1st, 2002 and was reported on in TRANSITS deliverable no. D2. The second TRANSITS workshop was held in Warsaw, Poland, on May 27th and 28th, 2003 and was reported on in deliverable no. D3. The third workshop was held on October 30th and 31st, 2003 in San Gaudenzio near Milan, Italy and was reported on in deliverable no. D5. The fourth training workshop took place in Hamburg, Germany on May 25th and 26th, 2004 and was reported on in deliverable no. D7. The present deliverable reports on the preparations for, and the delivery of the fifth training workshop. The course was presented using the latest version of the TRANSITS materials.

2. Workshop Preparations

The training workshop required careful preparations. The two TRANSITS project partners, TERENA (the Trans-European Research and Education Networking Association) and UKERNA (the United Kingdom Education and Research Networking Association), were both involved in this. TERENA's Karel Vietsch took responsibility for identifying a suitable location, arranging accommodation and arranging financial support to trainees if needed. UKERNA's Andrew Cormack took charge of ensuring the availability of teachers and preparing the contents of the workshop materials. The course was advertised jointly by both organisations, and Andrew Cormack and Karel Vietsch together took responsibility for the selection of trainees, asking for the advice of prominent members of TERENA's task force TF-CSIRT when needed. TERENA staff took care of having the printed workshop materials produced. TERENA's Karel Vietsch and Carol de Groot installed Internet connectivity at the workshop venue.

2.1. Selection of Venue

In view of the intention to spread the locations of the six TRANSITS training workshops over various regions in Europe, it was decided to hold the fifth workshop in Central/Eastern Europe.

Criteria for the selection of the venue included:

- A location at a reasonable travel distance from a major international airport. Many of the workshop participants have busy diaries and it was felt to be important to keep travel time as limited as possible.
- A secluded venue with the necessary meeting rooms, hotel rooms and facilities for meals in one location. Since the training benefits strongly from personal interactions, also outside the formal sessions, it is important to make intensive use of the 50 hours that trainees and lecturers are together.
- Moderately priced accommodation. While room hire, meals for workshop participants and travel and subsistence costs of the lecturers are paid by the TRANSITS project, trainees

are expected to cover their own travel and hotel costs. Some of their employers are not-for-profit organisations with limited means.

The Parkhotel in Průhonice met all these requirements. Staff members from CESNET, the national research and education networking organisation in the Czech Republic, volunteered to provide assistance in making the necessary arrangements.

2.2. Choice of Presenters

Lecturers were recruited from the most experienced staff members and former staff members of major professional CSIRTs. A number of members of task force TF-CSIRT have committed themselves to contribute to the TRANSITS materials and to act as teachers of course modules at a number of the training workshops. Some of the available volunteers had been co-authors of the original training course materials and/or had presented at the try-out workshop in January 2002 or the first four TRANSITS training courses.

It was therefore not difficult to find a sufficient number of very well qualified presenters. The following team was chosen:

Andrew Cormack	UKERNA	United Kingdom
Klaus Möller	DFN-CERT	Germany
Claudia Natanson	Diageo	United Kingdom
David Parker	UNIRAS	United Kingdom
Jacques Schuurman	SURFnet-CERT	Netherlands

2.3. Workshop Announcements and Selection of Participants

On September 1st, 2004 the announcement of the training workshop was published on the TRANSITS website (www.ist-transits.org). This announcement contained a course summary, an explanation of the pre-requisites, information about the time and venue and the costs, and instructions on how to apply for participation. At the same time the announcement was sent via the appropriate mailings lists to the members of TF-CSIRT, the FIRST membership and the research and education networking organisations in Europe (the TERENA membership). Five additional mailing list were used to spread the announcement: a general TRANSITS announcement list to which any interested person can subscribe to receive TRANSITS news (see www.ist-transits.org/maillinglist.php), and the mailing lists of participants in the first, second, third and fourth TRANSITS workshops. Reminders were sent to the same communities on September 27th. The workshop was also promoted with much emphasis in a meeting of TF-CSIRT on September 24th.

The following time schedule was mentioned in the workshop announcements:

1 October 2004	Deadline for sending in applications
11 October 2004	Applicants will be notified whether a place has been reserved for them at the workshop
28 October 2004	Deadline for payment of the accommodation costs and the registration fee.

Eventually, 40 applications were received before the deadline, and a number of further enquiries were received soon afterwards. This posed a substantial problem, because the workshop was planned to accommodate two groups of ten trainees. The nature and structure of the course did not allow raising these numbers significantly, nor did the limitations of the workshop venue. In the end it was decided to accept 23 applications, thereby stretching the capacity of the venue to its limit.

In the selection that had to be made, the following criteria played an important role:

- priority for applicants from CSIRTs that were just now in the process of being established, because at that point in a CSIRT's history the TRANSITS knowledge is extra valuable to enable the CSIRT to have a good start;
- priority for applicants from CSIRTs from which no other team members attended a TRANSITS training course before, because there is an additional value in spreading the TRANSITS knowledge to CSIRTs in which that knowledge has not been spread before;
- priority for applicants from Central/Eastern Europe because it would be easier/cheaper for them to travel to Prague than to the venue of the next TRANSITS workshop, which would be in Western Europe.

Other applicants who scored high but did not rank among the top-23 were promised a guaranteed place at the next TRANSITS workshop if they would apply again then.

2.4. Financial Arrangements

As described in the TRANSITS project workplan, all trainees were expected to pay their own accommodation costs as well as a (symbolic) fee of 100 euro. Participants were asked to pay these sums to TERENA no later than fourteen days before the event. This arrangement not only simplified financial administration, but it also reduced the risk of no-shows.

Within the TRANSITS budget, TERENA manages funds to cover part of the participation costs of training workshop participants from economically less-developed countries in Europe. This financial support will always cover only part of the total costs of these participants and will be limited to trainees from non-commercial, non-profit organisations. Six of the participants in the fifth TRANSITS workshop applied for reimbursement of part of their costs from these funds.

Within the TRANSITS budget, UKERNA manages funds to cover the travel and subsistence expenses of the lecturers who are not UKERNA or TERENA employees. These costs will be reimbursed after the event on the basis of invoices sent by the presenters to UKERNA.

2.5. Workshop Materials

The course was presented using the latest version of the TRANSITS materials. Participants received a workshop pack containing printed copies of the slides, exercises and supporting documentation. Digital copies of these materials were provided on the workshop CD-ROM, which also included the CSIRT Handbook (with thanks to the copyright holders, Carnegie Mellon University) and a paper on Incident Response made freely available by the US

National Institute for Standards and Technology (NIST). This includes a number of incident response scenarios, one of which was used for the Friday evening session. The CD-ROM also contained RFCs relevant to CSIRT work. Each participant pack also included a copy of the book *Incident Response* by Kenneth R. van Wyk and Richard Forno (published by O'Reilly & Associates, Inc.) and a Guidance Note on writing advisories published by UKERNA.

One week before the event the workshop materials were shipped to the CESNET offices in Prague, and from there they were transported to the workshop venue by TERENA staff.

3. Workshop Delivery

3.1. Participants

Twenty-three trainees attended the course, from thirteen countries:

Victor Barahona	Universidad Autónoma de Madrid	Spain
Martin Camilleri	mtCERT	Malta
Janos Drencsan	CERT Hungary	Hungary
Renato Ettisberger	SWITCH CERT	Switzerland
Katalin Ganzler	NIIF-CSIRT	Hungary
Stefan Grinneby	SITIC	Sweden
Tadej Hren	SI-CERT	Slovenia
Andrius Kiaune	State Security Department	Lithuania
Holger van Lengerich	Telefónica Deutschland	Germany
Jakub Mer	CESNET	Czech Republic
Sergey Nazinyan	AmCERT	Armenia
Ian Neilson	CERN	Switzerland
Luis Padilla	Universidad Complutense de Madrid	Spain
Hubert Pilarski	Polkomtel	Poland
Simon Portelli	University of Malta	Malta
Sharon Sciberras	mtCERT	Malta
Erika Stockinger	SITIC	Sweden
Robert Sultana	University of Malta	Malta
Balazs Szekeres	CERT Hungary	Hungary
Antti Tassberg	Nokia Corporate Security	Finland
Vladimir Třeštík	CESNET	Czech Republic
Pavel Vachek	CESNET	Czech Republic
Wilfried Wöber	ACOnet CERT	Austria

Of these trainees, eleven work for existing CSIRTs and twelve were from organisations that are in the process of creating a new CSIRT. Nine of these organisations had not participated in European CSIRT activities before. The majority of the CSIRTs represented are associated with research and education, but three commercial organisations and four government organisations were represented.

The presenters came from the education, government and commercial sectors and had more than 30 years of CSIRT experience between them.

3.2. Programme

The objectives of the training workshop were:

- to understand where CSIRTs fit into the organisation
- to understand the tasks and tools that are necessary to perform their function
- to develop and practice the skills that are needed by a CSIRT team member
- to understand the external issues (both legal and technical) that may effect the operation of a CSIRT.

The course consisted of five modules. Some of these included exercises that the trainees had to complete and discuss, while others included time for discussion among the whole class.

The modules were:

- **CSIRT Organisation**

Describes how CSIRTs fit into their organisations; planning the CSIRT, defining the constituency of the team and gaining management authority for it, deciding the services the team will offer, working with those outside the organisation, staffing the CSIRT, funding. Trainees discussed their own organisation and how their team fits into it.

- **Technical Aspects**

Understanding how intruders attack systems; intruders and their motivations, network protocols and how they can be abused, operating systems and services, types of vulnerability, information gathering, breaking in, hiding traces, denial-of-service attacks. A number of exercises were used to show how these appear in practice.

- **CSIRT Operations**

Describes the facilities, systems and tools needed by CSIRTs to operate successfully; housing the CSIRT, equipment, e-mail, remote access, information and contacts, servers and networks, incident response plans and procedures, tracking systems. As an exercise trainees discussed and developed incident response plans for their own teams.

- **Legal Issues**

Looks at the areas of legislation that are likely to affect CSIRTs in their work and that team members need to be aware of; origins of computer legislation, problems, data protection, computer misuse, working with law enforcement, monitoring, evidence, European developments.

- **Working with Vulnerabilities**

Discusses the roles that CSIRTs may decide to play in distributing and producing information about vulnerabilities; why do vulnerabilities exist, what should CSIRTs aim to do, sources of information and how to use them, advisories – distribution, interpretation, investigation and co-ordination.

The modules were presented in parallel in two groups. In order to encourage interaction with participants not known to them earlier, trainees were divided over these groups such that if possible people from the same organisation were not in the same group, and in each group the number of participants with the same mother language was minimised.

The arrangement of the most recent workshops was repeated, with the module on Technical Aspects being split across the lunch break to reduce the intensity of the lengthy block of teaching. Informal exercises were used in the modules on operations and organisation, which seemed to be particularly good for encouraging students to consider and discuss their own situations. Almost all trainees were sufficiently confident of their language skills to contribute to these discussions.

Based on suggestions made at previous TRANSITS training courses, an informal group session was added on Friday evening. This consisted of a scenario exercise, where the students worked together in three groups on the different phases of an incident, and were encouraged to consider all aspects of incident response covered in the course. This prompted lively discussions and was considered a great success.

At the suggestion of the CESNET volunteers who assisted in the organisation of the workshop, a PGP key-signing event was also added to the Friday evening session. This allowed trainees to see in operation one of the technologies that underpins CSIRT work, to compare the different models of trust (hierarchy versus web of trust), and to add their own keys to international trust networks. The keys that were signed as proof of identity during this session will be distributed to the students and placed on international key-servers.

The evening session proved to be extremely useful in itself and in allowing more time for discussion, and should be repeated in future workshops if possible.

The time schedule of the two workshop days was as follows:

Thursday November 11th

Time	Group 1 in Conference Hall	Group 2 in Bohemi
09.30	Welcome and introductions (Conference Hall)	
10.00	Operational Issues	Vulnerabilities
11.30		Technical Issues
12.30	Lunch	
13.30	Operational Issues (report back)	Technical Issues
14.30	Organisational Issues	
16.30		Legal Issues
18.00	Close	
19.30	Dinner	

Friday November 12th

Time	Group 1 in Conference Hall	Group 2 in Bohemi
09:00	Vulnerabilities	Operational Issues
10:30	Technical Issues	
12:30	Lunch	
13:30	Technical Issues	Organisational Issues
15:30	Legal Issues	
17:00	Presentation and Close (Conference Hall)	
18:30	Dinner	
20:00	Informal group exercise – incident response scenarios (Conference Hall)	
21:30	Key signing (Conference Hall)	
22:00	Close	

Group 1: Barahona, Camilleri, Kiaune, Van Lengerich, Mer, Nazinyan, Neilson, Pilarski, Stockinger, Sultana, Szekeres, Vachek, Wöber

Group 2: Drencsan, Ettisberger, Ganzler, Grinneby, Hren, Padilla, Portelli, Sciberras, Tassberg, Třeštík

3.3. Experiences of Presenters and Trainees

During the two workshop days, the TRANSITS training course was the sole user of the facilities of the Parkhotel, with meals, accommodation for most participants and teaching rooms all in the same building. Due to the large number of applications for the course a small number of students had rooms in an adjacent hotel. The various rooms being used for the workshop were very close to each other. The hotel staff were very helpful. Thanks to lunch and dinner arrangements in buffet style with choice of different dishes it was possible to have the meals within the rather short time slots available. Students and lecturers used the main teaching room and the restaurant/bar area for informal discussions outside the teaching sessions. Such discussions were seen to be particularly valuable in an area such as incident response, where there is rarely a single "correct answer": one of the aims of the course is to encourage trainees to develop ideas that are applicable to their own CSIRTs.

The teaching sessions were presented in two groups of ten and thirteen trainees, respectively, with each group covering all the training modules during the two days. Tutors sat in on each other's sessions to provide support and additional experiences.

Two wireless networks were available on the first day. The hotel's network connection stopped working on the second day, but the network connection specifically installed by TERENA for the workshop, connected by ISDN to CESNET, remained available. Internet connectivity is useful during the training sessions to illustrate resources and techniques that may be of particular use to students. It also allows the lecturers, who give their time as volunteers, and trainees to remain in contact with their own organisations.

Every trainee was asked to fill in a feedback form during the course to rate the content and presentation of each of the modules, and the workshop organisation and venue. Written comments were also sought to help in developing the materials and organising future workshops. Marks were requested for each module for level and quantity (from 1, trivial, to 5,

excessive), for usefulness, organisation, visuals and delivery (from 1, low, to 5, high). Marks on the latter scale were also requested for workshop announcements, application and selection process, pre-workshop information, meeting rooms, Internet connectivity, hotel rooms, meals and support staff. Twenty-two completed feedback forms were returned. Overall the results were positive, with the modules averaging between 3.3 and 3.6 for level and quantity (slightly higher and with less variation than for previous workshops), and 3.5 to 3.6 for usefulness. Revisions to the Vulnerabilities module following the previous workshop appear to have raised it to the same level as the others. The group exercise session was given the highest score, 4.1, for usefulness. Presentation was rated highly, scoring between 3.8 and 4.4. Internet connectivity at 3.6 appears to have been adequate. Logistics scored very high, between 4.3 and 4.6: improvements to the documentation of the application process appear to have succeeded in making this clearer and simpler. The venue scored between 4.1 and 4.4; meals scored the highest of any of the TRANSITS workshops, reflecting both the quality and the quantity of the food that was provided.

Many participants also took the time to give detailed comments on the course. Their suggestions for improving the materials and the application process will be used for future training course deliveries. General comments were all positive: "very good workshop, keep up the good work", and "overall experience was great, I learned a lot". A number praised the interaction between lecturers and trainees and the opportunity to learn from each other's experiences.

3.4. Results from Feedback Forms

Mean scores were as follows (all scores on a range from 1 to 5 – see section 3.3 for details):

Module:	Organisation	Legal	Vulnerabilities	Operational	Technical	Group exercise
Level	3.32	3.32	3.27	3.27	3.55	
Quantity	3.27	3.55	3.32	3.36	3.41	
Usefulness	3.59	3.55	3.52	3.59	3.59	4.12
Organisation	3.86	4.14	4.24	3.86	3.95	
Visuals	3.82	4.05	3.95	4.00	4.05	
Delivery	4.14	4.36	4.14	4.19	4.14	

Logistics	
Announcements	4.32
Application & Selection	4.30
Pre-workshop information	4.43
Meeting rooms	4.05
Internet connectivity	3.57
Hotel	4.20
Meals	4.43
Support	4.55

4. Actions Arising

The following action items will be taken up in the TRANSITS project as a result of the experiences from the fifth training workshop:

- The course modules will all be revised in the light of comments from trainees and presenters during the course.
- The informal group session will be included in future workshops, with the PGP key-signing announced in advance to allow students to create their own keys if they choose.
- In addition to their current preparatory work before the workshop for the organisation and operation modules, students will be asked before the course to try to identify their own country's laws that affect CSIRT operations.
- A mailing list has been created for the trainees and presenters from the course to enable discussions to continue.
- The successful aspects of this venue will be considered in the choice of venue for future workshops.