

## FIRST Network Monitoring Special Interest Group (NM-SIG) 30 August 2006

Minutes of the kick off meeting on June 25, 09:00-12:00, Baltimore (USA)

### ATTENDEES

AusCERT:	Karl Hanmore
CAIS/RNP:	Liliana Solha, Guilherme Venere
CERT/CC:	Jeffrey J. Carpenter
CERT-FI:	Erka Koivonen
CERT	Polska: Pjotr Kijewski, Miroslaw Maj
DFN-CERT:	Jan Kohlrausch, Jochen Schoenfelder
DIRT:	Bill Eaheart
GOVCERT.NL:	Menno Muller, Hans Petri, Carol Overes
HKCERT:	K.T. Yung
IIJ-SECT:	Yoshinobi Matsazaki
INTECO:	Eurique Curiel
IRIS-CERT:	Francisco Monserrat
JPCERT/CC:	Hironobu Suzuki
KrCERT/CC:	Arnold Yoon
NorCERT:	Christopha Birkeland, Pal Arne Hoff, Einar Oftedal
PRE-CERT:	Till Döriges
SWRX CERT:	Uday Banerjee
SBB-SIRT:	Masaru Akai, Kazuyoshi Sasaki
SITIC:	Jonas Thambert, Peter Wallstrom
SURFnet:	Rogier Spoor
UK COMMCERT:	John Hyllman, Steve Owen

### OTHER

- EWA-Canada/CanCERT: Ken Armstrong was unable to join due to a cancelled flight
- DFN-CERT: Klaus-Peter Kossakowski was unsure about his presence and sent two of his colleagues to join the meeting;
- NU-CERT: Roger Safian was unable to join to due late arrival.
- CNCERT/CC: Yonglin Zhou colleagues were unable to join due to VISA problems
- SWITCH-CERT: Peter Haag missed the invitation and discussions (Arnold Yoon will check the NM-SIG e-mail list);

### 1. OPENING AND INTRODUCTION

Menno Muller welcomes everybody. He is happy that so many FIRST members share the interest in forming a Special Interest Group on the topic of Network Monitoring. Goal of this meeting is to start the NM-SIG and to make operational plans for the forthcoming time. Menno sets the definite agenda.

### 2. QUICK ROUND OF MONITORING INITIATIVES AND PROJECTS

All teams make a short statement about their current experience with network monitoring (and future plans) and their expectations of this NM-SIG.

#### SITIC

As Swedish national CERT they run a distributed IDS using Prelude. They also study the system of SURFnet. They recently organized a conference on network monitoring, at which they tested the interest in this subject at the constituency. Now they want to expand their network monitoring work (planned to start this autumn).

## Minutes of the NM SIG kick off meeting - June 25 2006, Baltimore, USA

### CERT-FI

They are in the stage of building up a monitoring system and work on malware detection. They have a good cooperation with telco's in network monitoring. Now working on a distributed IDS.

### Kr-CERT/CC

Since 2003 they do run a network monitoring center for their ISP's. They want to see how we can share information on this topic in the NM-SIG. Hope that a number of small working groups will be formed to work on particular NM topics.

### CAIS/RNP

As Brazilian CERT for all Brazil Universities they do operate a Network Monitoring storm center using honeypots, honeynets, malware collectors and netflow collectors. The system brought down the number of infected systems by 60%. They use home made open source tools. They want to share their approach with the NM-SIG.

### NorCERT

In 2000 they started the VDI warning system to protect the Norwegian critical infrastructure. The project is run as a Public/Private partnership with the institutions working in the Norwegian critical infrastructure. The system is based on IDS and they are working on incorporating Netflow in the system. Have interest in using the SURFnet IDS software,

### AusCERT

They operate an in house developed system that is fully operational. Have learned much regarding the do's and (particularly) the don't, regarding setting up such a system. They are happy to share these experiences with the NM-SIG.

### CERT Polska

Running a Critical Infrastructure program. Are especially interested in Netflow based monitoring.

### HKCERT

Do not have an operational system yet. However, it is a part of their task to have such system. The rigid legal system in Hongkong makes network monitoring nearly impossible. By participating in the NM-SIG they expect to get an idea how to go about setting up such a monitoring system (best practices and software)

### IRIS-CERT

Expect the NM-SIG to be a platform for information sharing.

### DIRT

Operational system based on Netflow and IDS. Is especially interested in the best practices of the other NM-SIG members.

### INTECO

Perceive the NM-SIG as a good platform to share information.

### SBB-SIRT

Also interested in sharing information.

### IJJ-SECT

Operating in monitoring botnet activity.

**UK COMMCERT**

They perceive learning from each other as a valuable thing of the NM-SIG. Run a distributed IDS and want to share information.

**PRE-CERT**

They just migrated from an EC funded project, called eCSIRT.net, to a voluntary service. Want to hear what other government CERTs do on early warning systems.

**DFN-CERT**

Interested in developments on the issue of network monitoring.

**CERT/CC**

Already share a number of tools they developed. Interested in data analysis. On October 10-12 they organise a conference on analysing Network flow data.

**GOVCERT.NL**

They are in the stage of rolling out an operational network monitoring service (based upon the SURFnet IDS). The goal is to realize an early warning system to inform their constituencies (both the Dutch central and local government). It expects the NM-SIG to start working groups on clearly defined issues and to share trends, techniques and software.

**3. DECISION ON GOALS AND AMBITION NM-SIG**

The "Birth certificate Network Monitoring SIG v02 7 feb 06" has been sent to the list and is now taken as starting point for the discussion about goals and ambition of the NM-SIG. Menno Muller asks for some quick comments on this document.

Chrisophe Birkeland: The document doesn't say anything about setting up a framework for exchanging anonymised information.

Carol Overes: FIRST shall be the umbrella-organisation for incident sharing. The NM-SIG can provide tooling and/or advice for sharing of incidents.

Liliana Solha: What is the relation between FIRST and the NM-SIG?

Menno Muller: The NM-SIG is a subgroup within the FIRST community. Work on network monitoring should be done in the NM-SIG and the result should be available for FIRST. The NM-SIG should be the entry point for all FIRST members interested in network monitoring

Liliana Solha: The Birth certificate should express that we share everything within FIRST. That can be accomplished by stating on the FIRST website what the NM-SIG offers to the FIRST community.

Menno: I hope that one outcome of this meeting will be that we will set up a website as a sub-site of the FIRST website.

Liliana Solha: The NM-SIG should indicate clearly on the website what the current developments are. It should offer a clear entry point to all FIRST members interested in network monitoring.

Everyone agrees.

*Next the text of the draft Birt certificate (v0.2 - 7 feb 06) is discussed sequentially.*

**Why this SIG?**

Everyone agrees on the three bullets

**Goals**

First bullet: "Provide a platform to actively exchange monitoring technologies, software and knowledge"

Liliana Solha: The NM-SIG should contribute to the whole of FIRST. It should be clearly stated that membership of the NM-SIG, at this moment, will only be open to FIRST members. On the website there should be a public area with information about the NM-SIG. The rest, e.g. the tooling repository, information on our monitoring project should be published on the members-only part of the website.

K.T. Yung: Is it required that the establishment of the NM-SIG will be approved by the Annual General Meeting?

Menno Muller: Arnold Yoon, the Steering Committee member for this SIG, will address that issue later on in the meeting.

Christophe Birkeland: Why should membership for the NM-SIG only be open to FIRST members? Consequently you'll potentially miss out on interesting initiatives that are out there.

Menno Muller: Especially at the beginning of the NM-SIG trust is utterly important. FIRST membership offers an appropriate level of trust. Information about other initiatives will probably find their way to the NM SIG via the members who know about it.

Carol Overes: We could also decide to invite (non-FIRST) organizations to give a presentation at a NM SIG meeting. Hence get the best of both worlds.

**The conclusions (and decision) of the discussion about the goals:**

- We start with a group that mainly consists out of FIRST members.
- Invitations of non-FIRST members for presenting initiatives outside the NM-SIG to the group will be acceptable (we trust the one you trust).

Second bullet: "Promote situational awareness and support research into more secure systems and networks"

K.T. Yung: We can also propagate good things to non members or within FIRST. This can be achieved by putting general information about the NM-SIG on the public part of the FIRST website, and more specific information on the members-only part of the FIRST-website.

Everyone agrees.

Third Bullet: "Join forces in current global (software)developments to reduce cost and improve performance"

K.T. Yung: Global (software)development in this statement too generic. It should be focused on (software) development regarding network monitoring.

Everyone agrees.

Fourth Bullet: "Gradually work towards a common set of monitoring tools and techniques" **and**

Fifth bullet: "Participate in the long term development new technologies regarding network monitoring"

Liliana Solha: Setting up a tool repository may be very helpful. It turned out to be so in Brazil, where the repository is being managed by a separate working group. Common formats will also be valuable. An discussion follows on that comment.

**Conclusion: bullet 4 and 5 will be rewritten to express the following points:**

- working to a common set of standards or formats
- working to a long term repository of tools.

### ***Scope / Limitations***

First bullet: "The SIG's focus is on monitoring technologies in the broadest sense of the word (hence there's no limiting definition as to what monitoring is all about and what not);"

Erka Koivonen: The word Monitoring could create some confusion with the work of Intelligence Services.

John Hyllman: Hedging on the word Monitoring will also raise questions with Human rights organizations.

Peter Wallstrom: We should focus primarily and solely on technology. Thus stay far away from all sorts of legal issues.

There were suggestions to state that members of the NM-SIG will use monitoring only for legal purposes, but the outcome of the discussion was that this is something for lawyers. In the end it all is simply not the NM-SIG's turf to deal with all sorts of intricate and very complicated legal matters. Let's do what we are good and hence focus primarily on technology.

**Conclusion:** we decide not to change the text of this bullet.

Second Bullet: "The SIG has no ambition to set global standards for monitoring data exchange;"

Everyone does agree, but the following comment was made: It may gradually grow to a global operational framework. This will not be our ambition, but may be and additional outcome in the long term.

Third Bullet: "The SIG has no intention to become an auditing or certification authority regarding monitoring systems and technologies whatsoever"

Everyone agrees.

Fourth bullet: "The SIG is focused primarily on technical issues, rather than policy or legal issues"

Everyone agrees

**Conclusion:** all comments will be processed and the chair will send out an updated version of the Birth certificate.

## **4. DISCUSSION: HOW WILL THE NM-SIG ACHIEVE ITS GOALS**

Menno Muller suggests to two means:

- create a website stating what we do do and what's going on in the area of NM
- maintain an email list.

Liliana Solho: It is necessary to appoint someone who is responsible for the website. Everyone agrees that NM-SIG presence on the FIRST website is necessary

Arnold Yoon: Each team can give a presentation on the FIRST TCs in Seoul and Latin America.

Mirosław Maj: It will not be possible for many teams to visit these TCs. Maybe we can make an inquiry in order to compose an uniform survey of all activities by NM-SIG members.

K.T. Yung: We should make a questionnaire for NM-SIG members in order to make an inventory of their activities.

Carol Overes: Maybe a combination is possible: a questionnaire and presentations on the next NM-SIG meeting.

John Hyllman: It will be good to present the information only on the FIRST member pages so it could not be used by the wrong community.

Menno Muller: Only the general information should be made public. All other information should be available to all FIRST members.

Bill Eaheart: Hopefully publishing does gain interest to other FIRST members.

John Hyllman: It should be each team's responsibility to decide what they want to publish or not (expecting that being part of FIRST generates enough trust) .

Arnold Yoon: Maybe it turns out to be possible to publish a kind of compilation of the queries on the public FIRST site.

Menno Muller: We should consider three steps:

1. first discussion on the NM-SIG list and decide on a definite version
2. publication on the FIRST members site
3. maybe later a compilation on the public part of the FIRST site.

#### **Conclusion on the 'how' question:**

- a questionnaire-template for team information will be created by a small working-group (and filled in by all the NM SIG members);
- the information will be published on the FIRST members site;
- further discuss this issue in the next meeting on the 13<sup>th</sup> of September in conjunction with the GOVCERT.NL Symposium (see below).

#### **Questionnaire/template working-group**

- Bill Eaheart
- Carol Overes
- Jonas thambert
- Uday Banarjee

The template will be published on the email list. After processing the comments it will be sent to all NM-SIG members in order to fill it in.

The group aims to get the draft template ready during this FIRST meeting.

#### **Website working-group:**

- Liliana Solho
- Eurique Curiel

The working group will come up with a draft outline of the NM-SIG web-presence in July and post it on the e-mail list.

#### **Next meeting**

On September 14 and 15 the GOVCERT.NL symposium will be held in The Hague, Netherlands. This symposium will be visited by NM-SIG members from CERT-FI, SITIC, DFN-CERT, AusCERT, CERT/CC, CERT-Polska, JPCERT and SURFnet.nl.

On the day before the GOVCERT.NL symposium (Sep 13<sup>th</sup>) there will be a meeting arranged for NM-SIG members on these issues :

## Minutes of the NM SIG kick off meeting - June 25 2006, Baltimore, USA

- Discuss the 'how' question into much more detail;
- Presentations of monitoring activities of NM-SIG members
- The public and members-only page of the NM-SIG on the FIRST website
- The questionnaire-template

### 5. DISCUSSION: RULE SET AND PROCEDURES NM-SIG

Arnold Yoon thanks GOVCERT.NL for sponsoring this meeting and elaborates on the 'rules for SIGs'. The Steering Committee works on an operational framework for SIGs. This will be further discussed in the Annual General Meeting. FIRST can play a role in the infrastructure surrounding a SIG:

- logistics
- website
- email list
- IRC

A SIG needs some document stating (NM-SIG: birth certificate);

- who will be the point of contact for the Steering Committee
- what is the goal of the NM-SIG

Furthermore the chair should regularly report about the progress of the SIG, e.g.:

- minutes of meetings
- deliverables

SIGs are free in their funding and attraction of sponsors. A policy for information disclosure should be formulated

The meeting appoints Menno Muller as chair by acclamation. To decide if members will be available as vice chair, the teams will check their budget, as it will be necessary for the vice chair to visit the meetings. If no one will show up, Liliana Solho and/or Till Dörge will be available as vice chair.

Carol suggests a procedure for new members of the NM-SIG:

- must be a FIRST member
- fill in the questionnaire-template

#### Conclusion on the rules and procedures:

- New SIG members need to fill in the questionnaire ;
- Menno Muller is the chair of the NM-SIG;
- The NM-SIG has met the (formal) demands regarding setting up a SIG.

### 6. WRAP UP (DECISIONS AND ACTIONS)

#### DECISIONS

Decision nr.	Decision
1	The NM-SIG is a group for FIRST members, to keep an appropriate level of trust. Invitations of non-FIRST members for presenting initiatives outside the NM-SIG to the group will be acceptable. New member will have to fill in the questionnaire (which is currently being set up)
2	The definite results of the NM-SIG will be made available to the FIRST community (after having discussed it within the NM-SIG). The NM-SIG decides whether, and if so what information is distributed to the public
3	The Birth Certificate is the NM-SIG's official document with its goals, scope and the point of contact for the Steering Committee

**Minutes of the NM SIG kick off meeting - June 25 2006, Baltimore, USA**

<b>4</b>	Menno Muller (GOVCERT.NL) is appointed as chair of the NM-SIG and point of contact for the Steering Committee
<b>6</b>	Arnold Yoon is the NM-SIG FIRST SC Liaison
<b>7</b>	The NM-SIG is focused primarily and solely on technical issues (rather than policy or legal issues)
<b>8</b>	FIRST is the umbrella-organisation for incident sharing. Therefore, sharing of information about incidents is done within FIRST and not particularly within the NM-SIG. The NM-SIG can provide tooling and/or advice for sharing of incidents within FIRST
<b>9</b>	The NM-SIG will work on a common set of standards or formats, which can be used within the NM-SIG and/or FIRST community. On the longer term a repository of tools will be created and is accessible for FIRST members

**ACTIONS**

<b>Action item*</b>	<b>Description</b>	<b>Who</b>	<b>End date</b>	<b>Status</b>
<b>250606.01</b>	Process comments on Birth Certificate	<b>Menno Muller</b>	End July	Pending
<b>250606.02</b>	Creation web-presence of NM-SIG (public and members-only page & entry point for interested FIRST members)	<b>Liliana Solha (and working group)</b>	End July	Open
<b>250606.03</b>	Creation of a questionnaire in order to make an inventory of the monitoring activities within the NM-SIG	<b>Bill Eaheart (and working group)</b>	Mid July (draft)	Pending
<b>250606.04</b>	Propose a new date and agenda for the next meeting	<b>Menno Muller</b>	Mid July	Pending
<b>250606.05</b>	Update list of members and the mailing-list of the NM-SIG	<b>Arnold Yoon</b>	End July	Pending
<b>250606.06</b>	Draw up minutes of the kick-off meeting	<b>Hans Petri &amp; Menno Muller</b>	Early July	OK
<b>250606.07</b>	Creation of 'Rules and Procedures'-document for the NM-SIG	<b>Carol Overes</b>	Early Aug	Open
<b>250606.08</b>	Comment on the draft minutes, website outline and questionnaire / template	<b>ALL</b>	When asked for	Ongoing

\*day;month;year.number

**WRAP UP**

In the final round of questions/ famous last words everyone mentions that this was a very good start of something new. It's now up to each one of us to keep the flow going.

Menno Muller kindly thanks all attendees for their participation in this fruitful NM-SIG gathering and closes the meeting at 12:00 am.

**After the meeting CAIS/RNP gives a presentation of their monitoring work (in 7 projects).**

Plenty of positive feedback and comments are given