



Report on Sixth Training Workshop

IST-2001-39118

Training of Network Security Incident Teams Staff

TRANSITS



Deliverable no. D10

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: 18 March 2005

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	7
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

Sixth TRANSITS Training Workshop materials

Executive Summary

The sixth TRANSITS training workshop was held at the Chateau de la Tour in Gouvieux near Chantilly, France, on February 17th and 18th, 2005. 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 is therefore achieving its aims of both supporting the existing CSIRT community and expanding the CSIRT model into new organisations and countries.

The nature and the structure of the TRANSITS training course basically limit participation to two groups of about ten trainees. The sixth TRANSITS workshop was oversubscribed, but neither the character of the course nor the available space at the Chateau de la Tour made it possible to admit many more participants. In the end, the workshop was attended by 22 trainees.

Compared to earlier training courses, the workshop programme was extended with additional sessions on both days, so that the programme now runs from 9 am until after 10 pm on two consecutive days.

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.

Originally it was planned that during the lifetime of the TRANSITS project the course materials would be presented six times. In 2004 it became clear that the demand for training in the CSIRT community is definitely larger than what can be met in six training courses. Towards the end of that year, it turned out that within the limits of the maximum financial contribution of the European Union to the TRANSITS project it would be possible to organise not six but seven workshops. A change of the TRANSITS project contract that would make this possible was discussed at the review of the project that took place in Brussels on 15 December 2004. In their Consolidated Report, the reviewers expressed their agreement with the proposal. A request for an amendment of the contract was submitted by the TRANSITS consortium to the European Commission on 31 January 2005. On 24 February 2005, shortly after the sixth training course, the European Commission approved the request.

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 Voghera, 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 fifth workshop was held on November 11th and 12th, 2004 in Průhonice near Prague, Czech Republic, and was reported on in deliverable no. D9.

The present deliverable reports on the preparations for, and the delivery of, the sixth training workshop.

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 staff installed Internet connectivity at the workshop venue and provided additional logistic support.

2.1. Selection of Venue

In view of the intention to spread the locations of the TRANSITS training workshops over various regions in Europe, it was decided to hold the sixth workshop in Western 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.

After investigation of several possible locations in the Paris area close to Charles de Gaulle Airport, it was decided to hold the workshop at the Chateau de la Tour in Chantilly-Gouvieux.

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 five TRANSITS training courses.

It was therefore not difficult to find a sufficient number of very well qualified presenters. The team that was chosen was actually the same group of experts who had very successfully presented the fifth TRANSITS workshop:

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

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

2.3. Workshop Announcements and Selection of Participants

On December 20th, 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). Six 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, fourth and fifth TRANSITS workshops. Reminders were sent to the same communities on January 7th and January 13th.

The following time schedule was mentioned in the workshop announcements:

17 January 2005	Deadline for sending in applications
19 January 2005	Applicants will be notified whether a place has been reserved for them at the workshop
2 February 2005	Deadline for payment of the accommodation costs and the registration fee.

Eventually, 32 applications were received before the deadline, and a number of further enquiries were received soon afterwards. 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.

Applicants who scored high but could not be admitted this time were promised a guaranteed place at the next TRANSITS workshop if they would apply again then.

A new and unexpected problem arose due to the fact that two applicants – from Serbia and Montenegro and from Iran – needed a visa to travel to France. While this had never been a problem at previous workshops in other countries, the French authorities turned out to be particularly unhelpful, and in the end these two accepted applicants had to withdraw. Their places were taken by candidates from the reserve list.

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. Four of the final 22 participants in the sixth 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, two of which were used for the Friday evening session. The CD-ROM also contained RFCs relevant to CSIRT work. Each participant pack also included a copy of a Guidance Note on writing advisories published by UKERNA. The book *Incident Response* by Van Wyk and Forno, which had been included in the pack previously, was now out of print and no suitable replacement could be identified.

The workshop materials were brought to the workshop venue by TERENA staff, travelling by car from Amsterdam.

3. Workshop Delivery

3.1. Participants

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

Ronald Boontje	University of Amsterdam	Netherlands
James Cilia	University of Malta	Malta
Ricardo de Mingo	University of Barcelona	Spain
Marco Ferrante	University of Genoa	Italy
Achim Gsell	Paul Scherrer Institute	Switzerland
Christian Heim	University of Bern	Switzerland
Alberto Hernandez	Defence Joint Staff	Spain
Martin Gilje Jaatun	SINTEF	Norway
Thorben Jändling	JANET-CERT	United Kingdom
Tobias Marx	Paul Scherrer Institute	Switzerland
Branko Mažar	CARNet CERT	Croatia
Sara McAnaney	Trinity College Dublin	Ireland
Jens Melle	Volkswagen CERT	Germany
Charles Mifsud	University of Malta	Malta
Milda Mimiene	LITNET CERT	Lithuania
Martin Mogensen	DANCERT	United Kingdom
Kees Mulder	Delft University of Technology	Netherlands
Brian O'Hora	Trinity College Dublin	Ireland
David Prendergast	IBM	United Kingdom

Olav Seyfarth	Telefónica Deutschland	Germany
Laas Toom	EENet	Estonia
Koen Van Impe	BELNET CERT	Belgium

Of these trainees, twelve work for existing CSIRTs and ten were from organisations that are in the process of creating a new CSIRT. Seven 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 companies and one government organisation were represented.

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. 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.

The informal Friday evening group session, introduced at the previous TRANSITS workshop, was repeated with students being encouraged to work through two incident response scenarios in small groups, to identify the issues from each of the course modules that may arise.

A PGP key signing was included on the Thursday evening. This allowed trainees to see in operation one of the technologies that underpins CSIRT work, to compare 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 were later distributed to the students and placed on international key servers.

Previous course feedback had asked for information on new developments, so two short "work in progress" talks were given by lecturers in parallel sessions on Thursday afternoon, one on WARPs (Warning, Advice and Reporting Points), and the other on incident response for eScience Grids.

On Friday afternoon, one of the tutors talked students (and the other lecturers) through a genuine incident that he was currently working on.

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

Thursday February 17th

Time	Group 1 in Maxime + Loraine	Group 2 in Romy
09.00	Welcome and introductions	
09.30	Operational Issues	Vulnerabilities
11.00		Technical Issues
12.00	Lunch	
13.00	Operational Issues (report back)	Technical Issues
14.00	Organisational Issues	
16.00		Legal Issues
17.30	"Work in Progress"	
18.00	Break	
19.00	Dinner	
20.30	Key-signing party	

Friday February 18th

Time	Group 1 in Maxime + Loraine	Group 2 in Romy
09:00	Vulnerabilities	Operational Issues
10.30	Technical Issues	
12.30	Lunch	
13.30	Technical Issues	Organisational Issues
15.30	Legal Issues	
17:00	Extra session "technical"	
18:00	Break	
19.00	Dinner	
20:30	Informal group exercise – incident response scenarios	
22:00	Presentation and Close	

Group 1: Cilia, Heim, Jaatun, Marx, McAneney, De Mingo, Mulder, Prendergast, Seyfarth, Toom, Van Impe

Group 2: Boontje, Ferrante, Gsell, Jändling, Hernandez, Mažar, Melle, Mifsud, Mimiene, Mogensen, O'Hora

3.3. Experiences of Presenters and Trainees

All facilities needed for the workshop were provided by the hotel, with meals, accommodation and teaching rooms all in the same building. The spacious teaching rooms formed a self-contained unit including a coffee lounge so that trainees and lecturers were able to have both formal and informal discussions in the same convenient area. 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 hotel staff were very helpful, especially in serving excellent meals within the tight time constraints of the workshop programme.

The teaching sessions were presented in two groups of eleven trainees, 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.

TERENA staff installed a temporary wireless network in the teaching rooms for the duration of the course, connected to the Internet via the hotel's ADSL access. Setting this up without interfering with the hotel's wired and wireless network systems took a large part of the first morning, but the network worked satisfactorily thereafter. Network connectivity is useful during the teaching 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 formal modules averaging consistently between 3.2 and 3.5 for level and quantity, and 3.5 to 3.7 for usefulness. Presentation was rated highly, scoring between 3.8 and 4.5.

Of the informal sessions, the scenario exercise was given the highest score for usefulness, 3.5, with all the other sessions scoring at least 2.9. In addressing specific subjects the "current activity" sessions are inevitably going to be more relevant to some students than to others, but the general level of feedback seems to justify repeating them. Individual written comments on these sessions suggest that at least some students found them very useful and enjoyable.

Internet connectivity at 3.7 was the highest score for any of our residential venues. Logistics scored highly, between 4.1 and 4.3. The venue had the most consistently high scores of any of the workshops, between 4.4 and 4.5.

General comments on the workshop indicate that despite the intense schedule, students found the event both useful and enjoyable: "really great workshop, very useful, thank you" is typical, while "excellent – supports my understanding of CSIRTs; assists me personally in terms of career development; encourages further learning; provides communication channel with peers and experts" indicates that TRANSITS is achieving all its aims.

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
Level	3.30	3.27	3.27	3.30	3.50
Quantity	3.32	3.23	3.23	3.32	3.50
Usefulness	3.55	3.66	3.50	3.45	3.45
Organisation	4.25	4.00	3.95	4.05	4.05
Visuals	3.84	4.07	3.91	3.95	4.00
Delivery	4.48	4.26	4.29	4.29	4.15

Session:	Work in progress	Extra session "technical"	Key signing	Informal group exercise
Level	3.08	3.03		
Quantity	3.08	2.95		
Usefulness	2.92	2.97	3.29	3.48
Organisation	3.74	3.79		
Visuals	3.61	3.66		
Delivery	3.80	3.94		

Logistics	
Announcements	4.14
Application & Selection	4.32
Pre-workshop information	4.24
Meeting rooms	4.55
Internet connectivity	3.67
Hotel	4.38
Meals	4.36
Support	4.52

4. Actions Arising

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

- The course modules will all be revised in the light of comments from trainees and presenters during the course.
- The informal group sessions 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.
- 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 the final workshop.