INFORMATION SOCIETIES TECHNOLOGY (IST) PROGRAMME

Proposal acronym:	**eCSIRT.net**
Proposal full title:	**European CSIRT Network**
Proposal/Contract number:	**IST-2001-37558**

Final Report

Working package:	WP 1 – Project Management
Delivery:	D 1.3.4.1 / D 1.3.4.2
Date of preparation:	18 January 2004

Table of Contents

1 Introduction ... 3

1.1 Purpose of this Document ... 3

1.2 Document Structure ... 3

2 Results of the eCSIRT.net Project ... 5

2.1 The Common Language ... 5

2.1.1 Introduction ... 5

2.1.2 The stability of IODEF ... 5

2.1.3 The Code of Conduct ... 6

2.1.4 The common language definition ... 6

2.1.5 Integration and Implementation ... 8

2.1.6 Deployment of the common language ... 9

2.2 The Statistic Function ... 9

2.2.1 Type 1 and 2 Statistics ... 10

2.2.2 To Do for Type 1 and 2 Statistics ... 11

2.2.3 Type 3 Statistics ... 11

2.2.4 To Do for Type 3 Statistics ... 14

2.3 The Alert Function ... 15

2.3.1 In-band alert function ... 15

2.3.2 Out-of-band alert function ... 16

2.3.3 To Do ... 17

2.4 eCSIRT.net from a member perspective ... 17

3 Achievements of the Project ... 18

3.1 Original Problem Statement ... 18

4 Take-Up of eCSIRT.net Services ... 21

4.1 Input to TF-CSIRT Working Groups ... 21

4.2 Take-Up by TI Accredited Teams ... 21

4.3 Continuation as Volunteer Project ... 21

5 Presentations and Papers ... 23

1 Introduction

The eCSIRT.net project aimed at improving the efficient and effective cooperation of CSIRTs which should result in a quicker response to detected security problems. Better proactive security measures that are presented as best practice and result from the collected knowledge available within the CSIRT community will reduce the overall numbers of incidents. The enabled statistics do allow to measure the level of incidents and threats existing today for the first time, once qualified information will become available.

The public presentation of incidents and vulnerabilities might be seen as something that will undermine the public confidence. But it needs to be recognized that the public confidence is already heavily impacted by the headlines regarding attacks like Code Red, Nimda, Slammer, Blaster, etc. or widespread vulnerabilities like the SNMP vulnerability or any new MS Windows problem broadly discussed on the Internet. All named incidents are examples for global problems not restricted to a smaller set of organizations or directed towards a particular target but attacking the community at large. In the opposite, the availability of "true" information will result in a better understanding, and only if understanding leads to an improved security culture will users and organizations know that they need to take much better proactive steps to avoid incidents and not suffer from break-ins.

As of today cooperation among CSIRTs still is not fully supported by techniques or well established procedures, but progress is clearly visible. The eCSIRT.net project aimed to establish the necessary frameworks for the service applications based on automatic information exchange related to incidents or more specifically to CSIRT operations. Such application were far from fully established when the project started, and at least in the area of statistics and alerting has eCSIRT.net proven that "it can be done" and in the automatic exchange the project has delivered a pragmatic common language to guide all practitioners whenever the syntax of IODEF leaves options how to express specific details.

What is still needed are more standards related to IODEF and IDMEF, which addresses new problems that can only be recognized after having actually deployed the formats – without any protocol the format alone will be difficult to integrate in multilateral communication going back and forth.

Having touched already in this short paragraphs on the most important lessons learned, we will now first introduce further details about this report and then continue to discuss the working packages and related insights one by one.

1.1 Purpose of this Document

This document summarizes all achievements of the eCSIRT.net project and provides insights in the experiences the partners gained during the duration of the project.

In addition the main results of the project – as they are mostly available from the public web site – are introduced in more detailed, explaining their relationship and potential use.

At last this document will provide a summary of the activities that have been taken to ensure that the gained knowledge and insights will become part of the common knowledge within the CSIRT community.

1.2 Document Structure

The structure of this document was held as simple as possible. In the 2nd chapter the results of the project will be reviewed and explained what was made available to the CSIRTs and the public. In addition the project will be reviewed from a member perspective.

The next chapter will review the originally identified needs and comment on them in light of the achievements of the projects to put the project itself in perspective.

The 4th chapter summarizes options and some already taken approaches to continue to provide the established services or to introduce the gained knowledge and possibilities into the further developments.

The last chapter collects information about presentations and papers about the project.

2 Results of the eCSIRT.net Project

2.1 The Common Language

2.1.1 Introduction

The objective of this work package – or rather work packages, since we are joining WP2 and WP3 together here – was to make the IETF IODEF model “work” in real CSIRT life – no more, no less.

IODEF is a flexible model, a way to map the internals of an incident description to an IODEF XML object, that can be transferred (typically by e-mail), and read and processed elsewhere. Processed more *automatically* than is currently the case with incident data exchange, which is entirely manual labor and cut-and-paste at this moment.

So, in theory, if all CSIRTs were to adopt IODEF, that would make it possible to exchange incident data more efficiently, with automatic loading of some other CSIRT’s incident data (exchanged through an IODEF XML object) into the own database.

However, the IODEF model is **too** flexible to make that possible. There are too many degrees of freedom in mapping incident data onto the IODEF data model. And the result of that will always be IODEF XML, but without some additional deals on how to do things, one CSIRT’s XML would not be parseable by another team’s software.

In more formal words – IODEF provides the syntax – but the semantics are missing.

So what eCSIRT.net set out to do was – add the semantics to IODEF. This was named “create a common language”. The common language was to be a set of agreements additional to IODEF, that would make IODEF work in real life, as a means of exchanging incident data – between CSIRTs, towards collectors of statistics, for alerting purposes.

The “common language” additional to IODEF is thus the cork on which the eCSIRT.net project was floating. Once a workable common language was defined (the first stream of activity in the project), the project split in three parts, all dealing with a real life *application* of the common language: exchange of incident data between CSIRTs, statistics gathering, and an alerting function. Statistics (WP 4) and alerting (WP5) are treated in their own sections below. Incident data exchange is treated in this section, because the refinement of the common language was also part of the work package involved (WP3).

Now in this section on the common language, we shall in somewhat more depth describe what was achieved in that regard. However, before we embark on that course, a subsection needs to be inserted on a topic that involved much time in the beginning of the project, and which also was the reason to ask for extension of the project – which was granted. That topic is the stability of IODEF.

2.1.2 The stability of IODEF

When the project was defined, in early 2002, the IETF working group INCH was working steadily on what was soon to become the IODEF standard, meant for exchange of incident data by means of XML objects. INCH was working on the IODEF requirements, and the IODEF data model. Elements of IDMEF were included in order to satisfy the requirement that IDMEF information could be contained in IODEF objects.

However, when the eCSIRT.net consortium studied the existing IODEF material *in depth* in the summer of 2002, and discussed it at their joint meeting at Syros in September 2002 – it became obvious that there was no point in trying to define a common language based on IODEF, when the IODEF model itself was still so unstable, ambiguous, and hard to use.

So a concentrated effort was undertaken, on the one hand within the eCSIRT.net consortium to come up with proposals to make IODEF pragmatical and useful, and on the other hand, to feed these into the INCH process. The latter was done on the mailing list of INCH, in several IETF meetings, and even on a joint eCSIRT.net/INCH meeting – the involvement of the eCSIRT.net consortium and its liaisons was very close – and successful.

In the period from September 2002 till April 2003, the IODEF data model was changed from academically and ambiguous, into something that could meaningfully be used in real life. Since that time, the changes in the data model have only been minor, and it is expected that it will move to "standard" status this year (2004).

2.1.3 The Code of Conduct

The planned adoption of IODEF to use for exchange of incident data, statistics and alerts, is more than just applying a standard to the representation of incident data-in-exchange. Because the reason to implement the standard, is to enable, in the end, (semi-)automatic generation of incident data objects **and** (semi-)automatic processing of the same objects, at the other end of the communication line.

The latter would mark a major step forward in the efficient handling of big numbers of incidents, with other CSIRTs involved as well.

However, because this would mean that the classical manual process (simply reading e-mails from another CSIRT and acting on them) would be succeeded by a semi-automatic process, the question of *mutual trust* becomes of extra importance. It is clearly not acceptable to allow (even semi-)automatic processing of incident data generated by an unknown, or untrusted party. Bear in mind that the IODEF model does not only contain technical data about an incident, but also the expected actions to be taken.

Now the starting point of the eCSIRT.net consortium was already, that each member had to be a CSIRT accredited by the Trusted Introducer (TI). That ensured a basic form of mutual trust.

However, it was seen as necessary to develop additional to the TI accreditation, a Code of Conduct, that would need to be signed by any party wanting to participate in the eSCIRT.net incident data exchange schemes. The vision was, that also after eCSIRT.net would have ended, this combination of TI accreditation and acceptance of the Code of Conduct, would be a good vehicle for CSIRTs to decide whether they can use IODEF (and the associated automatisms) between one another – or not.

The Code of Conduct was finalised in December 2002, and signed by all eCSIRT.net members and accepted by liaisons as they joined. It is a high level Code of Conduct, but contains sufficiently practical conduct rules (e.g. on the confidentiality of the other's data - "be given highest priority", and on intellectual property rights - "must be protected") to be meaningful in the CSIRT operations.

The Code of Conduct was made available to TI accredited teams outside the consortium in September 2003. For non- European teams that would want to join in, an ad hoc approach was foreseen for the short term to replace the TI accreditation – the latter not being available for teams outside Europe.

The span of time following September 2003 was too short for other teams – not sharing 1.5 year of eCSIRT.net involvement together – to join in. However as is described below, at least within the community of TI accredited teams, the interest to take up the results of eCSIRT.net is growing – and a take up of eCSIRT.net results by a CSIRT will mean – at least for the time being – that that CSIRT will adopt the Code of Conduct.

2.1.4 The common language definition

As stated in 2.1.2 above, it took more time for IODEF to stabilize than had been expected at the outset of the project. However, in the spring of 2003, the stability of IODEF, and especially the usefulness, had become such, that the consortium took up the "common language" definition – that is, the set of rules and semantics additional to IODEF, that would make it possible for the CSIRTs in the consortium to start using IODEF **and** *successfully inter-communicate* using IODEF XML objects.

The entire reason to define the common language is found in those words "*successfully inter-communicate*". Because although IODEF can be used without problems in a stand-alone fashion – communication between teams using IODEF will only be possible in a (semi-)automated way, if additional rules are added to IODEF defining a course to take in the maze of IODEF possibilities.

The common language was developed within the consortium from April-July 2003 – in the remainders of the project it was updated regularly, but those were only minor updates.

The approach taken in the common language was to specify a specific profile within IODEF for eCSIRT.net – in fact, a specific unambiguous choice within the many degrees of freedom offered by the IODEF XML syntax. Essentially, it defines an incident data object as consisting of:

- ID (and alternative IDs, when multiple CSIRTs work on one incident)
- Description
- Assessment & impact
- Method of incident
- Expectation (the purpose in sending the XML object out!)
- Timestamps
- Contact data
- History
- Event data
    - Systems involved
    - All other relevant data
- Additional data

What is new here, one might ask? In classical inter-CSIRT communication, all of the above is used too, when necessary. However, that is all done in "free text format", and can only be "parsed" (assessed) by human intelligence – including a considerable admin overhead.

With the eCSIRT.net IODEF profile, most of the data is of a structured type, using the IODEF datamodel (containing parts of IDMEF as well, so software that generates IDMEF messages can easily be integrated with IODEF compatible incident databases). The fact that it is structured enables automated parsing of incoming eCSIRT.net profiled IODEF objects – this has the potential to remove all admin overhead from the CSIRT staff. In that way, it becomes possible, to receive an incident object, and have it automatically archived and displayed on screen for the CSIRT staff, in the local format the staff member is used to, with fields immediately displaying the possible impact (as estimated by the sending CSIRT) and the expectation (e.g. "please notify your constituent that cracking has been attempted from their IP range, and report back to us", or "for your information, no action requested", etc. etc.).

The eCSIRT.net common language definition not only specifies the precise path to use trough the IODEF XML data structure, it goes one step further towards the real life demands, offering a guideline to implementation. Just a few examples of that:

- In the contact data, the use of the classes *Name, Email, Telephone* and *Time zone*, are mandatory
- Use of timestamps for events and history is mandatory
- Additional data contains mandatory tags like "eCSIRT.net IODEF Profile Version 1.0", to enable automatic parsers to recognize the eCSIRT.net profile (and the version, should it change in the future)
- E-mail is defined as transport mechanism, and mandatory mail addresses are specified, like iodef-in@team.domain and iodef-return@team.domain, and (for gathering of statistics and spreading of alerts) iodef-stats@ecsirt.net and iodef-alerts@ecsirt.net.

Finally, the common language definition / implementation guideline recommends that – although the eCSIRT.net profile is a quite simple route through the IODEF data model, avoiding the exotic features also in the model – software adopted by CSIRTs to deal with eCSIRT.net IODEF objects, should have facilities to also deal with more complex IODEF objects. This will not be possible *in general* (if it were we would not need the common language) but it can be done by e.g. giving way to a manual approach with non-eCSIRT.net compliant objects, just presenting the various information contained in the XML object in a structured way, so the CSIRT staff member can work on that.

2.1.5 Integration and Implementation

With the common language in place, and IODEF being stable enough – the eCSIRT.net consortium devoted all of its time to attempts at implementing IODEF in their real life situation. One of the deliverables of the project was preceding that, and was intended to describe the state-of-the-art with regards to the integration of the various concepts enabling (semi-)automatic processing of incident data or events. This deliverable is the "Documentation on the integration of the common language into CSIRT operation", and is recommended reading for any CSIRT that wants to attempt to use IODEF or IDMEF – and indeed the overview that the document offers even encompasses EISPP and CAIF.

Directly following on the "integration" document is the list of available tools that eCSIRT.net has collected, the "Product list of IODEF/IDMEF solutions". This list has been updated until the very end of the project, and is considered to be a complete overview of the currently available products/tools in the range. Looking at the list, it is obvious that commercial products adopting IODEF or IDMEF are still scarce – hardly a surprise, given the relative youth of these developments, and the fact that there are no big commercial gains to be found in this relatively small community. Still – the take-up is there. In the open source arena three products can be used with IDMEF (extensions): Snort, Prelude and STAT. With regards to IODEF, the developers of RT (Request Tracker – an e-mail based incident database and workflow tool) have taken a keen interest, and other, suppliers of commercial workflow software, have approached eCSIRT.net members to look for cooperation in inserting IODEF into their software.

However, in the summer of 2003, when the eCSIRT.net consortium was ready to start implementing IODEF, using the new common language, the existing lack of tools was a genuine challenge. Therefore the decision was taken to develop some elementary tools – and thus lead the way in the application of IODEF. This activity was additional to the charter of eCSIRT.net, but unavoidable for the project to have success.

Initially, over summer, IHSH was developed – IHSH is a small command-line tool to manage (create, read, write and modify) IODEF XML objects. It utilizes the existing LibAir library developed at CERT/CC [1] , and can be invoked from Unix SHell scripts. Later, support for ARS (Action Request System – well known workflow management software package) was added [2] - thus offering a direct route from incident database (ARS) to outgoing IODEF message – and vice versa – all based on the eCSIRT.net IODEF profile.

Later in summer, JANET-CERT (consortium member) developed XML-IODEF - a Perl library used to create and parse IODEF messages, with Perl scripts directly (LibAir is not used by XML-IODEF) operating on the input data, or IODEF object. XML-IODEF does not integrate directly into an existing incident database (yet) – it was used for experimenting with the generation and parsing of eCSIRT.net profiled IODEF messages, just like what IHSH was used for mainly. At the end of 2003, most of the consortium members adopted the XML-IODEF Perl scripts – whereas IHSH was used for specific

[1] Developed by Roman Danyliw et al. of CERT/CC – liaison to the eCSIRT.net project and chairman of the IETF INCH working group – Arne Helme of Stelvio, on behalf of the eCSIRT.net consortium, worked closely together with Danyliw and Jan Meijer (SURFnet-CERT, also liaison to the project) to enable the developments described here

[2] The addition of ARS support – too specific to be developed under the eCSIRT.net umbrella – was enabled by additional funding from SURFnet, The Netherlands, which CSIRT (SURFnet-CERT) uses ARS as incident database

experiments, and by the liaison SURFnet-CERT, who also had the possibility to tie it in with their incident database.

Both IHSH and XML-IODEF are described in the second part of the “Guideline to Application of the Common Language” (the first part of that Guideline is contained in the common language specification itself). The “Product List” offers links to the complete packages, which are delivered including documentation – ready to use in real environments. Naturally both packages are open source.

2.1.6 Deployment of the common language

The deployment of the common language (which development essentially was WP2) headed off in three directions: statistics, alerting and exchange of incidents between CSIRTs. Statistics (WP4) and alerting (WP5) are treated below in separate sections. Exchange of incidents (WP3) is treated here.

Now WP3 did not only contain the actual exchange of incident data by means of IODEF messages, but also regular updates to the “Product List” and the “Guideline to How to apply the common language”. The latter two have been pursued till the very end of the project and are available in those “final” versions. “final” as in relative to the end of this project, cause evidently the development of IODEF/IDMEF in the area of CSIRT operation is still very much in development.

The actual exchange of incident data using common language compliant IODEF messages has been undertaken only in an experimental form, in a shared WP3/6 activity. This can already be concluded from the fact that the IHSH and XML-IODEF packages did not yet allow direct integration into the incident databases of the various CSIRTs. And besides – that sort of integration would have a significant effect on the operation of a CSIRT dealing with maybe hundreds of incidents a month. Therefore it is expected that real integration will only take place – even with the eCSIRT.net consortium members – later in 2004 or even 2005. However, the enabler of such an integration will clearly have been the eCSIRT.net project.

The experimental exchange of IODEF messages is shortly described in the WP6 report. It generally went well, though of course numerous caveats and little bugs were discovered along its course. However it clearly was a “proof of concept” for the common language approach taken in the eCSIRT.net project, to mould IODEF into a standard for real life use. Also, it proved the usefulness of the IHSH and XML-IODEF tools, and no doubt both will be used as part of, or as role models for, the integration efforts that will follow this project.

2.2 The Statistic Function

The objective of this work package was the establishment of the collection of statistic data, on the one hand in order to serve the teams involved with information on the other hand to satisfy the need for information of a wider audience. Contrary to other available statistics (see "List of links to public statistics on incidents" on the public web server), which are published by individual organizations, we had to meet challenges which are caused by the co-operation between different and independent teams in an international context.

The first hurdle was the definition of a common standard for the statistical report system to ensure that statistics will be useful and comparable. The discussions were characterized by the different positions of the individual teams, because for the following substantial questions solutions had to be found:

- What kind of data are to be collected?
- What kind of information can be published and to whom?
- Which are the confidentiality and privacy needs to meet?

After completion of the discussions we have reached an agreement to prepare the following statistics:

- Type 1: Statistics on workload and resources spent by teams
- Type 2: Statistics on incidents handled by teams

- Type 3: Statistics on the hazard level of internet connected systems

2.2.1 Type 1 and 2 Statistics

Beside this definition the following most important agreements have been taken in the Clearinghouse Policy:

- Requirements for the participation
- Communication and communication security
- Privacy and disclosure
- Classification of information
- Incident classification

Thus the basis for the collection and publication of statistics were reached. After a first phase of the data collection an internal Review was carried out. The following problems became visible:

- **Type 1 statistics:**

  Some of the data fields did not refer well enough to the data collected by most of the teams.

  The cause for this might lie in the use of different tools for the incident handling. Through this the collected data of the teams deviated too strongly from the given categories and could be compared only with difficulty with each other. Therefore a redefinition of some fields was necessary. Due to the participation in the eCSIRT.net project and the associated integration of new technologies for communication and co-operation (IODEF, eCSIRT.net communication infrastructure), a process was started for the harmonization of incident handling systems by some teams. The introduction of incident handling systems based on RT (request tracker) will guarantee a better compatibility of the statistical data in future.

- **Type 2 statistics:**

  Some incident classes were ambiguous and not really relevant to the current working of the teams.

  Surely, this problem is justified among other things by similar causes as described before. However, the main problem is due to a missing common accepted incident classification. On basis of the work of Telia/CC a scheme was adapted for eCSIRT.net statistics approach.

  Therefore it wasn't surprising that at the first attempt not everything was still to the best. In addition, in this case by application and integration of the incident classification scheme into the incident handling an improvement of the force of expression of the statistics will have to be expected in the future.

  The bases for the statistic collections were changed starting from September. Therefore statistics are shown for the time periods January till August and furthermore from September.

Unlike the organizational problems the technical realization proceeded smoothly for the collection and presentation of the statistical data. Since without exception approved applications and development tools were used. The confidentiality, integrity and authenticity of the transmitted information is guaranteed by using standardized cryptographic techniques (SSL/TLS). However, if statistics are to be produced in the future – as desired of all teams – a database must be used as with type 3 statistics, since the storage of the information within simple files does not scale. Data concerning the workload, resources spent and incident handled are provided manually using web forms. This allows a consistent and convenient reporting but leads to a small increase in the workload.

After completion of all work the following facts are given:

- According to the agreements of the Clearinghouse Policy, incident statistics are available - in a generalized and sanitized way - to the public. These statistics provide valuable information about incidents handled by the participating teams and about the general hazard level of internet connected systems.

- The internal eCSIRT.net statistics are available - in a still somewhat anonymous form - for all participating teams. In contrast to the generalized and sanitized public statistics the internal statistics contain more comprehensive information. These statistics provide detailed information about the workload and resources spend by each team. As well information about the processed incidents is contained. This enables each team to better understand trends and helps to provide a better service to the respective constituency.

2.2.2 To Do for Type 1 and 2 Statistics

- The incident classification scheme must be evaluated and enlarged if necessary by a larger group of teams. It is recommended to use TF-CSIRT or at least the TI Accredidated teams as forum for this.
- As well the integration of statistical functions into incident handling systems must be further researched and improved.
- An automatic anonymisation process is necessary for building statistical functions across multiple organizations.

2.2.3 Type 3 Statistics

One of the purposes of the clearinghouse function was to gather information on real attacks in the networks and get some insights in the general level of attacks to internet connected systems. This information should support the building of public awareness against the threats of the internet.

To be able to collect the necessary information Intrusion Detection Systems (IDS) were deployed in the networks of the project partners. These systems should collect data on real attacks and report them to a central management console.

The realization of this infrastructure took place in the following steps:

- Agreement on the level of detail of the collected information that each partner is willing to publish from his own network traffic.
- Identifying (Open Source) software to implement the intrusion detection mechanisms and the central database component.
- Implementation of an easy to deploy software that enables the partners to collect and log the data.
- A test and collection phase in which the data was collected.
- Creation of the internal and public statistics generated from the collected data.

The following paragraphs give a detailed description of these steps. The last sections present a summary of the lessons learned and future enhancements necessary to improve the established system.

Specification of requirements

One of the most important aspects of the collection of attack data is the sensitivity of the data in regard to privacy. Each logged attack can disclose information on IP addresses, provided services, installed software and transferred information of attackers and victims. Network based Intrusion Detection Systems are even able to monitor the whole traffic of the subnet they are placed in. Because of the privacy issues the partners agreed to collect only the data of single hosts which only server the purpose of the eCSIRT.net data collection. This decision proved to be a solution to another problem of intrusion detection techniques:

It is always difficult to differentiate between acts of scanning (as preparation for following attacks) and normal usage. For example an ICMP ping packet can be a means of scanning, but also a valid test to check for the availability of a host providing a requested service. On a host used only for the IDS data collection each packet that reaches the host can be regarded as abnormal use because no service is provided by this host to the public.

After some discussion the partners agreed that the collected data of each sensor should be accessible by each of the participating partners but not by the public. This way the teams get detailed information about the monitored attacks and excerpts from the data records can be included in according incident reports if necessary.

The statistics to be given to the public are generated from the full set of collected data, but they provide only summaries of the attacks so no direct conclusions can be drawn on the placement of the sensors and the number of attacks in each partners network.

For the encrypted and authenticated transmission of attack data the necessary cryptographic keys were exchanged using the already established trust of the TERENA Trusted-Introducer Service (http://www.ti.terena.nl/) according to the Clearinghouse Policy.

Implementation

For the realization of the Type-3 statistics a distributed IDS with central logging had to be deployed. Because the logging of the monitored attacks takes place over the internet, the data has to be transmitted in an encrypted and authenticated manner. An outstanding example of Open-Source IDS software that meets these requirements is the Prelude IDS (http://www.prelude-ids.org/) which uses encrypted SSL connections and client certificates for the logging. A further advantage of Prelude is its usage of IDMEF (Intrusion Detection Message Exchange Format) which is standardized by the IETF (http://www.ietf.org/html.charters/idwg-charter.html).

Only the network based components of Prelude were chosen because all attacks from the internet can be monitored on the network interface. One further issue had to be solved for the implementation: To monitor attacks to TCP-based services, the connection attempts of the attacker have to be answered by the attacked system (otherwise the connection is never established and the actual attack will never be started). Honeypot technologies were chosen as a service to establish TCP connections and even to answer to service specific requests.

Honeyd (http://www.citi.umich.edu/u/provos/honeyd/) is used to simulate some of the most common services that are targets of TCP-based attacks. The following services can be simulated by existing honeyd scripts:

- SMTP
- WWW
- TELNET
- SSH (only the first packet exchange before cryptographic techniques are used)
- FTP
- POP3

Some other attacks that do not necessarily need fully established TCP-connections (as UDP DNS requests, ICMP ECHO requests and TCP SYN scanning) can also be seen by the network based IDS component.

Because the data on the different sensors is logged to a central collector and some correlation between the alerts needs to be done, the clocks of the different sensors need to be synchronized very precisely. This ensures that each sensor creates reasonable detection time stamps for each attack. Otherwise it cannot be guaranteed that after the generation of the statistics some new alerts with old timestamps are written into the database (and adulterate the data). For this purpose a network time protocol (ntp) service was established. The central eCSIRT.net server is connected to a radio controlled DCF-77 hardware clock and synchronizes the time on each of the deployed sensors. The process of synchronization is also secured by cryptographic techniques.

To enable the teams to easily deploy the necessary, complex IDS sensors a bootable Linux CDROM was prepared that included the complete sensor software and a user interface for the necessary configuration. In this way the teams were able to realize a sensor in their own network within a few hours. The only difficulty unforeseen was some very specific traffic that is normally logged by the IDS (for example a multicast protocol running in one of the research network), which produced thousands of false alerts. This could be fixed with a second release of the bootable CDROM that included some changes in the IDS configuration.

The public statistics required some evaluation scripts that queried the attack database and generated according charts that are included automatically in the according web pages.

The access of the eCSIRT.net partners to the logged attack data is realized by the web-based management console of the Prelude IDS. This front-end provides not only display- and filter-functions for all collected alerts but also configurable statistics about the attacks and attackers.

Additionally a webpage of special internal statistics is generated automatically.

Collection phase

On the 28th of August 2003 the necessary cryptographic keys for the operation of the IDS sensors were distributed to the first partners. On the 1st of September 2003 the first sensor was deployed at DFN-CERT. One week later 4 sensors were already up and running. A total of 7 sensors was established in the middle of October. The collection of data took place continuously (with the exception of the 10th of October, when a fatal server crash required some work on the management console) until now. In this time more than 600.000 attacks were monitored by the sensors, the biggest amounts of which were ICMP scanning, IIS root.exe and cmd.exe Trials which are usually caused by the Nimda worm and HTTP URL-escape attacks.

Public Statistics

For the public statistics a webpage is generated automatically on which the different types of statistics are displayed. Actually there are four different statistics generated:

- The number of attacks per hour. The number of all attacks within each hour since 2003-09-01 seen by the sensors are displayed day by day. They are divided into the main classes of attacks that were collected by the system:
    - IIS cmd.exe and root.exe access (as tried by the Nimda worm)
    - Other IIS attacks (attacks that work on IIS only)
    - HTTP request string alerts (all fiddling with URLs concerning the path and the encoding)
    - Other WEB attacks (all other attacks for WWW-Servers)
    - ICMP-Scans (different kinds of ICMP Echo Requests)
    - All other alerts
- The number of attacks per day. The number of all attacks within each day since 2003-09-01 seen by the sensors are displayed in a monthly graph. The different classes displayed are the same as in the hourly statistics.
- The number of different attacks used by each single attacker. This gives an insight in how many different attacks exist in the repository of each attacker.
- The number of sensors attacked by a single host.

  This throws some light on the level of activity of the attackers. Obviously some attackers probed all the existing sensors of the eCSIRT.net project, so they seem to try lots of hosts in the internet in a very short time.

Internal Statistics

The participating partners have access to the web front-end of the IDS console. That way the teams can view all the logged alerts in detail. There are some statistical functions integrated into the webfrontend, as the list of top 20 attacks and top 20 attackers, as well as some customizable charts.

To get an overview of the characteristics of the different attacks in the different networks of the sensors a webpage displaying internal statistics was created. It shows the main classes of the logged alerts for each sensor.

Lessons learned

For the initial registration of each participant and the distribution of the necessary cryptographic keys the existence of a verified database of the partners contact information was essential. For this purpose the information of the Trusted Introducer Service of TERENA (http://www.ti.terena.nl/) could be used.

The choice of the sensor software was easy, the necessary modules already existed as open source software. The creation of a bootable CDROM for easy deployment of IDS sensors required much more efforts. A lot of work had to be spent on the solutions to problems raised by the concept of diskless sensors. So the logging had to be reduced accordingly and the configuration of the services have to be provided on a floppy disk. Even more work was required especially by the development of the necessary initialization scripts for each service.

The easy setup of IDS components and honey pot services hides the complex configuration process from the users. The deployment of the sensors was done by the partners which were able to complete this task within a few hours.

The complex sensor network showed that the common language for the logging of IDS data, IDMEF (Intrusion Detection Message Exchange Language), is a working means for gathering attack data in a widely distributed network.

The decision to log only data from single honey pot systems proved to be an easy solution that helped to avoid many problems. By using honey pots only no data of valid network usage is recorded so there were no concerns about the privacy of the data.

Honey pots are autonomous systems on their own, so for the configuration of the network based IDS sensor only those services had to be considered, that are provided by the system itself. So the configuration does not depend on the network environment it is deployed in (it only needs a valid IP address and some routing information).

After four month of data collection no further problems arose, so a very stable service was established during the project.

2.2.4 To Do for Type 3 Statistics

The further operation of the service would require some more work to increase the efficiency. Some of the most urgent tasks are described in the following paragraphs.

To be able to monitor TCP-based attacks honeyd was used to answer to the according requests of the attackers. There is only a small set of services that can be emulated by the published scripts for honeyd. The most important one, http, works sufficiently for most of the simple requests, others (telnet, ssh) would need further enhancement to be able to fake serious attackers. To see attacks on less common services (eg imap), additional scripts should be developed.

This would widen the spectrum of visible attacks.

For the consistency of the logged data all IDS sensors were configured using the same rules to detect attacks. This makes the logged data of the different sensors comparable.

On the other hand this restricts the ability of the sensors to detect very new attacks. A storm of attacks caused by a new internet worm could be simply ignored because no rules are configured that match this kind of attack.

An easy way to realize an updating mechanism would be to fetch the latest rule set daily from a server using SSL or SSH.

Using the established framework of the Trusted Introducer (TI) service, the exchange of private information (eg secret keys for the sensors) could be accomplished very easily. For the participation of further teams in the data collection, the actual TI service is not sufficient, because it only provides verified contact information for European CSIRT teams. The participation of the Japanese team (JPCERT/CC) for example, which provide important information from other regions, required the availability of information not readily available.

2.3 The Alert Function

The primary aim of the eCSIRT.net project is to improve the cooperation between the partners in the areas of incident handling. Therefore an alert function was implemented to realize fast exchange of important and time critical information about unusual events and attacks. Beside an Internet based component (in-band) a backup solution (out-band) was implemented to guarantee communication between the teams during crises.

Until now, a none-Internet-based communication infrastructure wasn't available for CSIRTs within an international cooperation. In this case a new subject area was treated. The availability of technical solutions does not represent the problem, but an insufficient common understanding and missing agreements. Therefore lengthy discussions were necessary to find an acceptable agreement regarding the generation of warnings and emergency alerts. The essential conclusions of the Alert Policy are:

- Definition of a framework for the participation in the Alert Function
- Communication and Communication Security
- Specification of a format for information exchange
- Use of the alert function

2.3.1 In-band alert function

The internet based alert function of the eCSIRT.net was implemented as an enhancement of the existing communication infrastructure. The building block of the in-band function is realized by a mailing list. The essential reason for the decision to use a mailing list for the alert function instead of a web based solution was that E-mail is the preferred communication medium of the participating teams. All modules of the alert function are running on LINUX based platforms and were realized with open source software except of the E-Mail gateway for securing the alert messages.

According to the alert policy the support of e-mail security services is absolutely mandatory in order to guarantee confidentiality and authenticity for any communication over the Internet. Furthermore the Support of different security standards should be satisfied. At present no open source software which fulfill these requirements was available so that commercial products had to be taken into account. However, a sponsor was identified for this project whose product the given requirements more than fulfilled. The SecureMail Gateway provided by bone labs operates as Proxy-Server.

Caused by the long standardization process the integration of IODEF into the working processes of the participating takes place quite late. Therefore a central solution based on web-forms was implemented to support the teams. An IODEF XML object is generated from the entered data and sent together with an ASCII representation to the mailing list. Through this the participating teams must satisfy only few technical requirements to the participation in the alert function, just a functional email address and a corresponding OpenPGP-Key or X.509 certificate. Very helpful for the establishment of the security services was the application of the TI accreditation framework, by which the correctness of the most important contact information was ensured.

The trial operation of the in-band alert function ran with respect to the used technology without problems. A few minor problems arose by the standardization of IODEF which was situated in the development and by representation problems of the web-forms at some browsers.

But during the trial operation some deficits were uncovered. The absence of the acknowledgment of receipt was criticized by the teams, so that such a function was implemented is now available as well.

2.3.2 Out-of-band alert function

In addition and as backup for the internet based alert function a second system was implemented which is based on telecommunication networks (In this case ISDN was chosen). The building block for the out-of-band alert function was realized just like the implementation of the other services by open source software. In this case GNU Bayonne, the telecommunications application server of the GNU project was used. The out-of-band alert system work partial like an answering machine (recording of messages, remote play-back, ...) but was extended by important functions: e.g. user Identification with UID and PIN, dialer with an auto retry function, logging and archiving of voice-mails.

Essentially two reasons are responsible for selecting this solution and not a commercial product that could have been chosen for this project as well:

- Available products would have had to be modified, in order to fulfill the requirements of the alert policy.
- The development and operating costs should be in a tolerable frame for this trial.

For this reason the out-of-band system was connected only with two lines to the telecommunications network for the project. For the use within such a small project group this dimension is sufficient. At an average length of two minutes for a voice-mail each team can be informed within 15 minutes. However, the practical limits of the system were shown in the test. As soon as incoming and outgoing calls had to be processed at the same time, the quality of the voice-mail system sank and the distribution of the messages was stretched. Based on improved hardware including active ISDN cards with their own processor, this situation should not arise. We set a high value on the scalability of the system, so that by the employment of better hardware and more network connections these restrictions will not arise any longer in a real service.

In the test operation the system was extended continuously with further functions. The implementation of the SMS functionality is to be emphasized thereby. In addition to the original voice-mail each team also is informed - if desired and available - with a SMS message that an alarm was triggered. However, the content of the current alert must be queried through a call to the alert system. Especially during out of hours coverage receiving a SMS provides some easy ways of handling the hotline.

After completion of all work the following facts are given:

> According to the agreements of the Alert Policy an infrastructure service to distribute warnings and alerts was implemented. By the implementation of the function it is ensured that:
>
> - the distribution of information is authentic and comes from an registered team
> - the distribution of information is possible even in times the traditional E-Mail exchange via the Internet (so called in-bound communication) is not available
> - different communication mechanisms are supported so that the possibility is reduced for a "single point of the failure" if one mechanism is no longer available.
>
> All participating teams in the service will gain valuable time they in turn can utilize to:
>
> - detect events, attacks and incidents otherwise not noted in time due to the lack of critical information
> - avoid attacks and incidents by applying ad-hoc countermeasures
> - limit the impact of any attack or incident that already occurred in their constituency by identifying traces based on the delivered information

2.3.3 To Do

At the in-band alert function the acknowledgement of receipt should be enlarged to the effect that also alert messages which are not generated by the web-form can be confirmed. As well the implementation of a web-form to get an overview of current alarms would be desirable.

At the out-of-band alert function it must be made sure that the time and the originator are on spoken. An automatic insertion of a time stamp and the originator of the message would be conceivable here. As well the availability of the distribution of fax-messages would be desirable.

2.4 eCSIRT.net from a member perspective

JANET-CERT has been an active partner of the eCSIRT project from its inception. Most of the work was completed by two of it's members Andy Bone the JANET-CERT Manager and John Green a team member. The team has viewed the overall project as being successful and chiefly meeting all its aims.

There have been several benefits to JANET-CERT and its constituents:

Primarily in **co-operation**, the creation and signing of a Code of Conduct for the CSIRTs was a major success and we believe with minor changes that this could be incorporated within the TERENA TF-CSIRT trusted-introducer program. To would tie teams in to using good practices and standards when dealing with multi national incidents and increase the trust between teams for the sharing of information.

The other major success of the project has been the **exchange of incident handling information** using IODEF. The project has shown that with co-ordination this protocol could become the standard with which all teams throughout the world exchange incident Handling data. The partners successfully managed, even with very different internal systems to exchange comprehensible and useful incident data.

JANET-CERT now intend to try and incorporate this protocol into the Request Tracker Incident Response (RTIR) Handling system for automated message storage and handling, not only with other CSIRTs but within its own network and constituencies. This project has been an excellent proving ground for this purpose and the team hope we may be able to extend this either through a new project or the TF-CSIRT environment.

The **"out of", and "in bound" alerting system** has also been a very useful exercise after some initial problems the service is now a useful addition to the teams arsenal against potential network disturbance. The benefit of early warning, is not only paramount to any CSIRT, but also its constituents, as it allows the CSIRT to give advanced warnings of potential threats, which could affect constituent sites on their network. The team would again hope to see this service continue and expand with the introduction of new teams.

The **statistics** generated from the partners of the project are useful, not only for their local management but for their constituents. Potential threats and trends can be considered and it also allows teams to make judgments on their performance against other teams. It is hoped that the partners continue to add their figures and maintain their sensors, and that other teams within the European TF-CSIRT join us in producing a picture of European activity.

Overall, JANET-CERT believe that this project has achieved a great deal in moving forward co-operation among CSIRTS in Europe, However, its important that the projects services are not lost and able to grow, this is the next challenge for the eCSIRT.net partners, whether through a similar project or the TF-CSIRT.

3 Achievements of the Project

3.1 Original Problem Statement

In the project proposal the following characteristics of the CSIRT co-operation were given. To allow a better differentiation, the old situation is listed within boxes:

Established communication: Based on Internet-based email only. Telephone and telefax might be used to confirm specific information or to discuss potential approaches.

Recent discussions have introduced IRC as another communication means, but this situation has not changed and is not expected to change in the near future.

For the exchange of incident related information still Internet-based communication is needed, in native mode at least – without the help of any email gateway or such.

No backup for Internet-based email.

For Alerting at least a backup for Internet email is available.

Established communication security: Based on PGP encryption and digital signatures. Keys are authenticated on an ad-hoc basis through CSIRT-to-CSIRT communication.

For the cryptographic mailing list not only PGP was used but also S/MIME. This not only provides a gateway between both "communities" but also removes both groups to support an application they have no real need to maintain.

Keys are authenticated before integration into the cryptographic mailing list, so at the time of the communication there is no doubt about the security or authenticity.

No key infrastructure.

For the purpose of the providing access to the protected group server as well as for important infrastructure components SSL Client Certificates are mandatory. To allow for a scaling approach an own CA was established. The Client Certificates would support email applications as well, given that an email address would be integrated, and the CA itself is not limited in it's support for other applications.

Established informal knowledge-transfer: If events are of enough interest or seem to be important, they might be shared with other teams.

During the course of the project, at least every two month on average a meeting was held. As these meetings were combined with other meetings as well, the participants got a great deal of opportunities to discuss and learn about other developments and projects from other teams.

No guidelines or requirements what should be shared with whom.

The established code of conduct provides a common ground for all participating CSIRTs. But this would not have been sufficient, therefore for specific services like statistics and alerting individual policy statements were developed. This provide efficient guidelines for any application of the services as well as setting a stage for issues not settled by any policy statement.

Supported integration of new entities: New CSIRTs are presented to the community by means of the European CSIRT Directory (TI, http://www.ti.terena.nl), for other areas of our global communities such directories are missing.

This was outside the scope of the project and was therefore not considered.

No formal integration of new CSIRTs. No efforts are made to formally introduce new teams, although each team is welcome to sign up for accreditation under the TI framework.

This was outside the scope of the project and was therefore not considered.

Successful cooperation on case by case basis: CSIRTs involved with the same incidents will share information based on a case by case basis and on the need to know principle.

This was outside the scope of the project and was therefore not considered.

No predetermined rules for cooperation on a routine basis.

This was outside the scope of the project and was therefore not considered.

Limited availability of statistical or trend analysis outside the CSIRT community: While value added information is available to single and cooperating teams it is rarely made available outside the CSIRT community.

The statistic function provides the basic mechanism for collecting information in order to develop meaningful statistical and / or trend information.

No availability of early warning information.

This was outside the scope of the project and was therefore not considered in detail, although the availability of specific information by the statistic function can provide a heads-up for participating CSIRTs.

No established way of providing sanitized information to the public.

As part of the statistic function the information is presented in two different views. While the restricted version for participating members only includes more detailed facts that might be used to identify a single team, such information is not available to the public. But still the public available presentation provides insights not available otherwise.

The eCSIRT.net project aimed to address – directly and indirectly – the recognized limitations and missing benefits of an established CSIRT infrastructure. By concentrating on the CSIRT-to-CSIRT communication and cooperation, an overall improvement for all participating CSIRTs can be achieved in regard to various aspect. The innovation is not only related to specific new technology but to new solutions to existing problems and new operational practices, but this paper will concentrate on three areas, that are approached via technical solutions that can be utilized in the environment of other CSIRTs as well.

To summarize the achievements therefore it is a fair statement to say:

1. **Improved communication:** By applying new established protocols – namely IODEF and IDMEF – communication is now defined in a formalized way that would allow a much better integration into the workflows and henceforth enable semi-automated handling of new incoming reports and facilitate complete and timely reporting to other CSIRTs.

   To be able to allow for this, there need to be a recognized and accepted common language for CSIRTs, that describe events and data of common interest in a unique and well understood fashion. While the protocols implement a technical and syntax oriented solution, the integration into workflows demand a semantical solution to avoid, that the same set of data exchanged is interpreted differently from the CSIRTs involved.

   What could not be achieved? As a take-up project allows not for software development activities and as the planned resources would not have allowed that anyway, there was no way to overcome one of the practical deficits recognized during the project: The availability of an IODEF-enabled helpdesk solution. As the finalization of the IETF definitions took much longer then expected, the availability of implementations is limited to Open Source Solutions. To exchange incident related information therefore simpler filter and im-/export solutions needed to be integrated into the existing infrastructure of the partners which proved to be difficult.

2. **Sanitized insights into the CSIRT community through public statistical and trend analysis:** While there is a clear need for confidentiality and privacy related to incidents, the silence about incidents, attack and their impact on the organizations as well as the society at large is not helpful. Based on the established common definitions and understanding necessary for the improved exchange of incident / attack related data, all events will already labeled in a standardized way. Thereby the collection and presentation of statistical analysis is made possible without much additional effort, as today any analysis would require to transform all data towards a common language first. The availability of any statistical and trend analysis is important for the teams, as they will gain arguments to support their position and services.

   In addition the data analysis will allow insights into the work of CSIRTs which would allow them to adjust their work accordingly to new trends. Without real insights which are available outside the CSIRT community the threats cannot be evaluated nor addressed on the policy level.

   What could not be achieved? As the automatic generation of statistics based on real incident information needs to involve a complex process of sanitization. This cannot be done manually for any larger number of incidents, as too much overhead would be involved. But without effective sanitization no data would be made available from CSIRTs to any third party. As the organizational and even legal problems were not foreseen for the project, this could not be addressed from within. Instead, other approaches were applied to overcome this underlying problem and still provide the much needed information.

3. **Backup for Internet-based communication especially in regard to alerts:** While all incidents and attacks are important to the impacted users and organizations, the need for 24 by 7 (round the clock) helpdesks and service offerings are still rare. But global attacks like Nimda, Code Red, Blaster or vulnerabilities like the SNMP weaknesses require immediate attention and at least the timely dissemination of heads-up and alert messages. As it is clear from the past experiences that the network itself will be impacted, backup for Internet-based communication is mandatory to allow CSIRT-to-CSIRT communication during crisis's. The project has developed effective alert mechanisms and based on the feedback during the project, not only the alerting itself, but also acknowledgement functions were developed.

   What could not be achieved? The sending of large documents during crisis's was identified as potential problem. One obvious solution would have been the establishment of a fax server, but as this was not expected during the preparation for the project, and no resources were left, this was only documented as a component of any future service.

4 Take-Up of eCSIRT.net Services

During the TF-CSIRT Meeting in Madrid, Spain, the take-up of the eCSIRT.net services was discussed within the community of European CSIRTs. Even before, there were some decisions made in regard to continuation of some of the services and efforts.

Basically there are three options for each contribution / service of the project:

1. Input to TF-CSIRT Working Groups, as these already know about the project and some services
2. Take-Up by TI as service oriented community
3. Take-Up by Volunteers

4.1 Input to TF-CSIRT Working Groups

Some results have been tailored towards the needs of the project. While they still serve as an example and have proven to be sufficient for the partners, such sensitive documents like any Code of Conduct needs more discussion within a group that should apply this code. In addition as the scope of the European CSIRT community is broader then the project, other considerations might as well provide enough reasons to change it or at least add to it.

Topics for TF-CSIRT Working Groups:

- **Code of Conduct** - The group of TI Accredidated Teams is developing a code, taken this document into consideration.
- **eCSIRT.net Common Language (WP2 and WP3)** - As the IETF finally concludes the work on the IODEF syntax definitions, the TF-CSIRT will continue to adopt an agreed upon interpretation of the IODEF exchange format. This will heavily build upon the Common Language defined in the project.
- **Integration of IODEF into Helpdesk solutions** – As the unavailability of IODEF-enabled helpdesk solutions caused much problems in the project, several members have started to incorporate libraries or filters in their environment. One member – Janet-CERT – will however start to fully integrate the IODEF functionality in their new Helpdesk solution.

4.2 Take-Up by TI Accredited Teams

The stable pilot services developed in the project - **WP4 Statistics Type 1 and 2 as well as WP5 Alerting** - could become part of a service delivery available to the European CSIRT community. Discussions with the TI Accredidated Teams however showed, that although enough was said on the functions and techniques, they would like to get an impression of the "look and feel".

To overcome this factor, it was agreed that during the phase from Mid of February to End of March 2003 tests for all TI Accredidated that would wish to participate in the test will be arranged. Thereafter, after collecting the feedback from the field test, a proposal will be considered in time for the next TF-CSIRT Meeting in Hamburg in May 2004.

4.3 Continuation as Volunteer Project

As some part of the project - most interestingly the IDS sensor network - caused much discussion and as there was no consensus, whether such network would be beneficial to all, and as the setup is far from being anywhere near the definition of a "service", it was felt that the network should be continued based on the efforts of volunteers:

- **NTP Crypto Time Server -** This component is necessary and will be continued by PRESECURE.
- **Collector for Sensor Network -** PRESECURE will continue to provide the hardware and resources for maintaining the Collector as well as to provide access from participating teams to it.
- **Future Extensions -** Future extensions like allowing an automatic update of configurations as well as signature files based on a secured master site needs to be developed. The work involved will be coordinated by PRESECURE, but efforts of all interested are needed to implement much desired new functions.
- **Participation -** To allow participation on the one hand without exposing the network to a group which does not know what to expect from each other, it was envisioned, that the participation would be offered to TI Accredidated Teams. Such teams would not need any other justification, while other teams - especially from the international realm - would need to be handled differently. It is mandatory, that each decision is taken by the group instead of one individual, as the success of the network is also tied towards the security felt by the participants.

5 Presentations and Papers

This chapter lists all presentations and reports about the project.

5.1 TERENA TF-CSIRT, May 2002

As the partnes of the project are all involved with the TF-CSIRT since its conception and are tied to the TI accreditation framework, it was believed to inform other CSIRTs as early and as complete as possible. Henceforth the May 2002 was taken as a chance to present the project outline and goals to the European CSIRT community.

The slides are available from the TF-CSIRT website: http://www.terena.nl/tech/certs

5.2 FIRST Conference, June 2002

Similarly as to the TF-CSIRT most partners of the project are involved in the international FIRST forum. Originally it was thought that the project would start on 1 June 2002, therefore the FIRST Conference was believed to be a good place to gain international awareness. As to the time the project was accepted the Conference program was already established, a submission to a panel on new developments was accepted.

The slides are available from the FIRST website: http://www.first.org

5.3 International CERT-RO Symposium, August 2002, Amsterdam

Klaus-Peter Kossakowski and Don Stikvoort were invited guests and speakers on the “International Symposium CERT-RO”, a closed symposium organised by the Dutch Government CSIRT “CERT-RO”, which took place August 27-28 in Amsterdam, The Netherlands. The topics were CSIRT regionalisation and cooperation, and Critical Infrastructure Protection (CIP). The importance of developments like eCSIRT.net to facilitate the inter- and extra-regional cooperation of CSIRTs, and to enable early-warning capabilities that will also benefit CIP, was emphasized by the attendees. [3]

5.4 TERENA TF-CSIRT, September 2002

As the partnes of the project are all involved with the TF-CSIRT since its conception and are tied to the TI accreditation framework, it was believed to inform other CSIRTs as early and as complete as possible. Henceforth the May 2002 was taken as a first chance to present the project outline and goals to the European CSIRT community. An update was provided during the September 2002 TF-CSIRT meeting as well.

The slides are available from the TF-CSIRT website: http://www.terena.nl/tech/certs

5.5 IETF Meeting, Atlanta, USA, November 2002

As the partners of the project are depending on the overall progress of the IETF driven development of IODEF and IDMEF, it was already proposed within the project proposal, to closely follow this development.

[3] The symposium minutes are non-public, however representatives from the Comission of the European Communities attended as well.

Henceforth the November 2002 IETF Meeting was taken as a chance to start the active participation within the working group. A presentation outlining the project and its goals to the International community was given.

5.6 French Security Working Group, Rennes, France, December 2002

CERT Renater presented the status and the IODEF approach with its applications for CSIRT activities.

5.7 TERENA TF-CSIRT, Zagreb, Croatia, January 2003

Don Stikvoort of Stelvio, on behalf of eCSIRT.net, presented the eCSIRT.net project and state of affairs to the TF-CSIRT community at the same event

The slides are available from the TF-CSIRT website: http://www.terena.nl/tech/certs

5.8 UKCERT Information Sharing Meeting, UK, February 2003

JANET-CERT presented the approaches developed and tested by eCSIRT.net for information sharing during a meeting of UK CERTs and related teams from industry, government and military.

5.9 DFN-Betriebstagung, Berlin, Germany, March 2003

DFN-CERT presented the eCSIRT.net defined usage of the standards to interested administrators in order to start developing more automated ways of exchanging data between sites involved in large scale attacks.

5.10 IETF INCH WG Meeting, March 2003

During this IETF meeting the participants of eCSIRT.net made a small presentations of the goals and desired outcomes of the project. They also participated and presented the reasoning for the changes made during the February 2003 interim meeting.

5.11 German CERT Meeting, Bonn, Germany, April 2003

Jürgen Sander provided an introduction into the project and its current status during a meeting of all German CSIRTs in April 2003.

5.12 IFIP Sec/2003, Athens, Greece, May 2003

The presentation and paper "Efficient co-operation of CSIRTs" for the IFIP/Sec 2003 conference focused on the technical challenges the eCSIRT.net project is facing. Firstly, in establishing a standardized common language for efficient inter-CSIRT communication and exchange of incident-related information, and secondly, the challenge of implementing efficient early-warning systems for incident handling on a large, global scale in an operational setting.

The IFIP paper was written by Arne Helme and Don Stikvoort of Stelvio, and Klaus-Peter Kossakowski of PreSecure. Arne Helme of Stelvio gave the presentation in Athens on behalf of eCSIRT.net. His travel report can be read below. The paper was included in the IFIP conference proceedings.

5.13 ES Security Group Review, Madrid, Spain, May 2003

IRIS-CERT presented it's current re-design of processes and internal infrastructure to a Spanish Security Group for identifying ways to improve the exchange of incident and attack related data.

5.14 UKCERT Information Sharing Meeting, UK, February 2003

JANET-CERT was requested to elaborate after the first presentation in March 2003, how the common language is used in responding to incidents and who such usage can be integrated into the CSIRT co-operation.

5.15 TF-CSIRT Warsaw, Poland, May 2003

The 9th TF-CSIRT Meeting was attended on request of TERENA to present an update on the project development. The presentation concentrated on the following topics:

- Code of Conduct
- Policy considerations for Clearinghouse and Alert Function
- Technical infrastructure for Internet-based and Out-of-Internet alerting

5.16 AFCEA Conference, Poland, May 2003

CERT-Polska presented to industry, government and military IODEF as establishing standard for improved automated information exchange within the CSIRT community.

5.17 JANET Security Conference, UK, June 2003

During its annual security conference, JANET-CERT presented their new helpdesk solution with the full integration of IODEF enabled communication.

5.18 FIRST 2003, Canada, June 2003

A presentation by Klaus-Peter Kossakowski was accepted by the program committee to review the Automatic Exchange of incident related data – and its application in CSIRT Operations. As the eCSIRT.net project aims to address – directly and indirectly – the recognized limitations and missing benefits of an established CSIRT infrastructure, it does so by concentrating on the CSIRT-to-CSIRT communication and cooperation. By adopting the approaches developed, an overall improvement for all participating CSIRTs can be achieved in regard to various aspect. The innovation is not only related to specific new technology but to new solutions to existing problems and new operational practices. The presentation concentrated on three areas, that are approached via technical solutions that can be utilized in the environment of other CSIRTs as well:

1. Improved communication
2. Sanitized insights into the CSIRT community through public statistical and trend analysis
3. Backup for Internet-based communication especially in regard to alerts

5.19 Presentation to CERT/CC, Pittsburgh, USA, July 2003

CERT-Polska was visiting CERT/CC in July 2003 and during the informational sessions reported on the status and progress of eCSIRT.net. Ways of using IODEF in day-to-day interchange were discussed.

5.20 IETF INCH WG Meeting, Vienna, Austria, July 2003

During this IETF meeting the participants of eCSIRT.net reported on the practical integration issues the members of the project phased.

5.21 TF-CSIRT Amsterdam, The Netherlands, September 2003

The 10th TF-CSIRT Meeting was attended on request of TERENA to present an update on the project development.

5.22 German CERT Meeting, München, Germany, November 2003

Jürgen Sander provided a status update during a meeting of all German CSIRTs in September 2003 in Munich, Germany.

5.23 BITKOM, Berlin, Germany, November 2003

Jürgen Sander provided an introduction into the statistic and alert function as well as the sensor IDS network during a meeting of German IT industry specialist.

5.24 IETF INCH WG Meeting, Minnesota, USA, November 2003

At the 58th IETF in Minneapolis in November, as part of the INCH meeting on the 13th of November, three presentations were delivered stemming from the eCSIRT.net process:

- the eCSIRT.net common language
  - author: Arne Helme of Stelvio on behalf of eCSIRT.net
  - delivered by Roman Danyliw, INCH chair and liaision to eCSIRT.net, by absence of Arne Helme
- Presentation of the IHSH tool
  - author: Arne Helme of Stelvio on behalf of eCSIRT.net
  - delivered by Roman Danyliw, INCH chair and liaision to eCSIRT.net, by absence of Arne Helme
- presentation the remaining open issues in the IODEF datamodel
  - Jan Meijer, SURFnet/CERT-NL, liaison to eCSIRT.net