

10.08.06

Deliverable DJ2.4.1,2: Report on Ad-hoc Advisory Groups Creation and Activities



Deliverable DJ2.4.1,2

Contractual Date: 31/08/06
Actual Date: 10/08/06
Contract Number: 511082
Instrument type: Integrated Infrastructure Initiative (I3)
Activity: JRA2
Work Item: 4
Nature of Deliverable: R (Report)
Dissemination Level: PP (Project Participants)
Lead Partner: SWITCH
Document Code: GN2-06-186v3

Authors: Christoph Graf (SWITCH)

Abstract

Work Item 4 (Relationship with TF-CSIRT) of JRA2 (Security) details the relationship with the TERENA Taskforce TF-CSIRT (Collaboration of Security Incident Response Teams). One item of this collaboration is the creation of ad-hoc teams to deliver security advice to any entity within GN2. This deliverable reports on cases of advice requested and how the cases were handled.

Table of Contents

0	Executive Summary	iii
1	Introduction	1
2	Activities	2
3	Conclusions	4
4	References	5
5	Acronyms	6
Appendix A	Case 1: "Storage of perfSONAR Login Details"	7

0 Executive Summary

Work Item 4 (Relationship with TF-CSIRT) of JRA2 (Security) defines the relationship between GN2 and the TERENA security taskforce TF-CSIRT (Collaboration of Security Incident Response Teams). It includes the creation of ad-hoc groups made up of TF-CSIRT members for delivery of advice on specific topics on behalf of any GN2 entities.

As a direct consequence of advertising this service at the first GN2 Technical Workshop, the Activity Leader of JRA1 initiated the first request for advice: "Storage of perfSONAR login details". The JRA1 Activity Leader requested feedback from security experts on the way perfSONAR login details are stored. The ad-hoc group provided an assessment methodology, applied it to the case and came up with concrete proposals to increase the security level. The advice will enable JRA1 to carry out future security analysis work of similar nature on their own. The case was closed to the satisfaction of the JRA1 Activity Leader.

Project:	GN2
Deliverable Number:	DJ2.4.1,2
Date of Issue:	10/08/06
EC Contract No.:	511082
Document Code:	GN2-06-186v3

1 Introduction

The TERENA TF-CSIRT is a well-established group of security experts and Work Item 4 of JRA2 (Security) defines the relationship between GN2 and this group. The main topic of this deliverable is the following collaboration item in the Description of Work:

- Creation of ad-hoc groups made of TF-CSIRT members for delivery of advice on specific topics, upon request by JRA2 leader, and delivery of advice reports

Any entity within GN2 is encouraged to contact the JRA2 Activity Leader, whenever specific advice is required on security related topics. The JRA2 Activity Leader will then call for volunteers within TF-CSIRT to form an ad-hoc group of experts to address the issue at hand. It should be taken into consideration that the volunteer work itself is not funded and that the security experts within TF-CSIRT are usually quite busy. It is therefore recommended to contact the JRA2 Activity Leader with concrete questions, which can be answered efficiently with limited manpower investment. Typical use cases will include reviewing security considerations or commenting on the soundness of architecture proposals.

2 Activities

The offer to create ad-hoc groups to address security issues has been made at several occasions, namely at several meetings with GN2 Activity Leaders and at the GN2 Technical Workshops. Even though interest was expressed, no formal request to create an ad-hoc group was received in Year 1 of GN2. In Year 2, one such request was received and dealt with. Chapter 2.1 has the details.

There was no case in Year 1. At the time, it was the belief of JRA2 participants that the interest in the service is low because GN2 is still in its early stages and that the interest will raise during future phases of GN2. Therefore, the offer to create ad-hoc groups to give advice on specific security topics was maintained in the same form in Year 2 and the service was advertised at the GN2 Technical Workshops.

As a direct consequence of this advertisement effort at the first GN2 Technical Workshop, the Work Item Leader of JRA1 initiated the first request for advice. The case was concluded to the satisfaction of the requesting party and we recommend keeping this service in its present form for the remainder of GN2.

2.1 Case 1: “Storage of perfSONAR login details”

At the GÉANT2 Technical Workshop in January 2006, the JRA1 Activity Leader contacted the JRA2/WI4 leader to discuss the option of reviewing security aspects of PerfSonar with a group of security experts from TF-CSIRT. Specifically, he asked that the way usernames and passwords for PerfSonar are stored within the monitoring infrastructure be assessed from the security point of view.

The following table shows the most important milestones in resolving this issue:

Date	Action
19 April 2006	After some private discussion between the work item leaders of JRA2/WI4 and the Activity Leader of JRA1, both agreed on a specific question to be answered by an ad-hoc group of TF-CSIRT experts.
19 April 2006	The call for volunteers into a ad-hoc group of experts was issued.

Project:	GN2
Deliverable Number:	DJ2.4.1,2
Date of Issue:	10/08/06
EC Contract No.:	511082
Document Code:	GN2-06-186v3

Date	Action
8 May 2006	Four TF-CSIRT members responded to the call for volunteers and two finally decided to work for the ad-hoc group. Three additional people were named by the requesting party to participate as well. The group was formed and called to work by the work item leader of JRA2/WI4.
13 July 2006	The summary report was finished and subsequently communicated to the requesting party and TF-CSIRT

The full report produced in answering the original question is attached as Appendix A and available from the GEANT2 web site [WI4-CASE1]. In the feedback received from the JRA1 Activity Leader he expressed his satisfaction with the results. The report is not directly producing an assessment of the risk associated with perfSONAR. Instead, it contains a methodology JRA1 may apply to assess the risks and decide on the acceptability. The JRA1 Activity Leader expressed his intention to apply this methodology.

Project:	GN2
Deliverable Number:	DJ2.4.1,2
Date of Issue:	10/08/06
EC Contract No.:	511082
Document Code:	GN2-06-186v3

3 Conclusions

Work item 4 (Relationship with TF-CSIRT) continues to offer the establishment of ad-hoc groups for delivery of advice on specific security topics to any GN2 entity. The positive feedback received from the first case, the evaluation of specific security aspects of the JRA1/perfSONAR framework, should be taken as a positive signal that the service can be valuable and useful.

The description of work for the next phase is therefore proposed to stay unchanged and the service will be maintained in its current form. The offer to all entities of GN2 to get security advice through ad-hoc groups of TF-CSIRT shall be renewed at appropriate occasions, including the GN2 Technical Workshops and more effort will be made to advertise the service to the community, including the GN2 management.

4 References

[TF-CSIRT] <http://www.terena.nl/activities/tf-csirt/>
[WI4-CASE1] <http://intranet.geant2.net/server/show/conMediaFile.5449>

Project:	GN2
Deliverable Number:	DJ2.4.1,2
Date of Issue:	10/08/06
EC Contract No.:	511082
Document Code:	GN2-06-186v3

5 Acronyms

TF-CSIRT TERENA Task Force “Collaboration of Security Incident Response Teams”

Appendix A **Case 1: “Storage of perfSONAR Login Details”**

A.1 **Introduction**

JRA2 is responsible for the security aspects of the GÉANT2 project. Work Item 4 of JRA2 describes the collaboration between JRA2 and TF-CSIRT. Work Item K of the Terms of Reference of TF-CSIRT is the counterpart of Work Item 4 of JRA2.

Work Item 4 of JRA2 describes a formalised way of delivering security expert advice from TF-CSIRT to GN2. This covers the creation of ad-hoc groups made of TF-CSIRT members for delivery of advice on specific topics, upon request by the JRA2 leader, and delivery of advice reports.

This report contains the security advice of TF-CSIRT experts initiated by a request for advice initiated by the Activity Leader of JRA1 of GN2.

A.2 **Process and timelines**

A.2.1 **Call for expert advice received**

After some private discussion between the Activity Leaders of JRA1 and JRA2, both agreed on a specific question to be answered by an ad-hoc group of TF-CSIRT experts on 19 April 2006.

A.2.2 **Call for volunteers issued**

The call for volunteers into a ad-hoc group of experts was issued the same day (19 April 2006).

Project:	GN2
Deliverable Number:	DJ2.4.1,2
Date of Issue:	10/08/06
EC Contract No.:	511082
Document Code:	GN2-06-186v3

A.2.3 Ad-hoc group created

4 TF-CSIRT members responded to the call for volunteers and 2 decided to work for the ad-hoc group. 3 people were named by the requesting party to participate as well. The group was formed and initially addressed by the Activity Leader of JRA2 on 8 May 2006.

A.2.4 Work method established

It was decided to carry out the work over email contacts.

A.2.5 Results made available

This summary report was finished 13 July and subsequently communicated to the requesting party and TF-CSIRT.

A.3 Request for advice

The following request for advice was sent on 19 April 2006 to TF-CSIRT to call for volunteers:

"We are working on some tools which need to have stored somewhere the routers login and password. Those tools will then access the router using either ssh or telnet to retrieve some information. The tools will be installed on PCs which are IP accessible from the outside world as a web-server (providing web-services) installed locally on those servers.

"Note that the web-service will legitimately expose information retrieved by the tool.

"We were wondering what could be the potential problems we would encounter with such approach and what would be the advices from security people on that topic. Are there potential solution which are existing and which wouldn't prevent the tool and service of working."

A.4 The group of experts

The group of experts addressing this issue consisted of the following individuals:

Project:	GN2
Deliverable Number:	DJ2.4.1,2
Date of Issue:	10/08/06
EC Contract No.:	511082
Document Code:	GN2-06-186v3

Role	Name	Affiliation
Group chair	Christoph Graf	SWITCH
TF-CSIRT experts	Klaus-Peter Kossakowski	Pre-Secure
	Catalin Meirosu	Terena
Requestor party	Nicolas Simar	DANTE
	Loukik Kudarimoti	DANTE
	Stijn Verstichel	University Gent

A.5 Recommendations of the ad-hoc group

A.5.1 Methodology

The group recommends adopting the following methodology:

- Identify assets in need of protection
- Identify relevant threats to those assets
- Assess the risk for each threat to an asset
- Address those risks, which are not acceptable

The ad-hoc group carried out the first two steps, initial input for the third and leaves it to the requestor party to work on the additional ones.

A.5.2 Assets in need of protection

The group identified the following assets, which need to be appropriately protected:

Asset	Description
Router	<ul style="list-style-type: none"> The routers being queried from the workstations authenticated with the credentials Services provided by those routers
Communication	The communication relevant to the web-service between those entities: <ul style="list-style-type: none"> the users (covering also potential abusers) the workstations the routers
Workstation	The workstations involved in querying the routers, including the hardware, software, configuration and services it offers
Credentials	The credentials used to access the routers

A.5.3 Threats relevant to those assets

The group considers the following threats particularly relevant in the context of this service:

Threat Categories	Threats
Confidentiality	<ul style="list-style-type: none"> Sniffing Copying Retrieve more information than authorised Observe user behaviour
Integrity	<ul style="list-style-type: none"> Integrity of the configuration Integrity of the operating system
Authenticity	<ul style="list-style-type: none"> Unauthorised access Unauthorised use
Availability	<ul style="list-style-type: none"> Service availability

In the next matrix, we map those threats to relevant assets and give a brief indication of risk relevance:

Project:	GN2
Deliverable Number:	DJ2.4.1,2
Date of Issue:	10/08/06
EC Contract No.:	511082
Document Code:	GN2-06-186v3

Threat Categories	Threats	Assets			
		Router	Communication	Workstation	Credentials
Confidentiality	Sniffing		X		
	Copying				X
	Retrieve more information	X		X	
	Observe user behaviour			X	
Integrity	Configuration integrity	X		X	
	OS integrity	X		X	
	Application integrity			X	
Authenticity	Unauthorised access	X		X	
	Unauthorised use				X
Availability	Service availability	X	O	O	O

X: risk particularly relevant

O: risk relevance depending on service requirements

The requesting party is recommended to analyse all above identified threats. It then should decide whether the risk associated with it in the current implementation is acceptable or not. In the latter case, additional steps are required to bring the risk to an acceptable level.

A.5.4 Observations and specific recommendations

A rather critical component in terms of risks is the workstation. Protection against almost all of the threats identified above depends on the integrity of the workstation. This implies, that an abuser able to exploit a weakness in the web-service or OS of the workstation poses a direct threat to all assets.

To address this issue, the group makes the following recommendations:

- **Web-service security:**

Attacks against web-services are very common and unfortunately often very sophisticated and not at all easy to detect. It is therefore key to carefully design and implement those services and to keep up to date on the threat level.

Project:	GN2
Deliverable Number:	DJ2.4.1,2
Date of Issue:	10/08/06
EC Contract No.:	511082
Document Code:	GN2-06-186v3

An interesting suggested reading is the "Threat Classification" by the Web Application Security Consortium at http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.pdf
The summary table of threats on pages 7 to 9 gives a rough overview.

- **Architectural change:**

The strong dependency on the workstation can be reduced by means of splitting the services on it to two separate workstations A and B in the following way:

- workstation A is retrieving the user information with the credentials from the router
- workstation A is then pushing the user information towards workstation B
- workstation B is serving the user

By this architecture we have added another workstation but have been able to separate the possession of the credentials from the web service. So we do not care too much any longer about the security posture of workstation B as the credentials are safe on workstation A.

A.6 Acknowledgements

Special acknowledgements go to the volunteer experts of TF-CSIRT: Cătălin Meiroșu from TERENA and Klaus-Peter Kossakowski from Pre-secure. Their contributions were key in writing this document.