

28.08.07

Deliverable DJ2.5.1,3: Report on Activities and Recommendations of JRA2 Advisory Panel



Deliverable DJ2.5.1,3

Contractual Date:	31/8/2007
Actual Date:	28/08/07
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	GN2-07-219

Authors: Gilles André (CERT-A), Gorazd Bozic (ARNES), Christoph Graf (SWITCH), Urpo Kaila (FUNET CERT/CSC), Jan Meijer (Uninett), Wilfried Wöber (ACOnet)

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 third deliverable of this panel, covering the third year of JRA2 activities.

Table of Contents

0	Executive Summary	iv
1	The JRA2 Advisory Panel	1
2	Activities and Recommendations of the Advisory Panel	2
2.1	The main objective of JRA2	2
2.2	Recommendations of the Panel	4
2.2.1	Promoting the establishment of CSIRTs	4
2.2.2	Defining the security service portfolio	4
2.2.3	Preparing for rare events	5
2.2.4	Becoming more proactive	5
2.3	Overview of trends relevant to JRA2	5
2.3.1	The shift from vandalism to financially motivated hacking	6
2.3.2	Overlay networking	6
2.3.3	Critical Information Infrastructure Protection (CIIP)	7
2.3.4	Legal issues	7
2.3.5	Convergence of Voice and Data	8
2.3.6	Virtualisation	8
3	Conclusions	9
4	Acronyms	10
5	References	11
Appendix A	List of members of the Panel	12

Project:	GN2
Deliverable Number:	DJ2.5.1,3
Date of Issue:	28/08/07
EC Contract No.:	511082
Document Code:	GN2-07-219

Table of Figures

Figure 1: The main classes of activities in JRA2	3
Table 1 List of active and retired members of the Panel	12

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.

Concrete recommendations on the activity plan of JRA2 are devised on the following topics:

- Promoting the establishment of CSIRTs
- Defining the security service portfolio
- Preparing for rare events
- Becoming more proactive

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

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

Project:	GN2
Deliverable Number:	DJ2.5.1,3
Date of Issue:	28/08/07
EC Contract No.:	511082
Document Code:	GN2-07-219

1 The JRA2 Advisory Panel

The purpose of maintaining 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 was 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. A list of (active and retired) members of the panel can be found in Appendix A.

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
- to give recommendations for work in subsequent years of JRA2

Project:	GN2
Deliverable Number:	DJ2.5.1,3
Date of Issue:	28/08/07
EC Contract No.:	511082
Document Code:	GN2-07-219

2 Activities and Recommendations of the Advisory Panel

The advisory panel formally met once in Year 3 of GÉANT2, adjacent to the TF-CSIRT meeting in Prague, Czech Republic, in May 2007, where it 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. This third revision of the report is mainly the result of mail discussions between April and August 2007 among the panel members.

In earlier revisions of this document, the panel commented on each work item. To better concentrate on the overall strategy of JRA2 and not to get locked into the structure of JRA2 too much, a different approach was taken this time. The panel starts discussing the objectives of JRA2 and recommendations are devised from that discussion. The overview of trends was discussed and addressed separately.

2.1 The main objective of JRA2

The main objective of JRA2 is to guarantee that the GÉANT2 community becomes and stays a secure community. This is a challenging task for a variety of reasons:

- **Complexity:** Like in the rule of the weakest link in a chain, the security level of a product strongly depends on the component with the weakest security. When applied to GÉANT2 with its complex interdependencies (e.g. for the provisioning of cross-border optical links, some partners are acting as consumers and providers at the same time) we have to maintain a reasonably high “minimum” security level throughout the GÉANT2 community.
- **Pioneering character:** Many of the services offered on GÉANT2 are pioneering work, where relevant operational experience is naturally limited or – in some cases, potentially – missing.
- **Moving target:** While threats on the network are constantly evolving, it may be of even greater importance in this context, that the services offered on GÉANT2 are evolving as well.

- Diversity: The security awareness and capabilities differ substantially within the GÉANT2 community. While many partners do operate CSIRTs as a regular service – some were even pioneering CSIRTs in Europe – some partners are still not yet operating CSIRTs.

JRA2 is therefore focusing on the following two classes of activities:

- Improve leading edge teams' services: The leading edge security teams with advanced security capabilities and know-how in the GÉANT2 community are key when it comes to identify the need for and the development of new and improved security services. In this context, the main focus of JRA2 for the remainder of GÉANT2 is to improve anomaly detection capabilities.
- Reach compliance level: establishing and maintaining a (reasonably high) minimum security level throughout the GÉANT2 community is an important prerequisite to offer reliable services. As threats and services change, this requires continuous efforts. The main focus of JRA2 for the remainder of GÉANT2 is to ensure the establishment of CSIRTs in all partner NRENs.

Figure 1 below explains how these two classes of activity are expected to influence the security capabilities of the partners of GÉANT2 over time. JRA2 is collaborating primarily with the experienced CSIRTs in order to develop new and to improve existing security services. On the other hand, the partners with only basic security capabilities – and in particular those without a (formally established) CSIRT – are supported by JRA2 to reach the minimum GÉANT2 security compliance level. As a result, the overall security capability of GÉANT2 will improve, the diversity across the partners will be reduced and GÉANT2 can continue to offer the advanced security teams a platform for driving leading edge CSIRT service development.

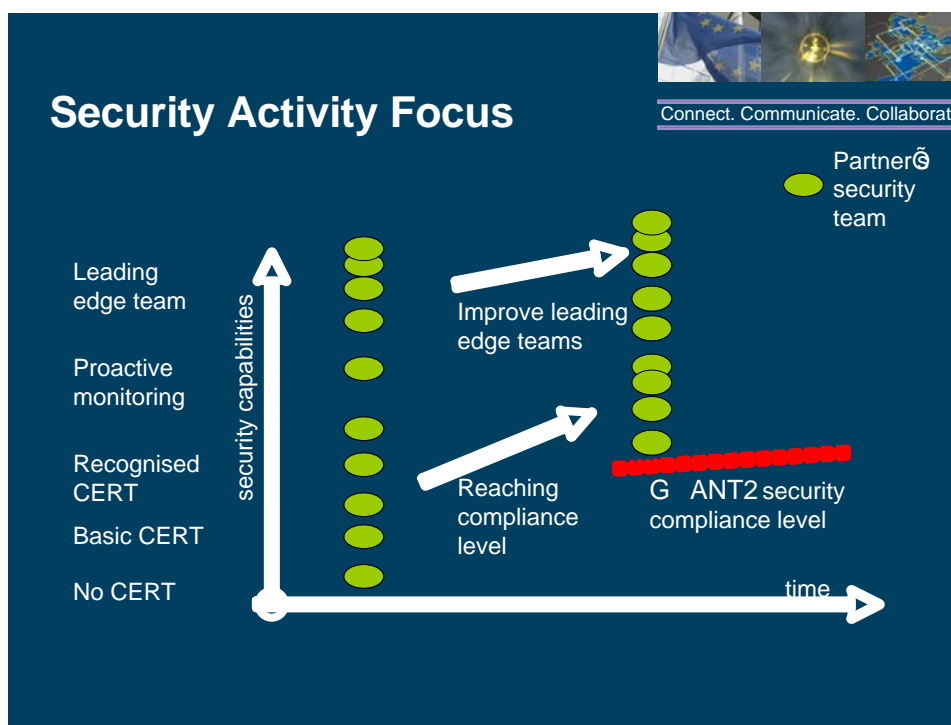


Figure 1: The main classes of activities in JRA2

Project:	GN2
Deliverable Number:	DJ2.5.1,3
Date of Issue:	28/08/07
EC Contract No.:	511082
Document Code:	GN2-07-219

2.2 Recommendations of the Panel

2.2.1 Promoting the establishment of CSIRTs

A decade ago, the operation of a CSIRT was still largely pioneering work and most CSIRTs served the academic sector. This has changed completely: It is now widely accepted that CSIRTs are useful, if not vital, and many entities exist promoting the establishment of CSIRT in different industry sectors. A very prominent example is the EU agency ENISA, which is actively promoting the establishments of CSIRTs with a specific focus on CSIRTs on national level.

This led to the following recommendations:

- The Panel strongly recommends working towards full CSIRT coverage within the NREN-community in Europe. The Panel acknowledges, that the NREN-sector is setting an example to be followed by other industry sectors.
- The promotion of the idea and providing support for the establishment of CSIRTs serving organisations and initiatives outside of our community used to be very important, but it is now of much less importance. The concepts to apply are well-known and there do exist entities doing that work already.
- We should seek collaboration with similarly scoped initiatives and organisations, but only where we expect benefits to our community.
- There do exist many different types of CSIRTs. Just to name a few: vendor CSIRTs, government CSIRTs, ISP CSIRTs, etc. JRA2 is recommended to streamline its efforts and to specifically target the requirements of NREN communities and the users of GEANT2-provided services.

2.2.2 Defining the security service portfolio

To promote the establishment of CSIRT functions within all GEANT2 partners – as planned by JRA2 – is an important first step. Other than the requirement to establish a CSIRT, the security service specification of GEANT2 is not very explicit. This is acceptable for the time being, but future updates to the security service specification should become more specific in terms of the service portfolio, which NREN-CSIRTs should be offering.

Specific recommendations:

- Extend future revisions of the security service specification of GEANT2 with clearer expectations regarding the service offerings of partner CSIRTs
- The service categories of the Trusted Introducer may serve as an initial list.

- Liaising with the Ad-hoc Working-group on CSIRT Services (WG-CS) of ENISA should be considered.
- It is important to include all partner CSIRTs, not already represented in JRA2, into these discussions.

2.2.3 Preparing for rare events

During the last couple of years, the Internet did not suffer large-scale, distributed problems, as experienced in the years before (like those caused by malware like SQL-slammer, Code Red and alike). But despite the lack of recent cases, our CSIRT infrastructure needs to maintain or improve the ability to react to such incidents. “On the job training” only works to establish or to maintain skills required to deal with relatively frequent events. Preparing for rare events requires periodic drills.

Specific recommendation:

- Assess the preparedness of the CSIRTs and specifically their ability to interact with each other in a timely and effective manner by scheduling regular training events.

2.2.4 Becoming more proactive

The terms CERT (Computer Emergency Response Team) and its synonym CSIRT (Computer Security Incident Response Team) clearly stem from a time when such teams were established primarily in order to react to critical situations. But the experience accumulated by those teams should not only be used to improve the reactive capabilities, but also to improve incident prevention capabilities in a balanced way. This can happen in many different ways, e.g. through publication of BCP (Best Common Practice) guides, contributing to policy work or early involvement in the architecture and design phase of new services.

Specific recommendation:

- Ensure on project level, that the security implications of new services are assessed during the service architecture development or early design phase and that the know-how available in the security teams is used for that purpose.

2.3 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.

Project:	GN2
Deliverable Number:	DJ2.5.1,3
Date of Issue:	28/08/07
EC Contract No.:	511082
Document Code:	GN2-07-219

2.3.1 The shift from vandalism to financially motivated hacking

The last couple of years were no longer plagued by disruptive global worm outbreaks, which impacted the availability of the Internet at large. Unfortunately, this is not a consequence of less malicious activity, but only of a shift in its nature. Instead of very noisy worm outbreaks infecting millions of machines at once, and potentially bringing the Internet to a grinding halt, we are faced with a – not necessarily smaller – number of infected systems remaining undetected and at the disposal of criminals for a variety of activities. The reason is quite simple: Using the Internet as a target for vandalism is financially not as attractive as compared to making use of the Internet for other criminal activities.

This has far-reaching effects on many aspects of CSIRT activities:

- Instead of reacting very quickly to very evident problems, we now need to invest much more effort to detect the well-hidden malicious activity. Anomaly detection is a key technology to help.
- Most malicious activity will not harm the transmission infrastructure, but put end system integrity at risk. We need good procedures to deal with identified integrity risks (infections). Well-established relationships with site security contacts are vital.
- With lots of concurrent malicious activity going on in parallel, we need a good information-sharing infrastructure in place to exchange the malicious activities' pattern or fingerprint information.
- Well-maintained and regularly patched systems are less likely of getting compromised. CSIRTs are encouraged to share their knowledge of malicious activity with their constituency. This will help to raise awareness and help their constituents to better protect against malicious activity in a proactive way.

JRA2 is advised to improve its anomaly detection capabilities and to share the detected pattern information efficiently. NRENs should then, by means of the Toolset, be able to identify the systems affected within their own network and get in contact with their site security contacts to get them fixed.

There is a substantial risk that detection efforts on layer 2 and 3 (e.g. as provided by netflow) will lose some of their effectiveness in the years to come and more effort needs to be spent on application design. The network footprint of malicious activity and the possibility to take proactive measures on layers 2 and 3 depend substantially on application design. Sharing knowledge of malicious activity may again help to raise awareness.

2.3.2 Overlay networking

Overlay links, such as bandwidth-on-demand links, will often be used for overlay networks carrying IP traffic. 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 thus 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 (sets of) dedicated overlay links, there is no immediate impact on the general purpose IP service in case of security breaches on the overlay network. Special care is needed when overlay

Project:	GN2
Deliverable Number:	DJ2.5.1,3
Date of Issue:	28/08/07
EC Contract No.:	511082
Document Code:	GN2-07-219

networks become interconnected with the general purpose IP service in real time. Ideally, a similar level of protection should be guaranteed for IP traffic carried over such overlay links than for general purpose IP traffic.

Nevertheless, even if there is no real-time interconnect for IP traffic with the general purpose IP network(s), systems that are alternatively connected to a dedicated IP-based network and an organisation's internal network do pose an additional risk. This risk is essentially equivalent to moving systems, which have been exposed to malicious activity on the Internet and may already be compromised, behind a protective border (e.g. firewall) onto the organisation's intranet or LAN.

JRA2 is advised to develop recommendations for policy measures to manage interconnections between overlay networks and the general purpose IP service and the level of protection for the traffic they carry.

2.3.3 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.

If large scale, serious problems will show up in the future, this will impact the perception of computer security. Such events will create new service and communication 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.

2.3.4 Legal issues

For many reasons, applicable law was not enforced widely or with vigour against crimes committed in the "virtual world". This is about to change and the Internet is becoming a commodity losing its special status with regard to the rules of the law. Since CSIRTs deal a lot with crimes being committed on-line they are increasingly exposed to interaction with law enforcement agencies, with legal advisors and maybe even become involved in court cases. This creates a need for additional education, but also requirements on the technical and procedural level, like being able to perform forensic analysis or to gather and properly document facts that can be used in court as evidence.

Privacy issues and the evolving European and national security practices also create a need for CSIRTs to regularly review their own documentation, operational guidelines and mandate.

JRA2 is advised to address the educational needs and to check whether organisations in partners' constituencies would benefit from a similar toolset as it is now being developed in JRA2 for forensic analysis and for court-acceptable evidence gathering.

Project:	GN2
Deliverable Number:	DJ2.5.1,3
Date of Issue:	28/08/07
EC Contract No.:	511082
Document Code:	GN2-07-219

2.3.5 Convergence of Voice and Data

Voice services (telephone) are still mainly accessed through dedicated devices and the (circuit switched) 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 carrying voice and data streams are increasingly being shared and that the phone is often nothing else than a phone-shaped computer, connected to the packet-switched IP-based network. 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. As (traditional) voice services are often the medium of choice for alerting emergency services, the expectations regarding reliability 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 IP-network based voice services may require modifications or extensions.

JRA2 is urged to account for the risks introduced by convergence of voice and data streams onto the same transmission paths. This is particularly relevant to the risk analysis regarding the CSIRTs’ co-operation tools and the processes facilitating rapid incident response.

2.3.6 Virtualisation

Virtualisation techniques of many kinds are used to hide the internals of systems from the users. Most of the underlying complexity is then hidden behind an Interface. It helps the service designer and user alike, as they need not deal with what is on the other side of this interface. But there are new risks associated with this approach: it makes it increasingly hard to understand service interdependencies and many new dependencies on the network are created. As a result, the criticality of the network increases.

Many of the services offered by CSIRTs are of particular relevance in the presence of perturbations on the network. JRA2 is therefore advised to take into account that some of the increasingly popular virtualisation techniques may not be appropriate for its own purposes, under certain conditions.

Project:	GN2
Deliverable Number:	DJ2.5.1,3
Date of Issue:	28/08/07
EC Contract No.:	511082
Document Code:	GN2-07-219

3 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.

Concrete recommendations on the activity plan of JRA2 were devised on the following topics:

- Promoting the establishment of CSIRTs
- Defining the security service portfolio
- Preparing for rare events
- Becoming more proactive

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

- The shift from vandalism to financially motivated abuse
- Security implications of overlay networks, such as bandwidth-on-demand links
- 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
- Virtualisation

4 Acronyms

CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CSIRT	Computer Security Incident Response Team
ENISA	European Network and Information Security Agency
GN2	Multi-Gigabit European Academic Network
IPFIX	Internet Protocol Flow Information Export
JRA	Joint Research Activity
NREN	National Research and Education Network
TF-CSIRT	TERENA Task Force on Collaboration of Computer Security Incident Response Teams

5 References

[TF-CSIRT] <http://www.terena.org/activities/tf-csirt/>

Project:	GN2
Deliverable Number:	DJ2.5.1,3
Date of Issue:	28/08/07
EC Contract No.:	511082
Document Code:	GN2-07-219

Appendix A List of members of the 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 CSIRT (Computer Security Incident Response Team) representative was still being sought at that time. Eventually the vacancy could be filled in May 2005 by inviting Gilles André. Two members had to resign from the Panel in Year 3 of GÉANT2 due to their workload situation: Jimmy Arvidsson, Telia-Sonera and Marco Thorbrügge, ENISA. The Panel's chairman, Jan Meijer, is now working for Uninett (formerly as security expert at SURFNET, NL).

Name	Affiliation	Country	Field or function	Status
Jan Meijer	Uninett	Norway	Advisory panel chairman, security researcher	Active
Gorazd Bozic	ARNES	Slovenia	TF-CSIRT Chair, member ex officio	Active
Christoph Graf	SWITCH	Switzerland	JRA2 Activity Leader, secretary ex officio	Active
Jimmy Arvidsson	Telia-Sonera	Sweden	Industry participant	Retired
Marco Thorbrügge	ENISA	Greece	Government/Commission Agency	Retired
Urpo Kaila	Funet CERT/ CSC	Finland	R&E incident response expert	Active
Wilfried Wöber	ACOnet	Austria	R&E incident response expert	Active
Gilles André	CERT-A	France	Government CSIRT	Active

Table 1 List of active and retired members of the Panel

Project:	GN2
Deliverable Number:	DJ2.5.1,3
Date of Issue:	28/08/07
EC Contract No.:	511082
Document Code:	GN2-07-219