



# Report on Seventh Training Workshop

IST-2001-39118

Training of Network Security Incident Teams Staff

TRANSITS



## Deliverable no. D11

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: 27 May 2005

## CONTENTS

<b>Executive Summary</b>	<b>3</b>
<b>1. Workshop Objectives and Background</b>	<b>3</b>
<b>2. Workshop Preparations</b>	<b>4</b>
2.1. Selection of Venue	5
2.2. Choice of Presenters	5
2.3. Workshop Announcements and Selection of Participants	6
2.4. Financial Arrangements	6
2.5. Workshop Materials	7
<b>3. Workshop Delivery</b>	<b>7</b>
3.1. Participants	7
3.2. Programme	8
3.3. Experiences of Presenters and Trainees	11
3.4. Results from Feedback Forms	12
<b>4. Actions Arising</b>	<b>13</b>

*Annex I*

*Seventh TRANSITS Training Workshop materials*

## **Executive Summary**

The seventh TRANSITS training workshop was held at the Hotel Riviera in Carcavelos, Portugal, on April 28<sup>th</sup> and 29<sup>th</sup>, 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 Portuguese national research and education networking organisation, FCCN, had been particularly active in publicising the event among universities in Portugal, where they are actively encouraging the establishment of CSIRTs. We expect that this TRANSITS training workshop will have made a significant contribution to the formation of a CSIRT community in the country.

The nature and the structure of the TRANSITS training course basically limit participation to two groups of about ten trainees. The seventh TRANSITS workshop was very much oversubscribed, and because this would be the last training event organised as part of the TRANSITS project, it was decided to exceptionally admit more participants than usual. In the end, the workshop was attended by 30 trainees.

Like in the sixth TRANSITS workshop, the workshop programme was extended with additional sessions on both days, so that the programme ran from 9 am until after 10 pm on two consecutive days.

The workshop in Carcavelos was the last training workshop that was supported by funding from the TRANSITS project. The project partners, TERENA and UKERNA, are currently making arrangements for the continuation of activities after the end of the project. These arrangements will be reported in the Final Report on the TRANSITS project.

## **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, the European Commission approved the request.

The first training workshop took place in Oegstgeest, the Netherlands, on October 31<sup>st</sup> and November 1<sup>st</sup>, 2002 and was reported on in TRANSITS deliverable no. D2. The second TRANSITS workshop was held in Warsaw, Poland, on May 27<sup>th</sup> and 28<sup>th</sup>, 2003 and was reported on in deliverable no. D3. The third workshop was held on October 30<sup>th</sup> and 31<sup>st</sup>, 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 25<sup>th</sup> and 26<sup>th</sup>, 2004 and was reported on in deliverable no. D7. The fifth workshop was held on November 11<sup>th</sup> and 12<sup>th</sup>, 2004 in Průhonice near Prague, Czech Republic, and was reported on in deliverable no. D9. The sixth workshop took place in Gouvieux near Chantilly, France on February 17<sup>th</sup> and 18<sup>th</sup>, 2005 and was reported on in deliverable no. D10.

The present deliverable reports on the preparations for, and the delivery of, the seventh 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 and arranging accommodation. UKERNA's Andrew Cormack took charge of ensuring the availability of lecturers 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, and following an enthusiastic invitation from FCCN, it was decided to hold the seventh workshop in Portugal.

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 around Lisbon, it was decided to hold the workshop at the Hotel Riviera in Carcavelos.

## **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 six TRANSITS training courses.

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

Andrew Cormack	UKERNA	United Kingdom
Jan Meijer	SURFnet-CERT	Netherlands
Klaus Möller	DFN-CERT	Germany
Don Stikvoort	S-CURE	Netherlands

Normally the TRANSITS workshops have five presenters, but on this occasion one of the confirmed lecturers was unable to attend at the last minute, so his presentations were done by one of the other four, who is actually a specialist for the subject matter (legal issues) of the module concerned.

### **2.3. Workshop Announcements and Selection of Participants**

On March 8<sup>th</sup>, 2005 the announcement of the training workshop was published on the TRANSITS website ([www.ist-transits.org](http://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). Seven 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](http://www.ist-transits.org/maillinglist.php)), and the mailing lists of participants in the first, second, third, fourth, fifth and sixth TRANSITS workshops.

The following time schedule was mentioned in the workshop announcements:

28 March 2005	Deadline for sending in applications
30 March 2005	Applicants will be notified whether a place has been reserved for them at the workshop
13 April 2005	Deadline for payment of the accommodation costs and the registration fee.

Eventually, 35 applications were received before the deadline, and a number of further enquiries were received soon afterwards. After careful consideration, 32 applicants were admitted to the course, substantially more than the usual maximum of about 20 participants.

An unexpected problem arose due to the fact that relatively many of the applicants came from organisations in Portugal, and bureaucracy, especially in the public sector, seems to be more of a problem there than in other countries that the TRANSITS project has dealt with in the past. As a consequence, in several cases it turned out to be impossible for the employer of the prospective workshop participant to make a payment within two weeks. Because of this, two applicants decided to withdraw from participating in the course. In other cases, participants paid for the accommodation costs and the registration fee themselves, in the hope that they would be reimbursed by their employer later.

### **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.

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. None of the participants in the seventh 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.

The workshop materials were shipped by TERENA to the offices of FCCN in Lisbon, and transported from there by them to the workshop venue.

## **3. Workshop Delivery**

### **3.1. Participants**

Thirty trainees attended the course, from eleven countries:

Guido Aben	SURFnet-CERT	Netherlands
Rovshan Akbarov	AzNet	Azerbaijan
Leonardo Amor	Telefónica	Spain
Raymond Azzopardi	mtCERT	Malta
Dan Bailey	NISCC	United Kingdom
João Barros	TVCabo	Portugal
Paulo Carvalho	University of Porto	Portugal
Stephen Cassar	mtCERT	Malta
António Costa	University of Trás-os-Montes	Portugal
Mário Filipe	University of Évora	Portugal
Adrian Gschwend	Berne University of Applied Sciences	Switzerland
Peter Hammond	NISCC	United Kingdom

András Kabai	CERT-Hungary	Hungary
Bob van der Kamp	GOVCERT.NL	Netherlands
Ivo Marques	University of Aveiro	Portugal
Ricardo Martins	University of Aveiro	Portugal
Jorge Matias	Technical University of Lisbon	Portugal
Nuno Neves	University of Lisbon	Portugal
Hans Petri	GOVCERT.NL	Netherlands
David Pinedo	CERT.PT	Portugal
Sergio Pozo	University of Seville	Spain
Richard Pryor	NISCC	United Kingdom
José Ramada	University of Minho	Portugal
Paul Reilly	Trinity College Dublin	Ireland
Arsénio Reis	University of Trás-os-Montes	Portugal
José Ríos	University of Alcalá	Spain
Pedro Rosa	University of Lisbon	Portugal
Inger Tøndel	SINTEF ICT/SIS	Norway
Henner Vogt	Telefónica	Germany
Harald Volz	University of Basel	Switzerland

The majority of the CSIRTs represented are associated with research and education, but three participants came from commercial companies and eight from government organisations.

### **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 two previous TRANSITS workshops, was repeated with students being encouraged to work through two incident response scenarios in small groups, in order 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.

Two short "work in progress" talks were given by lecturers in parallel sessions on Thursday afternoon, one on international co-operation and the European Abuse Forum, and the other on an incident handling application.

On Friday afternoon, one of the tutors talked students (and the other lecturers) through a genuine incident that he had been working on recently, while in a parallel group security issues for Grids were discussed.

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

#### Thursday April 28<sup>th</sup>

Time	Group 1	Group 2
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	Parallel "Work in Progress" sessions	
18.00	Break	
19.00	Dinner	
20.30	Key-signing party	

#### Friday April 29<sup>th</sup>

Time	Group 1	Group 2
09:00	Vulnerabilities	Operational Issues
10.30	Technical Issues	
12.30	Lunch	
13.30	Technical Issues	Organisational Issues
15.30	Legal Issues	
17:00	Two extra parallel sessions	
18:00	Break	
19.00	Dinner	
20:30	Informal group exercise – incident response scenarios	
22:00	Presentation and Close	

**Group 1:** Amor, Azzopardi, Barros, Costa, Filipe, Hammond, Kabai, Martins, Matias, Neves, Penedo, Petri, Reilly, Ríos, Volz

**Group 2:** Aben, Akbarov, Bailey, Carvalho, Cassar, Gschwend, Van der Kamp, Marques, Pozo, Pryor, Ramada, Reis, Rosa, Tøndel, Vogt

### **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. Students and tutors were able to use the teaching rooms as well as the nearby coffee lounge and bar for informal discussions. 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; meals and breaks were self-service, and therefore fitted in easily into the TRANSITS course schedule.

The teaching sessions were presented in two groups of fifteen 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. 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. Unfortunately, it became apparent that the hotel system was intended to connect a single computer in each room, rather than a local-area network, and it was prone to unexpected interruptions throughout the two days. The hotel's own information about their service was limited: although the hotel management had informed the workshop organisers that VPN access would not be possible, this turned out to be the most reliable way to use the network.

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-seven completed feedback forms were returned.

Overall the results were positive and consistent with previous workshops, with the formal modules averaging consistently between 3.2 and 3.4 for level and quantity, and 3.4 to 3.6 for usefulness. Presentation was rated highly, scoring between 3.9 and 4.3.

The "work in progress" talks scored between 2.5 and 3.3 for usefulness. In addressing specific subjects these sessions are inevitably going to be more relevant to some students than to others, but the general level of feedback seems to justify including them. They can also provide useful feedback for the presenters on how suitable their ideas are for different CSIRT contexts. The general sessions scored highly for usefulness: 3.4 for the PGP key-signing and 3.5 for the scenario exercises.

Internet connectivity scored only 2.5, reflecting the problems that were encountered.. Otherwise logistics worked well, with scores between 4.0 and 4.6. The hotel facilities had the second highest rating, 4.6, of all the TRANSITS workshops; meals and rooms also scored well at 4.3.

General comments on the workshop indicate that despite the intense schedule, students found the event both useful and enjoyable: "very good", "well organised", "presenters, speakers and organisers all excellent" were typical remarks.

### **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):

<b>Module:</b>	<b>Organisation</b>	<b>Legal</b>	<b>Vulnerabilities</b>	<b>Operational</b>	<b>Technical</b>
Level	3.15	3.23	3.35	3.15	3.37
Quantity	3.19	3.27	3.22	3.33	3.44
Usefulness	3.58	3.35	3.56	3.56	3.56
Organisation	4.08	3.96	4.08	3.88	4.04
Visuals	3.88	3.80	4.04	3.76	4.00
Delivery	3.96	4.16	4.33	3.88	4.12

<b>Session:</b>	<b>Cooperation European Abuse Forum</b>	<b>Incident Handling Application</b>	<b>Grid security</b>	<b>Real- life Incident</b>	<b>PGP Key- signing</b>	<b>Informal group exercise</b>
Level	2.43	2.68	3.17	3.39		
Quantity	2.43	2.64	3.08	3.44		
Usefulness	2.50	2.77	3.33	3.33	3.38	3.52
Organisation	3.00	3.48	4.18	3.50		
Visuals	3.14	3.43	3.50	3.61		
Delivery	3.17	3.52	4.00	3.67		

<b>Logistics</b>	
Announcements	4.00
Application & Selection	4.00
Pre-workshop information	4.19
Meeting rooms	4.30
Internet connectivity	2.45
Hotel	4.56
Meals	4.26
Support	4.59

#### **4. Actions Arising**

This was the last workshop funded by the TRANSITS project, but there is wide support for continuing the training workshops in the future. It also appears that the materials have now grown to the limit that is possible to cover within a two-day course; a number of students suggested that the material could easily occupy three, less packed days.

Actions arising out of the workshop:

- The course modules will all be revised in the light of comments from trainees and presenters during the course.
- A mailing list has been created for the trainees and presenters from the course to enable discussions to continue.
- The successful and unsuccessful aspects of this venue and previous ones will be reviewed and documented as part of the Final Report on the TRANSITS project.
- Discussions will be held with other interested parties to ensure that the TRANSITS materials continue to be presented at training courses in Europe after the end of the project.