

01.08.05

Deliverable DJ2.5.1: Report on Activities and Recommendations of Advisory Panel



Deliverable DJ2.5.1:

Contractual Date: 31/8/2005
Actual Date: 01/08/05
Contract Number: 511082
Instrument type: Integrated Infrastructure Initiative (I3)
Activity: JRA2
Work Item: 5
Nature of Deliverable: R (Report)
Dissemination Level: PU-Public
Lead Partner: SWITCH
Document Code: GN2-05-141v4

Authors: Gilles André, Jimmy Arvidsson, Gorazd Bozic, Ghristoph Graf, Urpo Kaila, Jan Meijer, Marco Thorbrügge, Wilfried Wöber

Abstract

This deliverable reports about the composition, activities and recommendations of the advisory panel to JRA2. The panel consist of security specialists from several different fields and is intended to comment on the work carried out by JRA2, to give an overview of trends and evolution of network security and incident handling processes and to give recommendations for work in subsequent years of JRA2. This is the first deliverable of this panel, covering the first year of JRA2 activities.

Project:	GN2
Deliverable Number:	DJ2.5.1
Date of Issue:	01/08/05
EC Contract No.:	511082
Document Code:	GN2-05-141v4

Table of Contents

0	Executive Summary	iv
1	The JRA2 Advisory Panel	1
2	Composition of the Advisory Panel	2
3	Activities and Recommendations of the Advisory Panel	3
3.1	General Observations	4
3.1.1	Recommendations Based on Observations	4
3.2	Comments on the Work Carried out by JRA2	5
3.2.1	Work Item 1: Securing GN2 Network Elements and Services	5
3.2.2	Work Item 2: Building of Security Services	5
3.2.3	Work item 3: Designing and Establishing an Infrastructure for Co-ordinated Security Incident Handling	6
3.2.4	Work item 4: Relationship with TF-CSIRT	7
3.2.5	Work item 5: Establishment of an Advisory Panel	7
3.3	Overview of Trends Relevant to JRA2	7
3.3.1	Critical Information Infrastructure Protection (CIIP)	7
3.3.2	Legal	7
3.3.3	Convergence of Voice and Data	8
3.3.4	Overlay Networking	8
4	Conclusions	9
5	Acronyms	10

Table of Figures

Table 2.1: Composition of the advisory panel

2

Project:	GN2
Deliverable Number:	DJ2.5.1
Date of Issue:	01/08/05
EC Contract No.:	511082
Document Code:	GN2-05-141v4

0 Executive Summary

The GN2 JRA2 advisory panel consists of security specialists from several different fields relevant to network security. The Panel is tasked to comment on the work carried out by JRA2, to give an overview of trends and evolution of network security and incident handling processes and to give recommendations for work in subsequent years of JRA2.

The JRA2 activity leader and the TF-CSIRT chairman jointly selected the advisory panel during the first months of JRA2. A call for participation was made at the TF-CSIRT meeting in Malta in September 2004. The panel was initially presented to JRA2 and TF-CSIRT during the TF-CSIRT meeting in London in January 2005 and formally met during the TF-CSIRT meeting in Zurich in May 2005.

The following main trends relevant to JRA2 were identified, their relevance discussed and recommendations devised for future phases of JRA2:

- The availability and integrity of network-based services is becoming increasingly crucial
- Increasing enforcement of relevant laws and security practices to the “virtual” world
- Convergence of voice and data
- Security implications of overlay networks, such as bandwidth-on-demand links

1 The JRA2 Advisory Panel

The purpose of setting up the GN2 JRA2 advisory panel is to create a forum in which experts both from within GÉANT2 and outside of it discuss and shape the strategic direction of JRA2 during the lifetime of the project. The panel is selected jointly by the Activity Leader of JRA2 and the chairman of TF-CSIRT (TERENA Taskforce Collaboration of Computer Security Incident Response Teams) at the beginning of GÉANT2 and is composed of active members of TF-CSIRT, including experts from GÉANT2, security researchers, incident response individuals from R&E networking, industry and government.

The panel is explicitly tasked to address the following issues in its yearly deliverables: to comment on the work carried out by JRA2, to give an overview of trends and evolution of network security and incident handling processes and to give recommendations for work in subsequent years of JRA2.

2 Composition of the Advisory Panel

The JRA2 activity leader and the TF-CSIRT chairman jointly selected the advisory panel during the first months of JRA2. A call for participation was made at the TF-CSIRT meeting in Malta in September 2004 and the panel was initially presented to JRA2 and TF-CSIRT during the TF-CSIRT meeting in London in January 2005. A government CERT (Computer Emergency Response Team) representative was still missing at this time, the vacancy could be filled in May with Gilles André.

Name	Affiliation	Country	Field or function
Jan Meijer	Surfnet	The Netherlands	Advisory panel chairman, security researcher
Gorazd Bozic	ARNES	Slovenia	TF-CSIRT Chair, member ex officio
Christoph Graf	SWITCH	Switzerland	JRA2 Activity Leader, secretary ex officio
Jimmy Arvidsson	Telia-Sonera	Sweden	Industry participant
Marco Thorbruegge	DFN-CERT	Germany	R&E incident response expert
Urpo Kaila	Funet CERT/ CSC	Finland	R&E incident response expert
Wilfried Wöber	ACOnet	Austria	R&E incident response expert
Gilles André	CERT-A	France	Government CERT

Table 2.1: Composition of the advisory panel

3 **Activities and Recommendations of the Advisory Panel**

The advisory panel formally met once, adjacent to the TF-CSIRT meeting in Zurich, Switzerland, in May 2005 and approved the chairmanship of Jan Meijer. The remainder of this document is based on the discussion and findings during that meeting and discussions by mail and phone afterwards. Jimmy Arvidsson and Urpo Kaila were not able to be present at the meeting, but their input was obtained by the JRA2 Activity Leader after the meeting over email.

Project:	GN2
Deliverable Number:	DJ2.5.1
Date of Issue:	01/08/05
EC Contract No.:	511082
Document Code:	GN2-05-141v4

3.1 General Observations

Before going into details of the work carried out, we analyse the work plan of JRA2 during the first year of GÉANT2, its participants and devise some very general recommendations from those observations.

The vast majority of participants to the JRA2 activity are people involved in operational security within a NREN security team. This explains why the JRA2 participants form a natural subset of the participants of the Terena task force TF-CSIRT, with a rather similar membership from a larger community than GÉANT2.

The perceived benefit of the participants by obtaining technical and operational information, increasing skills and jointly developing tools and procedures is the main incentive and the lack of competitive elements a strong supporting element of the co-operation of CSIRTs in JRA2. This is particularly true for any activity, which involves the sharing of data. It is therefore important to show the relevance and benefit of any data sharing activity and not accept the principle of “data sharing” as beneficial per se.

For the majority of participants, the need to solve problems in their daily work and to improve effectiveness is the main incentive to participate in JRA2. All development activities are confined to areas where no appealing product is commercially available and the goal is to develop new tools to offer new services.

A minority of participants is driven by the desire to carry out long term research.

The fact that most JRA2 participants come from NREN security teams explains why the content of work item 2 (Building of security services) is solely about tools helping to solve problems on the basis of data gathered from the network. It is a major concern of those teams to keep their networks clean and fight misuse. Other groups of teams, namely government CERTs, do not have direct access to such data and do not feel directly responsible for or control a network with customer traffic. However, it should be noted that not all NREN security teams do have access to such data.

With the exception of work item 1 (Securing GN2 network elements and services), the work plan of JRA2 can be characterised as a wish list based on the needs of GN2 partner security teams (usually NREN CSIRTs).

3.1.1 Recommendations Based on Observations

Given the current composition of the participants in JRA2, the main focus in the future must not be on research per se, but on the perceived value for participating security teams. Considering the strong bias towards operational issues, a return on invested manpower must be rather clear and not too distant in the future.

In order to keep in touch with research, participation from teams with research interests should be maintained and encouraged or other measures should be put in place.

Not all teams have access to network generated data like netflow. Their needs are currently not taken care of and there is substantial risk that they will not be able to protect their networks in the same way. All NRENS should be encouraged to find ways to feed network-generated data to their security team.

3.2 Comments on the Work Carried out by JRA2

The panel is convinced that the work carried out by JRA2 is relevant to the GÉANT community and also beyond, to the private sector and particularly to ISPs. Our comments and recommendations address therefore only those aspects of the work, where we propose changes, foresee new opportunities or risks.

3.2.1 Work Item 1: Securing GN2 Network Elements and Services

The panel is commenting the discussion within JRA2 relating to the proposed addition of Denial-of-Services (DoS) mitigating devices into the core of GN2 in future phases. The main purpose of “The Toolset” introduced in Work Item 2 (Building of security services) is to provide analytical capabilities to security teams and will support detection and analysis of policy violations, namely DoS attacks. But “The Toolset” does not provide enforcement capabilities. DoS mitigating devices provide the capability to reduce the damage of DoS attacks at very short notice.

While DoS mitigating devices have undoubtedly positive effects on services being protected, it is not evident that placing them into the core of GN2 is providing best use of such equipment. Ideally, DoS mitigating devices should be located topologically as far away as possible from the service being protected, but still able to attract traffic from all relevant sources. The core of GÉANT2 is a suitable location to protect services within NRENS with GÉANT2 as primary upstream provider. Services located within NRENS with other primary upstream providers than GÉANT2, such DoS mitigating devices are less effective.

The varying usefulness of the DoS mitigating devices should be taken into consideration, when deciding about including DoS mitigating devices in the GÉANT core. Some statistical figures about DoS activity on the GÉANT core would be helpful for the same purpose, too.

3.2.2 Work Item 2: Building of Security Services

The main focus of this work item is a collection of tools, referred to as “The Toolset”. Its goal is give the GÉANT partner’s security teams the capability to effectively enhance the security of services run across GÉANT. Its area of application is therefore covering the backbone of GÉANT2, the NREN backbones and campus networks.

The work carried out in WI2 is very much dependant on the availability of netflow data gathered from the network to provide input for “The Toolset”. This is fine for the moment, and netflow is likely to stay an important source of information during the years to come. The availability of netflow data is, however, endangered from

Project:	GN2
Deliverable Number:	DJ2.5.1
Date of Issue:	01/08/05
EC Contract No.:	511082
Document Code:	GN2-05-141v4

several perspectives: equipment capable of providing netflow data is more expensive than equipment not offering that feature and scalability to higher speeds is not necessarily guaranteed. Efforts must be taken to manage the reliance on the availability of netflow appropriately. This can happen in two ways: by securing the availability of netflow data or by reducing the reliance on netflow data. The former can be achieved either by making netflow an important requirement in future equipment decisions or by adding dedicated netflow providers to the network. The latter can be achieved by using other sources of traffic related data, e.g. traffic scanners.

Making the availability of netflow data an important requirement is recommended for the time being. The capabilities of netflow based tools are impressive and not easily replaced with other tools. While complete netflow data is an interesting asset, netflow data from sampled traffic is still very useful and - within limits - quite acceptable. The Panel recommends addressing cost and scalability issues by weighting against the sampling rate.

Another approach is to rely on other information sources, e.g. traffic scanners. A clear advantage of traffic scanners over netflow is, that such scanners can additionally base decisions on the payload of network traffic. Netflow, on the other hand, is limited to traffic metadata, like TCP/IP header and routing information. While this is an interesting research topic deserving attention and support, we discourage the allocation of high amounts of effort in this activity for the following reasons:

- it is a high risk research activity, which is not well fitting the operational and result-driven participants of JRA2
- the value of basing decisions on the contents of network traffic is expected to reduce over time, as network traffic encryption is increasing
- evaluating network traffic metadata is much safer from violating privacy regulations than evaluating the contents of network traffic

Other sources of traffic metadata should be assessed for applicability within the scope of JRA2 to reduce the reliance on netflow data.

3.2.3 Work item 3: Designing and Establishing an Infrastructure for Co-ordinated Security Incident Handling

This work item aims at establishing an infrastructure for security incident handling. If confined to the small subset of GÉANT partners participating in this work item, the operational impact of this infrastructure is marginal. It needs to be expanded in the future to cover all partners of GÉANT, which should be required to run reasonably capable security teams following agreed operational standards. In order to achieve this goal, close co-operation with work item 1 (Securing GN2 network elements and services) is required to work out appropriate policy terms and with work item 2 (Building of security services) to ensure the operational needs are made known to the service developers and get properly prioritised.

Project:	GN2
Deliverable Number:	DJ2.5.1
Date of Issue:	01/08/05
EC Contract No.:	511082
Document Code:	GN2-05-141v4

The noticeable uptake of the incident information exchange standard IODEF in Asia Pacific area may indicate that this standard may – after a long period of no noticeable interest – finally become important. This should be taken into consideration by this work item. It might warrant a good investigation on what this use entails and that might influence how WI3 is going to facilitate incident data exchange in the next phases. Real-time Internetwork Defense (RID) is an extension to IODEF and its potential usefulness within the scope of this work item should be assessed.

Also development of other available tools and procedures, like RTIR, should be assessed and investigated to enhance productivity and performance of security teams, which are active in GN2.

3.2.4 Work item 4: Relationship with TF-CSIRT

No specific recommendation was devised.

3.2.5 Work item 5: Establishment of an Advisory Panel

No specific recommendation was devised.

3.3 Overview of Trends Relevant to JRA2

This chapter gives an overview of the trends considered relevant by the members of the advisory panel in the areas of network security and incident handling processes.

3.3.1 Critical Information Infrastructure Protection (CIIP)

The network itself and network-based services are increasingly perceived as a critical infrastructure and create more interest on the managerial level. Security teams today are primarily talking a technical language, techie to techie. Communicating with the managerial level as part of their organisation's or customers' risk management processes will become more important in the future.

Depending on whether large scale, serious problems will show up in the future, this will create new service needs for CSIRT teams to provide appropriately shaped information to the managerial level. Should such service needs – most likely event driven – arise, they should be taken up seriously.

3.3.2 Legal

For many reasons, applicable law was not enforced with vigour to crimes committed in the “virtual world”. This is about to change and the Internet is becoming a commodity without a special status with regards to the rules

of the law. Since CSIRTs deal a lot with crimes being committed they are increasingly exposed to interactions with law enforcement agencies, with legal advisors and maybe even court cases. This creates needs for additional education, but also needs on the technical layer, like forensic analysis and court-acceptable evidence gathering.

Privacy issues and evolving European and national security practices creates also a need for the CSIRTs to review their own documentation and guidelines.

JRA2 is advised to address the educational needs and to check whether a similar toolset as now in development in WI2 might be of use for forensic analysis and court-acceptable evidence gathering.

3.3.3 Convergence of Voice and Data

Voice services (telephone) are still mainly accessed through dedicated devices and voice service is perceived as a suitable fallback medium in case of network failures or other emergencies. The regular telephone user is not usually aware that the networks used for voice and data are increasingly being shared and that the phone is often nothing else than a phone-shaped computer. Telephone users become unwillingly Internet users and are exposed to the same risks and threats as the regular Internet users. As such, they also become customers of CSIRTs. And since voice services are often the medium of choice for alerting emergency services, the expectations are pretty high.

“The Toolset” being developed in JRA2 is well suited to offer substantial help in detecting and fighting network abuse of many kinds. Protecting network based voice services might require modifications or extensions.

WI3 (Designing and establishing an infrastructure for co-ordinated security incident handling) is urged to account for the convergence risks of voice and data. This is particularly relevant to the risk analysis of the CSIRT co-operation tools and processes facilitating rapid incident response.

3.3.4 Overlay Networking

Overlay links, such as bandwidth-on-demand links, will often be used for overlay networks. While extensive care is taken – and the CSIRTs play an important role – to protect the general purpose IP service, the traffic on the overlay network is opaque to the CSIRTs and cannot be protected. Furthermore, no assumptions can be made as to the management of the overlay network. As long as the traffic on the overlay network is confined to the dedicated overlay links, there is no impact on the general purpose IP service in case of security breaches on the overlay network. Special care is needed when overlay networks become interconnected with the general purpose IP service. Ideally, this should be prevented.

JRA2 is advised to provide policy measures to regulate interconnections between overlay networks and the general purpose IP service.

Project:	GN2
Deliverable Number:	DJ2.5.1
Date of Issue:	01/08/05
EC Contract No.:	511082
Document Code:	GN2-05-141v4

4 Conclusions

The panel is convinced that the work carried out by JRA2 is relevant to the GÉANT community and also beyond, to the private sector and particularly to ISPs,

Given the current composition of the participants in JRA2, the main focus in the future must not be on research per se, but on the perceived value for participating security teams. Considering the strong bias towards operational issues, a return on invested manpower must be rather clear and not too distant in the future.

In order to keep in touch with research, participation from teams with research interests should be maintained and encouraged or other measures should be put in place.

The following main trends relevant to JRA2 were identified, their relevance discussed and recommendations devised for future phases of JRA2:

- The availability and integrity of network-based services is becoming increasingly crucial
- Increasing enforcement of relevant laws and security practices to the “virtual” world
- Convergence of voice and data
- Security implications of overlay networks, such as bandwidth-on-demand links

5 Acronyms

CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
GN2	Multi-Gigabit European Academic Network
JRA	Joint Research Activities 2: Security
NREN	National Research and Educational Network
TF-CSIRT	TERENA Taskforce Collaboration of Computer Security Incident Response Teams