

19.09.06

Deliverable DJ2.5.1,2: Report on Activities and Recommendations of JRA2 Advisory Panel



Deliverable DJ2.5.1,2

Contractual Date:	31/8/2006
Actual Date:	19/09/06
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	GN2-06-248v4

Authors: Gilles André (CERT-A), Jimmy Arvidsson (Telia-Sonera), Gorazd Bozic (ARNES), Christoph Graf (SWITCH), Urpo Kaila (FUNET CERT/CSC), Jan Meijer (Surfnet), Marco Thorbrügge (ENISA), 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 second deliverable of this panel, covering the second year of JRA2 activities.

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	3
3.1.1	Recommendations based on observations	3
3.2	Comments on the work carried out by JRA2	4
3.2.1	Work Item 1: Securing GN2 network elements and services	4
3.2.2	Work Item 2: Building of security services	4
3.2.3	Work item 3: Designing and establishing an infrastructure for co-ordinated security incident handling	5
3.2.4	Work item 4: Relationship with TF-CSIRT	5
3.2.5	Work item 5: Establishment of an advisory panel	5
3.3	Overview of trends relevant to JRA2	5
3.3.1	The shift from vandalism to financially motivated hacking	6
3.3.2	Overlay networking	6
3.3.3	Critical Information Infrastructure Protection (CIIP)	7
3.3.4	Legal issues	7
3.3.5	Convergence of voice and data	7
4	Conclusions	9
5	Acronyms	10

Table of Figures

Table 2.1: Composition of the advisory panel

2

Project:	GN2
Deliverable Number:	DJ2.5.1,2
Date of Issue:	19/09/06
EC Contract No.:	511082
Document Code:	GN2-06-248v4

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 panel was initially presented to JRA2 in January 2005. It formally met in May 2005 and several times informally thereafter. It remained in its initial composition during the first two years of GN2.

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 to the “virtual” world
- Convergence of voice and data

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
- 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	ENISA	Greece	Government/Commission Agency
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, in conjunction with the TF-CSIRT meeting in Zurich, Switzerland, in May 2005 and approved the chairmanship of Jan Meijer (on long-term leave from May-October 2006). The remainder of this document is based on the discussion and findings during that meeting and discussions by mail and phone afterwards. This second revision of the report is mainly the result of mail discussions between April and August 2006 between the panel members.

3.1 General observations

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

It does not come as a surprise, that the majority of partners taking part in JRA2 are more security aware and advanced than the GN2 average. A minority of GN2 partners does currently not yet operate a recognised CERT. The rule of the weakest link in a chain applies to many security matters and is particularly relevant when it comes to maintaining the security of a project like GÉANT2.

3.1.1 Recommendations based on observations

Driving the advancements in security operations is a noble goal requiring proper attention. But because of the rule of the weakest link in a chain, raising the security level of partners with lower security level will be even more beneficial to the overall security of GÉANT2. We therefore recommend to work towards an improved minimum security baseline for all partners and advancing security operations alike.

Project:	GN2
Deliverable Number:	DJ2.5.1,2
Date of Issue:	19/09/06
EC Contract No.:	511082
Document Code:	GN2-06-248v4

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 primarily 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

No specific recommendation was devised.

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 to 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 dependent 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 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. JRA2 decided in Year2 of GN2 to continue to rely entirely on the availability of netflow data and deliberately not use payload inspecting traffic scanners. The development of the FlowMon probe is meant to reduce the reliance on netflow provisioning of networking equipment.

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.

The development of the FlowMon netflow probe is an interesting effort, albeit bearing substantial development risks. It allows those sites without netflow data generating networking equipment to get hold of netflow data by feeding the probe with raw network traffic. A sustained effort will be needed in the future to keep up with new developments in the networking area (speed, interfaces) in order to maintain its usefulness. It is therefore advisable to enlarge the user community beyond GÉANT2.

Sources of traffic metadata other than netflow or new variants of it (e.g. IPFIX) might become available and 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 properly mandated and set up, funded, manned and recognised security teams following agreed operational standards.

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 The shift from vandalism to financially motivated hacking

The last couple of years were no longer plagued by 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 bringing the Internet to a grinding halt, we are faced with a not necessarily smaller number of infected systems staying undetected 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 to make use of the Internet for other criminal activities.

This has far-reaching effects on many aspects of CERT 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 key.
- 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 key.
- With lots of concurrent malicious activity going on in parallel, we need a good information-sharing infrastructure in place to exchange the malicious pattern information.
- Well-maintained systems are less likely of getting compromised. CERTs are encouraged to share their knowledge of malicious activity with their constituents. This will 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 extract the systems affected within their own network and get in contact with their site security contacts to get them fixed.

There is substantial risk, that efforts on layer 2 and 3 (as provided by netflow) will loose some of their effectiveness in the years to come and more efforts 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.

3.3.2 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 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, a similar level of protection should be guaranteed for IP traffic carried over such overlay links than for general purpose IP traffic.

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

3.3.3 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 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.

3.3.4 Legal issues

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 also create a need for the CSIRTs to review their own documentation, 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 now in development in WI2 for forensic analysis and court-acceptable evidence gathering.

3.3.5 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.

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,

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 to the “virtual” world
- Convergence of voice and data

5 Acronyms

CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
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