SIXTH FRAMEWORK PROGRAMME
Structuring the European Research Area Specific Programme

RESEARCH INFRASTRUCTURES ACTION

European Network of Affined Honeypots

Contract No. RIDS-011923

D0.2: Requirements Collection and Analysis

Abstract: This document presents the requirements for the NoAH infrastructure, as they are drawn from the responses on NoAH's questionnaire and from the discussion between consortium members.

Contractual Date of Delivery	***09/30/05***
Actual Date of Delivery	***11/18/05***
Last Update Date	***06/02/06***
Deliverable Security Class	***Public***
Editor	***FORTHnet***
Contributors	*DFN-CERT, FORTH*

The NoAH Consortium consists of:

FORTH-ICS	Coordinator	Greece
VU	Partner	Netherlands
TERENA	Partner	Netherlands
FORTHnet	Partner	Greece
DFN-CERT	Partner	Germany
ETH Zurich	Partner	Switzerland
Virtual Trip	Partner	Greece
Alcatel	Partner	France

Table of Contents:

1. Introduction

The goal of the NoAH project is to produce a design study and perform the necessary technical work towards the development of an infrastructure for security monitoring based on the honeypots technology. In order to specify NoAH's requirements, National Research Network organizations (NRNs) and Internet Service Providers (ISPs) should primary analyse their requirements with respects to their needs from a honeypot infrastructure and the privacy concerns regarding the released information. The requirements of Computer Emergency Report Teams (CERTs) from such a system, should also be considered when NoAH's requirements are specified.

In order to define the requirements for the NoAH infrastructure, as well as to investigate emerging and future needs for security monitoring, a questionnaire regarding security issues with honeypot collaboration, was prepared and delivered to NRNs, ISPs and security-involved people from other Organizations and Companies.

The distributed questionnaire, contained thirty nine questions, divided into the following five sections:

1. Part A : General Organization Information (4 questions).
2. Part B : Organization Infrastructure (5 questions).
3. Part C : Monitoring issues (9 questions).
4. Part D : NoAH operation (8 questions).
5. Part E : Cooperation with NoAH (8 questions).

The questionnaire was anonymous, in order to attract more people to filling it in and none of the containing questions were compulsory. Answering the questions involved selecting the most appropriate answer from a list of possible answers in each case. The respondents could also provide a comment/remark on a specific question.

The invitation for participating in NoAH's survey was sent to NRNs, Universities, ISPs and other commercial and governmental organizations and also to individual persons involved in security monitoring issues. There were totally 42 responses for this questionnaire in a four-month period (June 2005 – September 2005).

Along with this questionnaire, there was internal consortium collaboration for the definition of requirements from an early warning system, such as NoAH. All project partners clearly expressed their needs for security monitoring and their expectations from NoAH's infrastructure. In this way, different opinions and approaches in all aspects of NoAH's design were evaluated.

In the following four sections we summarize and comment responses obtained for each question of NoAH's questionnaire. Following, there is a section containing the requirements of a Computer Emergency Response Team (CERT) and a section that presents the results of a survey on projects related to NoAH. Finally, overall conclusions and directions obtained from the requirements analysis process are presented.

The complete set of questions of the questionnaire is presented in Appendix A2.

2. General information about the organizations

This section contains questions related to the organizations that were invited to participate in NoAH's questionnaire. Some of the aspects that these questions aim to investigate are the type of the participating organization and their network resources. The collected information will contribute to the development of the requirements regarding NoAH's operation and collaboration with existing resources.

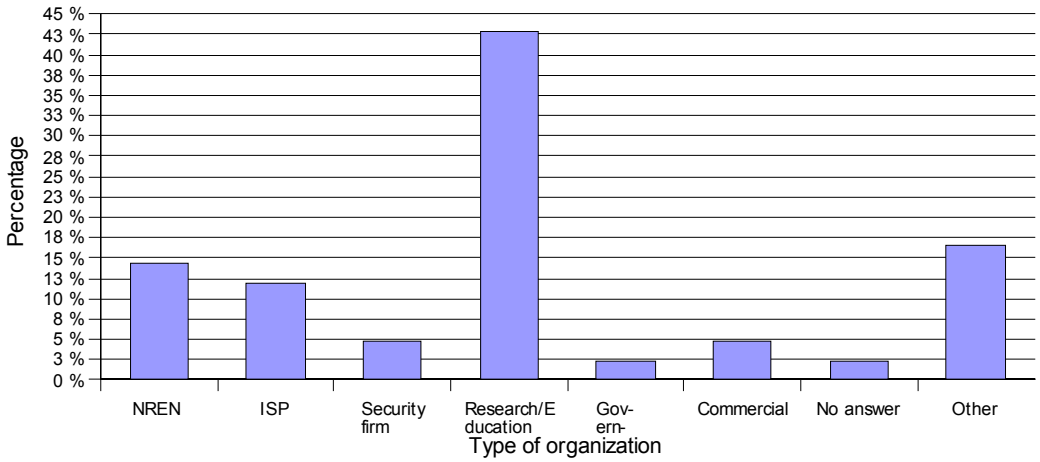

Figure 1 : Organization type

Figure 1 illustrates that out of the 42 organizations that responded to NoAH's questionnaire, 14.26% of them are NRNs (6), 11.90% ISPs (5), 42.86% of them are research organizations and universities (18), 2.38% government organization (1) and 4.76% are commercial organizations (2). There are also questions answered by one Telecommunications company, one RREN, one Open Source Security Solution Developer, one FFRDC and one Technology Integrator.

Concerning the number of hosts of those companies, 69.05% of them (29 out of 42), operate networks with more than 50 hosts (Figure 2). It is worth mentioning, that some of these organizations have a really large number of hosts, sometimes greater than 3.000 or 5.000 hosts around the world.

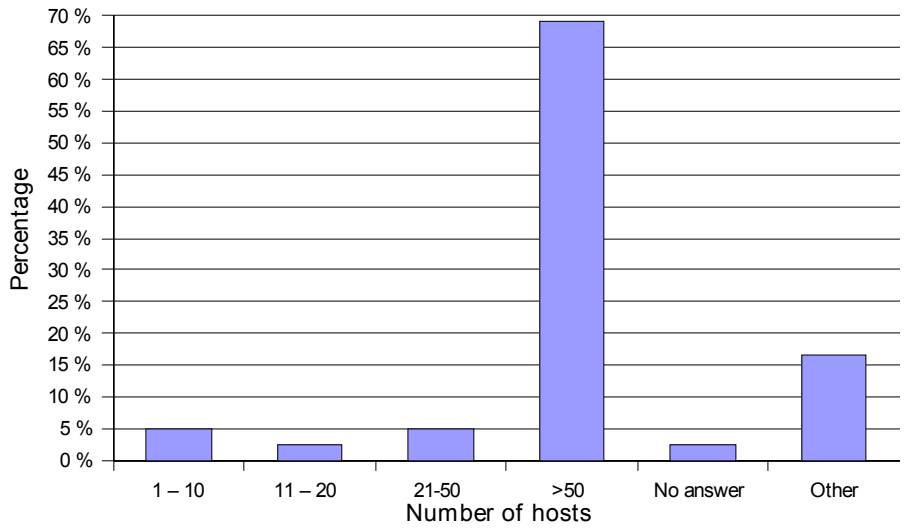

Figure 2: Number of hosts

88.10% of the responding organizations (37/42), use LAN network architecture for their internal network while 33.33% (14/42) of them also use MAN and 59.52% of them (25/42) WAN architecture (Figure 3).

Regarding the operating systems used within an organization, Linux (several versions) and MS Windows, are more popular (40 out of 42 organizations). There are also some organizations that use Unix (32 cases) and others that use non-accurately defined operating systems (Mac OS X, OpenVMS, AS400, HP UX) (Figure 4).

Finally, as it is illustrated in Figure 5, most organizations operate their own NOC (Network Operation Centre) and only a few (3 organizations) have their NOC outsourced.

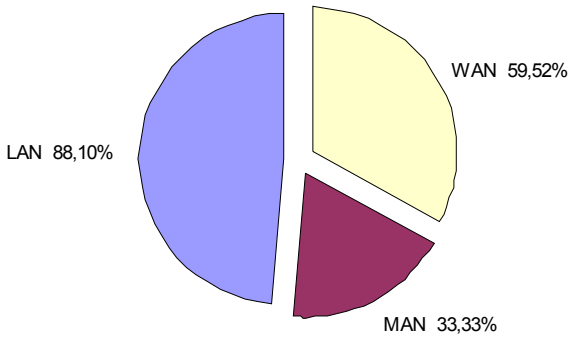

Figure 3: Organization network

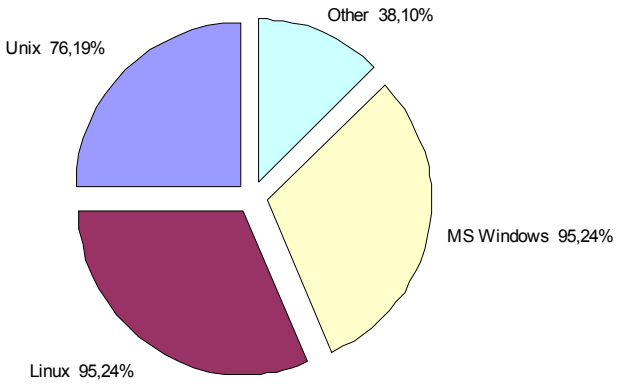

Figure 4: Operating system(s) used

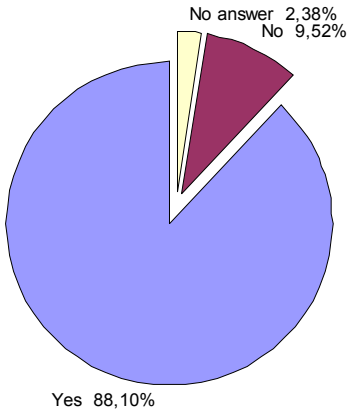

Figure 5: Security Department / NoC

As the above responses indicate, the majority of organizations are interesting in using early warning security systems, such as NoAH. Different organizations have different needs and requirements from such a system. So, a flexible infrastructure like NoAH's should be easy to configure. Also, system is necessary to be scalable and expandable in order to correspond to future needs that have not been preceded yet.

Even more, an infrastructure like NoAH's, should be platform independent in order to work efficiently, since there are more than one operating systems used within a unique organization as well as different network architectures. Finally, the system should not interfere with an organization's internal network in order to be protected against any malicious and unpredictable threat.

3. Monitoring issues

This part of the questionnaire aims to investigate the existing needs for security monitoring, as well as, the tools and methods that are currently used for protection against cyber attacks.

As indicated in Figure 6, only a small fraction is not interested in system monitoring, while more than 93% consider this as important or even a crucial task. The importance of system monitoring is even more clear in Figure 7, which indicates that several security tools are already used by all the participating organizations. Firewall and anti-virus software are used almost by everyone (88.10%) , while the 73.81% of the responding organizations (31/42) use passive monitoring tools (such as Dark Space Telescope, Snort, Ethereal) and 64.29% (27/42)use active monitoring tools (such as RIPE TTM , ZAP). There are also 17 cases of organizations (40.48%) that already use honeypots technology (such as, honeyd, MwCollect).

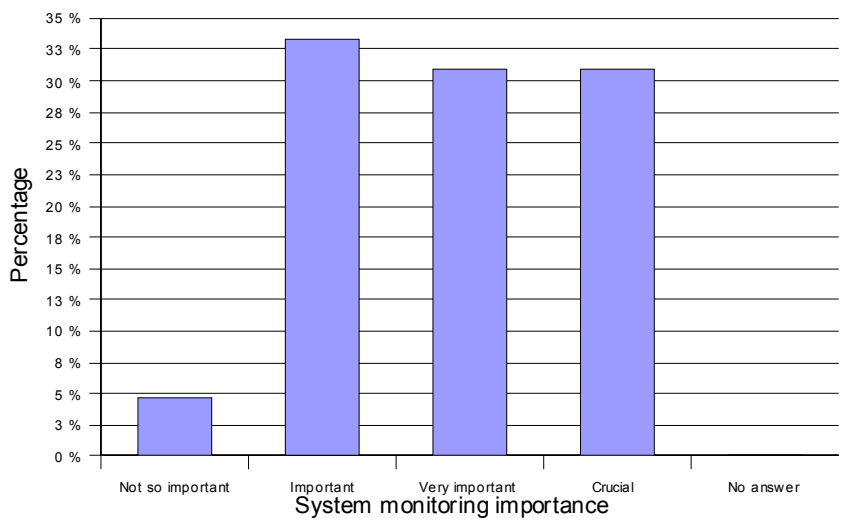

Figure 6: System monitoring importance

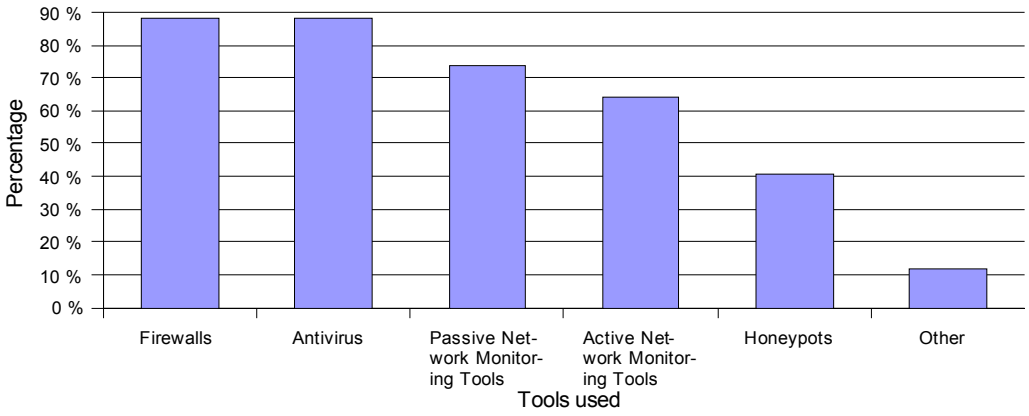

Figure 7: Security / monitoring tools used

88.10% of the organizations mentioned that their system monitoring tools aim to detect intrusion attempts against their infrastructure (37/42). 59.52% (25/42), also use these software for failure diagnostics and 52.38% for debugging performance problems (22/42). It is also mentioned that system monitoring tools are also used for malware analysis. Figure 8, indicates those statistics.

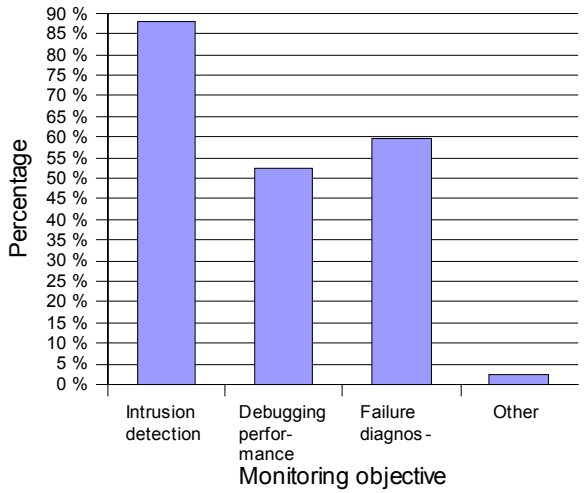

Figure 8: System monitoring objectives

The most frequent kind of detected attacks concern virus and worms (92.86%). Intrusion attacks and spamming are also commonly detected (73.81). DDoS attacks and network traffic sniffing are also possible to occur (54.76% and 35.71% respectively). There are also two other kind of attacks mentioned: bots and insider malfeasance. The above ratios are illustrated in Figure 9.

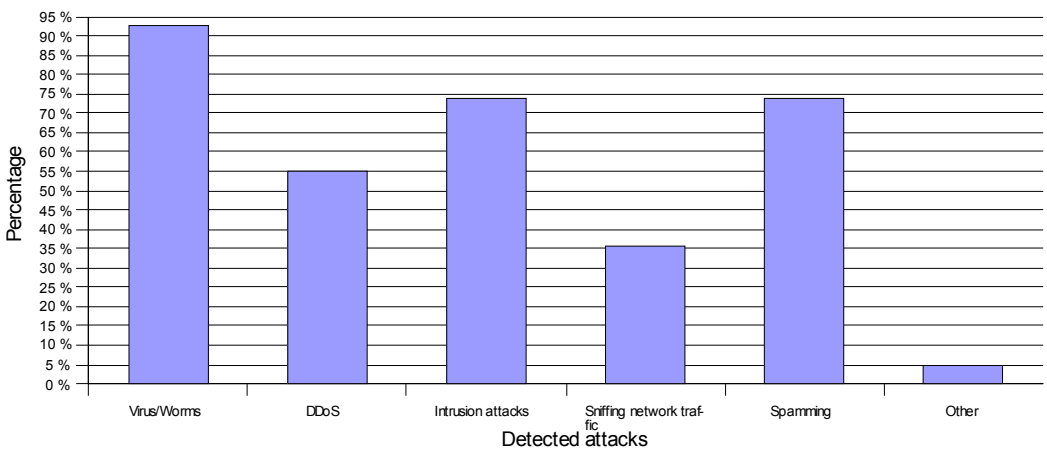

Figure 9: Attacks usually detected

The network services operated differ among the organizations. Almost everyone operates WWW services and email and also operates SSH (TELNET) services (97.62%). DNS and FTP services are also very frequently used (92.86% and 80.95% respectively), while SNMP service is used by some of the organizations (71.43%). Figure 10 also indicates that 47.62% of the queried organizations, use peer to peer applications, 21.43% use ERP and 16.67% use CRM applications. It is also mentioned that video streaming applications are used. These services are the common target of various cyber attacks. In order to protect against the

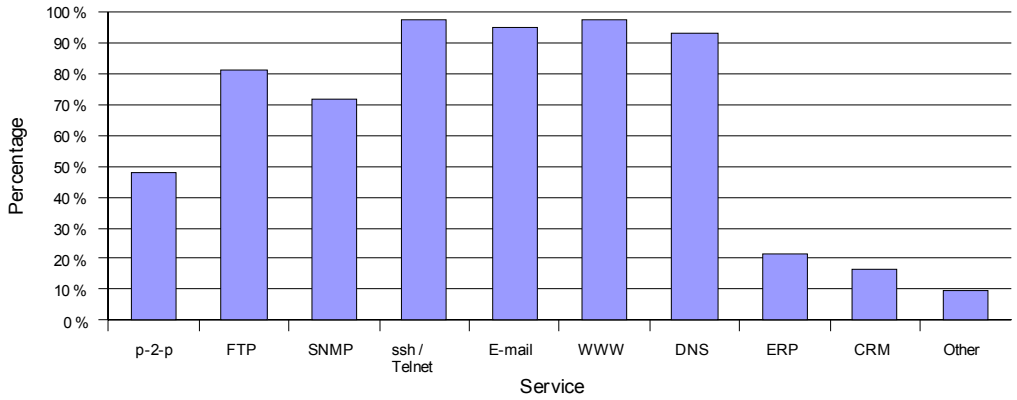

Figure 10: Services operated

cyber threats, the organizations operating the above services, use a variety of system monitoring and security tools.

Referring to the response time of the system in case of a detected attack, 47.62% of the participants (20/42), consider as satisfying response time an interval of time between 10 to 30 minutes. However, 35.71% of them (15/42), think that the response time of a potential system should be less than 10 minutes. Finally, three participants accept a response time greater than 30 minutes and two of them would prefer it to be less than 1 minute. The above statistics are illustrated in Figure 11.

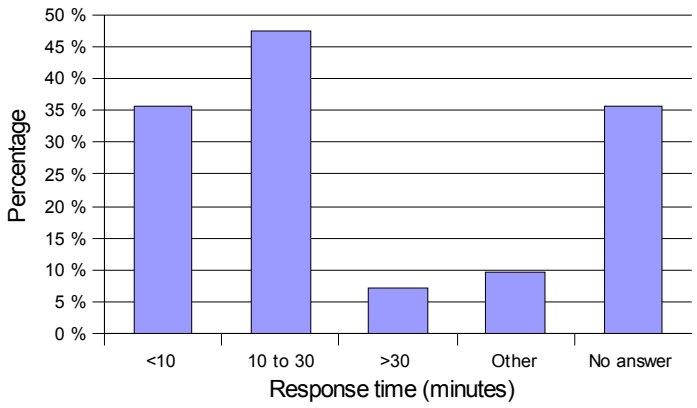

Figure 11: Satisfying response time

Concerning the number of honeypots needed in order to produce a valid alert on a potential attack, Figure 12 indicates that 23.81% of the participants (10/42) think that 6 to 10 honeypots should be used. However, 19.05% of them (8/42) thinks that 1 to 5 honeypots are enough for a valid alert and 26.19% believe that more than 20 honeypots should be used (11/42 respectively). Finally, there is one participant that believes that 11 to 20 honeypots should be used and two others who think that the number of honeypots needed for a valid alert production, depends on the attack and could vary from case to case. It is worth mentioning that 21.43% of the participants (9/42) responded "No answer" to the specific question. The above responses are probably relevant to the size of each organization's network, as well as to the desired reliability of the infrastructure.

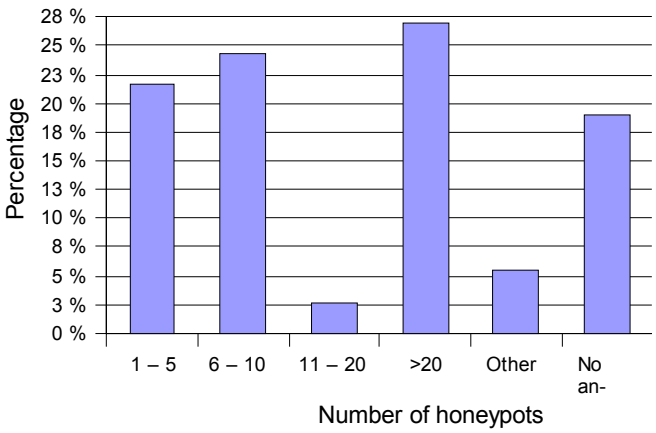

Figure 12: Number of honeypots

The data produced by the monitoring system, in most cases should be received by the organization's network operator/administrator (83.33% of the responses). The system administration and the network administrator (if any) of the organization should also be aware of those data (71.43%). Finally, if there is a corporate manager, he/she should also receive the data (11.90%). Other potential recipients of the data produced by the monitoring system - that are mentioned - are CERT, potential security officers/contacts/groups or an IDS team. The above are shown in Figure 13.

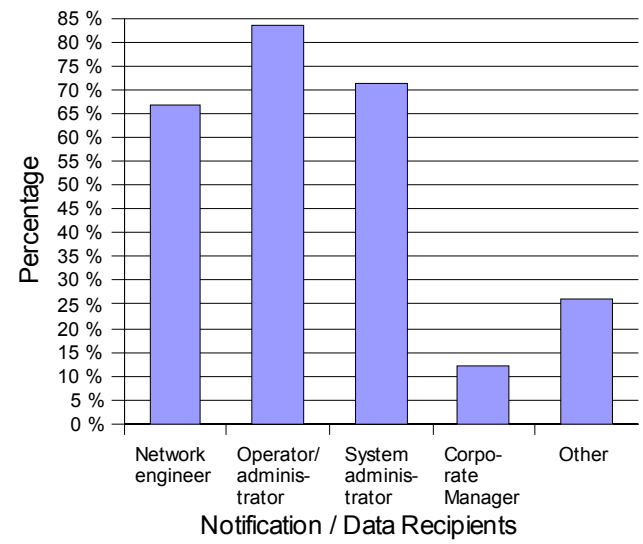

Figure 13: Notification / Data Recipients

In conclusion, an infrastructure that use honeypot technology, such as NoAH, should primary be able to detect different kinds of cyber attacks. Each attacker may exploit different kind of services in order to invade one honeypot (e.g. mail services may be under attack). So NOAH's honeypots should be flexible enough in order to be a useful security tool for everyone. What is more, the reaction in case of a detected attack should be as fast as possible. Once an attack is detected, NoAH should send the data concerning the attack the sooner possible. However, these data should be well formatted and easy to understand by different people (e.g. engineers, administrators, etc).

4. NoAH operation

The questions contained in this section aim to investigate the desired operation of NoAH's infrastructure. Particularly, the issues examined are related with NoAH's configuration and installation process, as well as, with the type/volume of data that potential users should be interested in receiving from such an infrastructure, and the usage of this data.

Concerning the data usage, Figure 14, indicates that most of the participating organizations (38/42 – 90.48%) would use the obtained data for research. However, 76.19% of them (32/42) would also like to use it for education and 45.24% for commercial purposes, as well (19/42). Finally, there are cases mentioned, where the acquired data could be used for strategic or national security purposes.

Following, in case of a detected attack, almost everyone agrees that all the participants of NoAH infrastructure should be immediately alerted (36/42 – 85.71%). Some of them (76.19%), would also like to receive guidelines or hints on how to defend against this attack. Logging all Internet traffic is something that 45.24% of the participants (19/42) agree with, although there is a negative comment about this, underlining that logging all Internet traffic is a step towards the wrong direction and that no one should be monitored against their will. Finally, it is suggested that NoAH infrastructure should provide automated data feeds for independent analysis. The above metrics are illustrated in Figure 15.

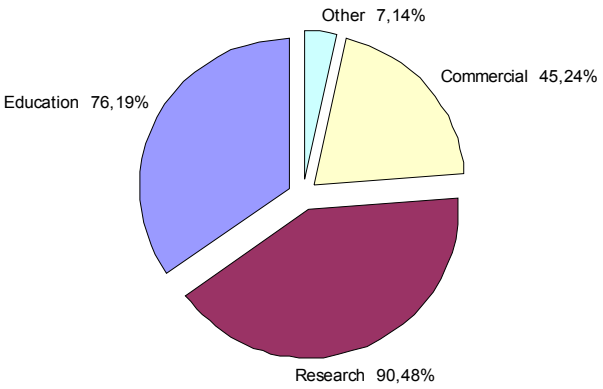

Figure 14: Usage of NoAH data

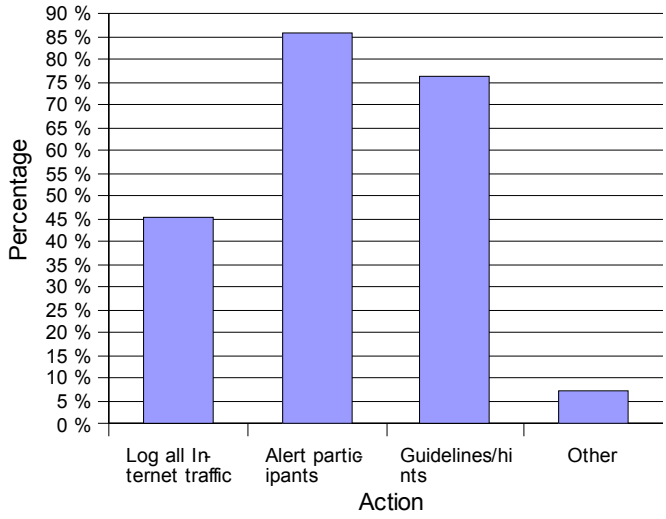

Figure 15: Actions in case of attack

It is interesting to point out that 45.24% of the participants in NoAH's questionnaire have used honeypots in the past. Figure 16, also indicates, that 33.33% of participants (14/42) have never used honeypots before, while there were 9 of them (21.43%) that did not answer the specific question.

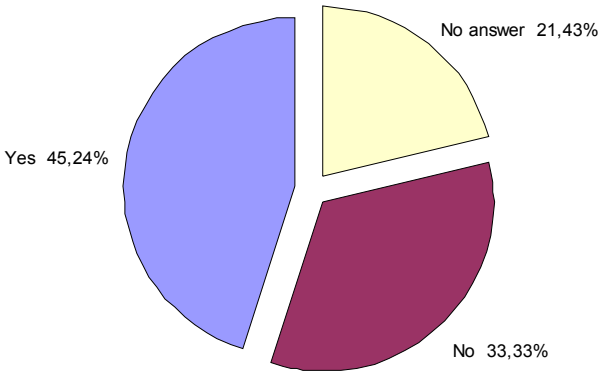

Figure 16: Have you ever used honeypots?

The level of interaction for the participants who have previously used honeypots is medium for the 14.29% of them, high for the 16.67% of them and low for the 7.14%. The honeypots that some of the participants have worked with is Honeynet, Honeyd and custom made honeypots. The above statistics are indicated in Figures 17 and 18 respectively.

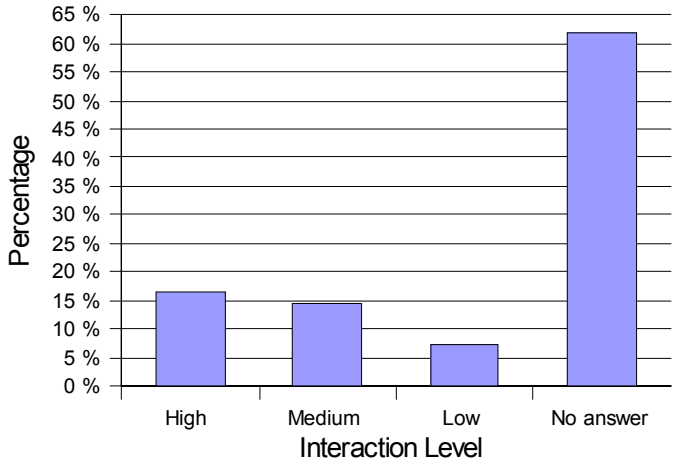

Figure 17: Level of honeypot interaction

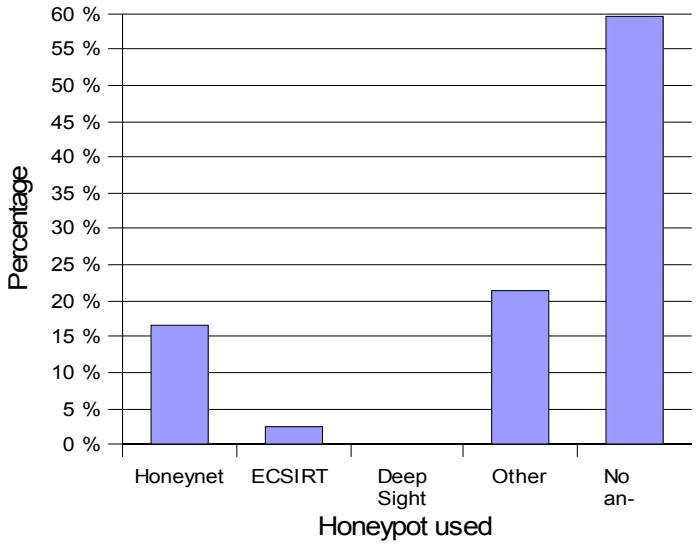

Figure 18: Honeypots used

Regarding the installation of a honeypot within the organization (Figure 19), 73.81% of the participants (31/42) responded positive in such a case. There were also three negative responds (7.14%) and 19.05% of the participants avoided answering the specific question. However, in hypothetical case where NoAH's honeypots were installed in one's organization (Figure 20), 71.43% of the participants (30/42) responded that they would like themselves to be responsible for the installation and configuration of those honeypots. 14.29% of them (6/42) would like to get a remote installation and configuration while 11.90% would prefer a central help-desk. Following, for the question concerning the maintenance and management of a NoAH's node within one's organization (Figure 21), almost every participant responded that they would like to do it themselves (33 out of 42 – 78.57%). However, in five cases they would like it to be done by an independent consortium.

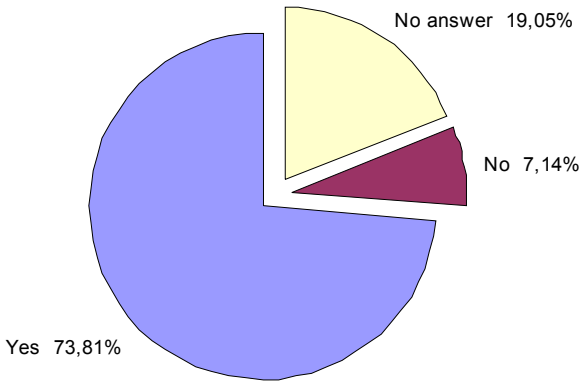

Figure 19: Agree to have a honeypot?

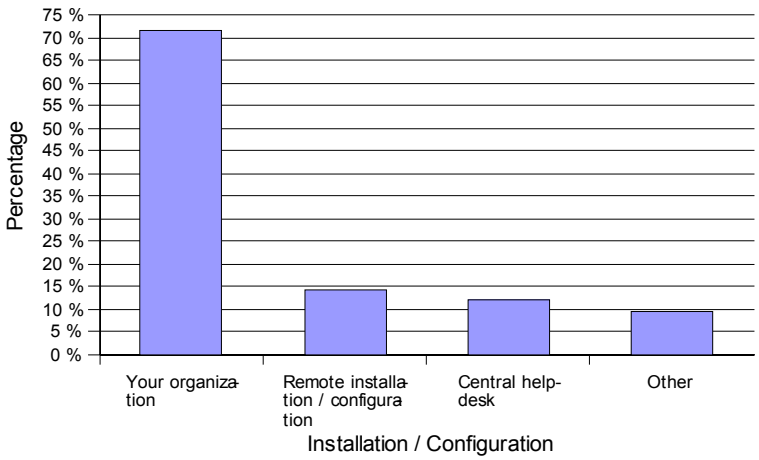

Figure 20: Honeypot installation / Configuration

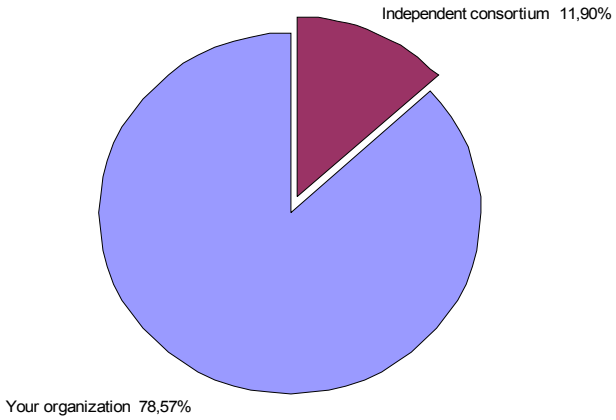

Figure 21: Honeypot maintenance

Finally, for the question regarding whether the participants would be willing to share the obtained data with others or not (Figure 22), there were 29 positives questions (69.05%), one negative (2.38%) and twelve of the participants avoided answering it (28.57%).

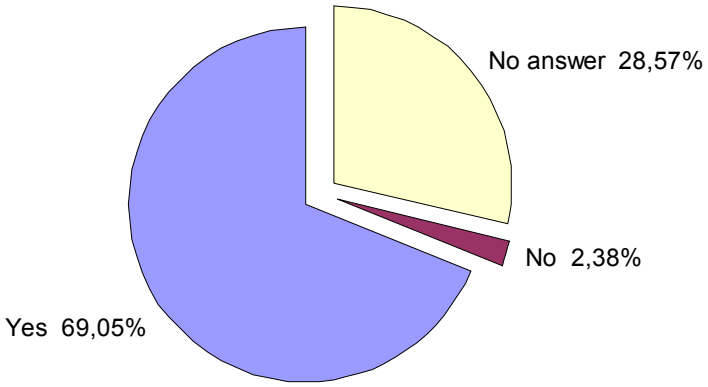

Figure 22: Share honeypot data?

Concluding, as figures above indicate, most of the people answering the questionnaire seem somewhat concerned about having NoAH's honeypots installed within their organization. It is also obvious, that in case they joined NoAH's infrastructure, they would prefer themselves to be responsible for installing, configuring and maintaining the honeypots within their organization. Regarding the reaction of NoAH's infrastructure in case of attack, most of the potential users seem to prefer to receive an alert along with some hints/guidelines about the attack and how to defend.

5. Cooperation with NoAH

This part of the questionnaire deals with the information the NoAH infrastructure should provide. Particularly, it examines the kind of data that would be of more help for potential users, depending on their needs and expectations from security monitoring.

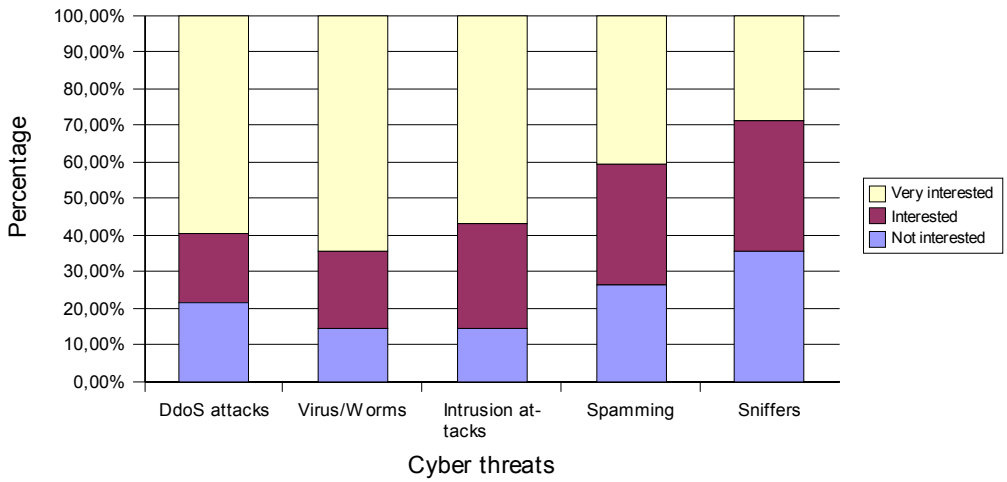

Figure 23: Level of interest per attack type

As indicated in Figure 23, potential users are interested in cooperating with NoAH for detecting various kinds of attacks. The most frequent attacks they would like to be aware of are the existence of virus and worms (27 positives answers), DDos attacks and intrusion attempts (25 positive answers respectively). There is also interest in email spamming and sniffers (17 and 12 answers respectively).

Concerning the information about the attack that will be of most use, almost everyone would like to get feedback on the type of attack (95.24% of obtained answers). There is also great interest in receiving a signature for the attack (85.71%) as well as getting information about the method used by the attacker, on each case (78.57%). Information about the tools used by the attacker and about the attacker's sophistication also interests the organizations queried (66.67% and 59.52% respectively). There is also a request for information about the speed the attack is spreading. Finally, regarding the attack's origin, everyone would like to

know the attackers' IP or DNS and 25 of the respondents would also like to receive geographical information about them (country / city / providences). There is also one case that a personal identification about the attacker would be useful! The above statistics are illustrated in Figure 24 and Figure 25, respectively.

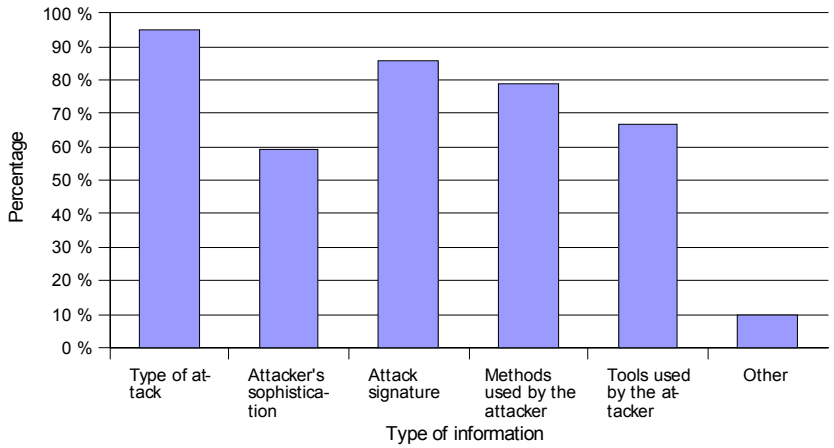

Figure 24: Information provided by honeypots

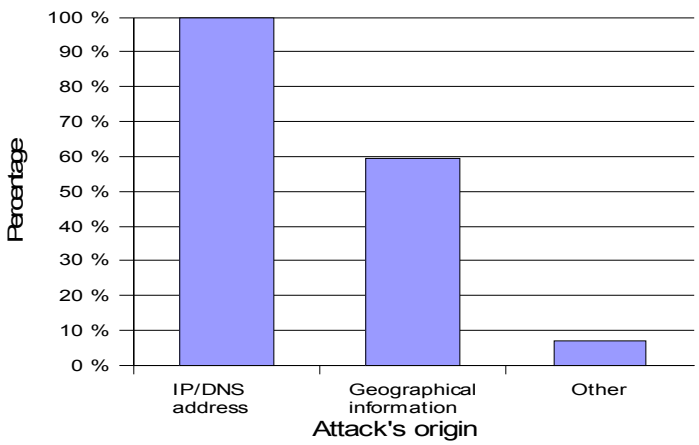

Figure 25: Attack's origin

Referring to the kind of alerts sent by NoAH in case of a detected attack, Figure 26 indicates that almost everyone (88.10%) would like to get an email alert. Log files (47.62%) and a web site that is automatically updated (35.71%), also seems to be preferred by the respondents. Finally, there is a small ratio of them that would like to get an SMS alert (33.33%). It is worth pointing out that there is an argue on the efficiency of those alert mechanisms, since there might be cases of threats that spread faster than all these alert mechanisms can act.

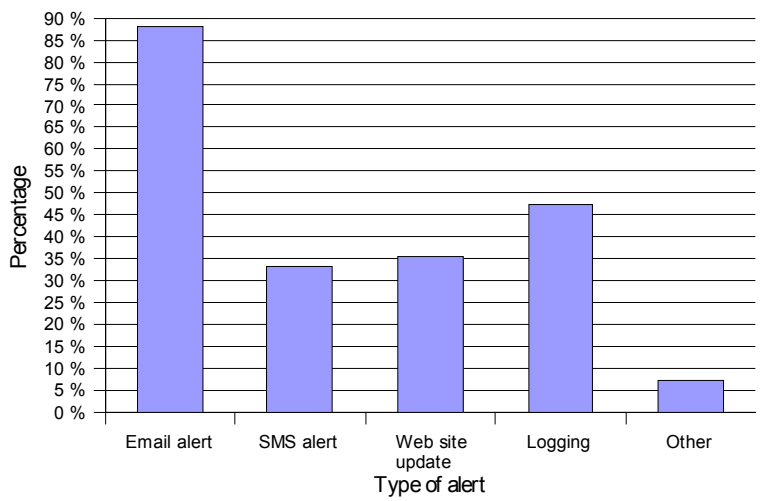

Figure 26: Alert on attack detection

About the tolerance on false positives, Figure 27 illustrates that 50% of the participating organizations would accept 0-2 false alarms per day, 26.19% of them would not mind in getting three to five false positives and 2.38% would even tolerate ten false alarms. However, there is one case of a participant who supports that there must not be any false alarms.

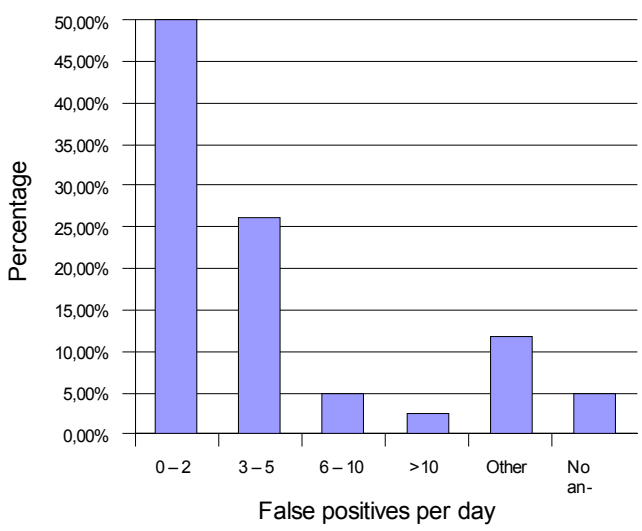

Figure 27: Rate of false positives per day

Concerning the signature of an attack, almost everyone (92.86%) would like to get an IP packet-based signature, while 42.86% of the participating organizations would also like to get a signature which is composed of a series of system calls used by the attacker. These ratios are illustrated in Figure 28.

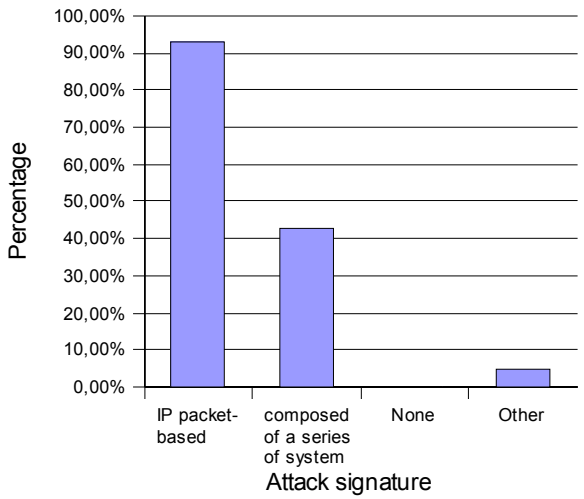

Figure 28: Attack's signature

For the question about potential cooperation with NoAH, there where 25 positive responses (59.52%), one negative (2.38%) and 16 of the respondents (38.10%) avoided answering the specific question (Figure 29).

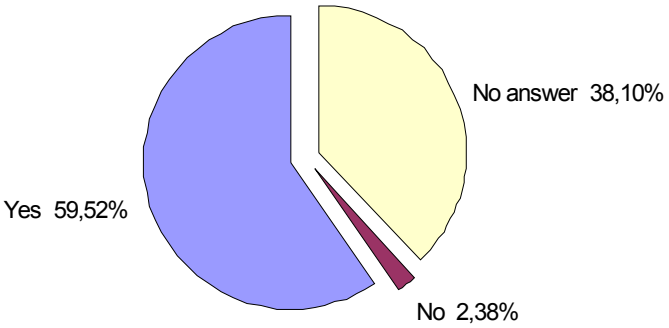

Figure 29: Cooperation with NoAH?

In conclusion, there is an increased interest for protection against virus and other kind of intrusions. However, the NoAH system should be able to detect as many different kinds of attacks as possible. Once an attack is detected, most users would primarily like to get information about the attacker, such as an IP/DNS or their identity, if possible. NoAH should generate signatures that contain such information and send it to all participants immediately by email or via updating a web page. NoAH's infrastructure should be developed in such a way that minimizes fault positives on possible attacks, in order to increase its reliability.

6. Requirements for NoAH from the point of view of a CERT

Computer Emergency Response Teams (CERTs) have special needs and constraints for honeypots that go beyond pure knowledge gain about the methods and tools used by attackers. In the following, a brief summary of the typical activities of a CERT is given and their requirements towards honeypots are explained. The current threat of botnets is used as an example.

6.1 Technical honeypot-architecture Requirements

Computer security teams come with different names like Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT). Despite the different names all of these normally provide incident response and some kind of alerting service for their constituent sites.

- Incident Response and Coordination

Incident Response means helping all affected sites to overcome the consequences of a security incident. The definition of a security incident as well as what is done to help the site varies widely. At the core of incident response the following questions are answered:

- What has happened?
- How did the compromise proceed?
- Which sites are involved in the incident?
- How to recover from the compromise?
- How to close the vulnerabilities?

In order to provide incident response, specific knowledge about methods, tools and common aims of attackers is very helpful. Most often several sites are involved in an incident. These are normally contacted in order to request help to track the attacker or just to inform the site about local malicious activity.

While staying in touch with all sites involved in the incident, relevant information gained at the first site is given to the next. This information is often anonymised by the CERT because some sites do not

want to publicly disclose the existence of the problem. The knowledge gained can also be useful in other incidents since the attackers often proceed in similar ways. The CERT takes on the role of information hub and this kind of incident response is often also called incident coordination.

- Alerting Service

In contrast to incident response, the alerting service aims at disseminating information concerning severe problems not only to the affected sites but also to the constituency of a CERT or even the general public. Alerts can be issued concerning different topics:

- Newly found vulnerabilities
- Available patches or workarounds
- Currently spreading malware, e.g. in the form of a new worm
- New tactics or tools for exploitation of vulnerabilities currently used by attackers

Sources of information are normally vendors, public or closed mailing lists, or research conducted by the CERT itself. A special case of alerting is the so called early warning which is intended to inform sites about emerging problems before they actually cause real harm. E.g. Scans for vulnerable systems are often done prior to the actual deployment or spread of a new exploit or before a vulnerability is widely known. A CERT detecting a sudden rise in scans for a certain service could conclude that a new worm is spreading or a new vulnerability has been found in an implementation of the corresponding service.

- Honeypots and Incident Response

Honeypots have obviously been of interest to CERTs since their conception, because they allow to gain first-hand knowledge about the attackers. From the perspective of a CERT there are certain constraints and needs beyond pure research.

The aforementioned information exchange via the CERT can be extended to honeypots. Information gained from a high interaction honeypot can be used in the same way without any real system being compromised or information stolen. This controlled information gain can

be widely expanded by deploying a whole network of honeypots. Important information for incident response include the following:

- How is the system compromised?

The knowledge gained by the analysis of a compromised system can be used to protect other systems. This gives the site the chance to shield vulnerable services or at least give them more attention if no patch is available.

- What tools are used to attack the system?

Since a high interaction honeypot is intended to be compromised and there is no regular use, all actions of the attacker including all software and exploits used can be recorded. Using a carefully prepared high interaction honeypot, even encrypted exploits can be captured in memory while being executing.

On the network and host level this helps detection or maybe even avoidance if the attack can be filtered. On the local system, certain exploits can be rendered useless by changing the environment slightly - e.g. removing a certain directory which is used as a drop zone by the exploit.

- How can this kind of attack be detected?

The observed data concerning the attack can be used by either host-based or network-based IDS systems to recognise similar attacks at an early stage.

- How is the compromise seen in the log files?

Attacks very often leave traces in the system logs of the compromised system. These traces enable the sites to decide quickly if a problem already exists.

- What is the attacker doing on the compromised machine and how can he be detected?

Most compromises follow a specific pattern. After the compromise, tools are installed to attack other systems and to stay in control after the

compromise is detected and the vulnerability has been closed. This includes the creation of certain kinds of accounts or the installation of backdoors. Again, this knowledge enables the sites to decide quickly if a problem exists.

Less obviously, the machine the attacker is connecting from is either the real source of the attack or, most probably, already compromised and a former victim. A CERT will usually inform the owners of the machine and explain the problem - urging them to stop the abuse or even track the attacker back another hop.

Compromised systems are used very often as a platform for subsequently attacking other systems. The tools used by the attacker on the honeypot to compromise more systems often include lists of already compromised or vulnerable machines. The owners of these are normally also contacted by the CERT (incident coordination).

Besides this directly useful information, the CERT learns how attackers work in general and might understand similar incidents more easily.

- Honeypots and Alerting Services

The information gained from honeypots can also be used within alerts sent to the whole constituency of the CERT or even the general public. This is usually done during wide spread exploitation of single vulnerabilities e.g. by a spreading worm.

In addition, honeypots can provide other information useful for alerting and the so called early warning. If rumours spread among attackers concerning a new vulnerability, scanning for the affected program or service will start. Most often this results in scans from few source IPs, which try to cover large parts of the Internet. This can be used as an indicator of emerging problems.

In the same way, the spreading of a newly created worm can be detected by it's slightly different scanning activity. The number of sources of scans will very rapidly grow while the worm continues to spread.

To gather information about scans and scan sources and to be able to make the above distinction, as much as possible statistical data is

needed. Whether the honeypot is of high or low interaction does not matter in this case. Since a low interaction honeypot is easier to deploy it will most probably be used to acquire this kind of data from multiple sources.

However, low interaction honeypots are limited by their properties. Most early warning approaches are based solely on finding anomalies in statistical data. But such anomalies can also be caused by singular licit events or e.g. by misconfigured software and will cause false positives: early warnings which turn out to be a non issue. To eliminate false-positives, high interaction honeypots are needed to complement and validate statistical data gained from low interaction honeypots.

- Example: Tracking a botnet with honeypots

A collection of compromised hosts under single command via a control channel is called a botnet. This is a typical abuse scenario CERTs have to manage and will be used as an example.

The control is exercised via a control channel which can facilitate HTTP, DNS or any other protocol. Most often IRC is used because it is easy to implement and a very resilient network of servers is publicly available.

- A typical botnet scenario

A typical botnet scenario could be the following. Single machines are compromised and malware is installed. The compromise itself can be achieved by various ways - e.g. through a worm, email-virus, a backdoor left behind by another malware.

Within the malware there is at least one set of connection information for a control channel. This botnet uses IRC:

hostname: x4711.evil-bot.net
port: 6667
channel: #drones

A compromised machine will look up the IP of the host name, connect to the port and enter the channel. Now commands can be given to all compromised machines connected to the channel at once. They

became bots within the botnet. The person issuing the commands is also connected to the channel and often called a bot herder. The server and the channel the bot connected to are often called Command and Control (C&C) server respectively channel.

All sorts of commands can be given to the compromised hosts like updating the malware, opening a proxy port to send out spam, stealing personal information from the users of the compromised system or attacking a site with a distributed denial of service attack (DDoS).

If the control channel is blocked or the control server is taken down, there are most often additional control channels included in the bot. These will be used if a certain error condition is met and a time out occurs - e.g. the name 'x4711.evil-bot.net' not being resolved any more or pointing to 127.0.0.1 for more than 48 hours.

Some botnets employ control channels, which emulate licit traffic very well - e.g. communicating by DNS response packets. And sometimes the botnet is not structured in a more complex topology - e.g. a loosely connected peer to peer network instead of strictly centralised network. These mechanisms make the detection of the control channels and the single bots a lot more difficult and will provide a challenge for the future.

- Requirements derived from the example

Botnets are known to grow up to several hundred thousand hosts and there are probably at any time several million hosts under control of attackers. It is important for the internet community to understand the workings of botnets and find effective ways of removing control over a botnet from the attacker.

One important step is gaining knowledge about the different control channels available to the bot. In the controlled environment of a high interaction honeypot, unusual control channels can be found, too, which is increasingly important.

This can only be done if the malware is to be allowed to execute and also possibly to load additional code from an external address. It is certainly not wanted that the botnet controller is able to give commands to the bot e.g. to attack a certain site or to send out spam. The distinction

between necessary actions for the bot to connect to his C&C and the control connection itself can be difficult, but represents a necessary risk.

A further requirement is the automatic classification of malware in order to avoid wasting energy on already known malware. One has to take into account, that the malware might be functional identical to previously found and analysed malware, but is not binary identical. Advanced methods of recognition of malware have to be applied. The derivation of a similarity to other known malware will also be useful in order to minimize the overhead for malware analysis.

A high interaction honeypot allows collecting information about incidents, software and mechanisms used by the attackers in a controlled manner without exposing a high risk to the deploying site.

7. Analysis of related projects

The NoAH project will perform the technical preparatory work towards the implementation of a European Infrastructure of Advanced Honeypots. The Infrastructure will consist of a Network of Honeypots that will be able to collaborate towards studying, identifying, and responding to cyber-attacks, including both those attacks that were previously encountered, as well as new types of attacks. This infrastructure will provide a wealth of information about the way attackers operate within the Internet. Such information can be used by a wide variety of stakeholders including security administrators, security researchers, Incident Response Teams[1], the European Network and Information Security Agency, National CyberSecurity Agencies, and many more in order to be able to defend the Internet in the most effective way.

All members of NoAH have different experiences and different possibilities concerning hardware resources, time and number of staff members, etc. For the cooperation of the NoAH partners as well as external partners, it is necessary to determine rules for implementation, communication, data handling, information exchange and legal aspects of such a widespread security infrastructure. These rules will be defined as some sort of policy, augmented by set of procedures and tools implementing what was defined by the policy. The policy will at the same time provide all present and future members with necessary information about the participation with all its rights and duties. Especially the data which will be collected requires a clear statement within the policy regarding:

- anonymization / pseudonymization
- privacy
- legal issues

The following sections provide a short overview on some policies of other related projects in order to analyze, what we can learn from established practices. It is followed by a list of requirements and suggestions for a minimal NoAH policy concerning the technical, organizational and legal aspects that need to be considered for any practical setup.

[1]Also known as CERT (Computer Emergency Response Teams) or CSIRT (Computer Security Incident Response Team)

The following projects deal with similar to NoAH issues, for example setting up a network of Intrusion Detection Sensors or honeypots across Europe and providing statistics (eCSIRT and Leurre.com), analysing new types of attacks in-detail (honeynet.org) and exchanging sensitive information (nsp-security).

After a short summary of the projects this section takes a look at their policies specifically in order to understand, how they might contribute to a NoAH requirements analysis and policy statement.

7.1 eCSIRT.net

Between July 2002 and December 2003 a number of established CSIRTs (Computer Security Emergency Response Teams) from the European CSIRT community received funding through the 5th Framework to run a trial project. This project was called eCSIRT.net and focused on the deployment of new techniques and practices that would satisfy the basic and existential need of incident response teams (CERTs or CSIRTs) to much more efficiently cooperate and exchange incident related data, and to collect shared data for statistical and knowledge-base purposes. Part of the project was devoted to set up a network of IDS sensors across Europe and collect the data about attacks for further analysis.

After the project ended, some teams decided to continue the established sensor network across Europe, which provides data since September 2003.

The co-operation of the volunteering teams providing the infrastructure support as well as the teams supporting the network by running IDS sensors in their area of interest is still based on the same policy and procedural framework, protecting the interest of all participating teams.

eCSIRT.net
Anonymous statistical data which results from the IDS are presented on a public web server. In addition, more detailed data is presented on a private part of the web server which can only be accessed be the eCSIRT partners. Copyright-issues, data protection and guidelines for participation are declared as followed: Copyright: All documents and other material on this web server are protected by German and foreign laws. Permission for any reproduction must be required unless permission is granted explicitly on this page (read below). Permission to Use: Permission is granted for internal and non-commercial use: • to reproduce the graphics and documents of the eCSIRT Sensor Network data as obtainable through this public web site and • to prepare derivative works from these • provided the URL https://www.ecsirt.net, the disclaimer and the copyright notice are included with **all** reproductions and derivative works Permission is granted for external and non-commercial use: • to reproduce the graphics and documents of the eCSIRT Sensor Network data as obtainable through this public web site and • to prepare derivative works from these • provided the URL https://www.ecsirt.net, the disclaimer and the copyright notice are included with **all** reproductions and derivative works It is recommended that graphics for reproduction on other web sites are not copied but included as links to the eCSIRT.net web page. It is also recommended that you provide us a short information about reproductions and derivative works by sending email to info@ecsirt.net.

eCSIRT.net

Guidelines for participation:

The co-operation is determined by the following guidelines:

- The co-operation is voluntary and can be terminated at any time.
- Co-operation within the project will not infringe on partners business.
- Information and intellectual property rights of all partners must be protected.
- The confidentiality of constituent data will be given highest priority.
- Services provided by the partners should steadily improve.
- Policies, procedures and workflows of all partners should be optimized by the exchange of knowledge and practice within the partner community.
- The partners will develop and enable means for an improved exchange of knowledge and practices and will provide training material.
- The work and co-operation of partners should set an example for other CSIRTs and should provide a model for similar initiatives around the world.

The eCSIRT.net initiative is open for participation by all European teams that have been shown to follow established best practices by joining the TI accreditation framework[2]. Teams outside Europe are welcome to liaise with eCSIRT.net and participate in discussions to progress the goals described above, so they can be implemented internationally. This will also progress the methods and practices developed so they can be utilized and applied in other settings.
(Accepted by the eCSIRT.net partners on 9 December 2002 in Amersfoort, The Netherlands)[3].

The scope of the eCSIRT.net policy is quiet similar to what to be envisioned for NoAH. This is not surprising as it was as well a collaborative effort with some of the results being made available for

[2] http://www.trusted-introducer.org
[3] http://www.ecsirt.net

public consumption. Therefore the overall situation and the role of the policy was comparable. Nevertheless some of this policy rather provides some code of conduct, again not surprising as the code of conduct of the German CERT Community was used in preparation of the eCSIRT.net policy. Overall some statements can easily be adopted, while others not.

7.2 The Honeynet Project

The Honeynet Project is a non-profit organization dedicated to improve the security of the Internet by providing cutting-edge research for free. Founded in October, 1999 they have been providing the following services for free to the public:

- **Raise Awareness**

  One of the goals is to raise awareness of the threats and vulnerabilities that exist in the Internet today. Many individuals and organizations do not realize they are a target, nor understand who is attacking them, how, or why. The Project members provide this information so people can better understand they are a target, and understand the basic measures they can take to mitigate these threats. This information is provided through a series of papers called „Know Your Enemy“.

- **Teach and Inform**

  For those who are already aware and concerned, they provide details to better secure and defend resources. Historically, information about attackers has been limited to the tools they use. The Honeynet Project provides critical additional information, such as their motives in attacking, how they communicate, when they attack systems and their actions after compromising a system. This service is provided through the „Know Your Enemy“ whitepapers and the „Scan of the Month“ challenges.

- **Research**

  For organizations interested in continuing their own research about cyber threats, the Honeynet Project provides the tools and techniques they have developed.[4]

[4] http://www.honeynet.org and http://www.honeynet.org/tools/index.html

Honeynet Project

The Honeynet Project gives detailed information about handling the data collected by the honeypots concerning data control, data capture and data collection:

I. Data Control:

Once a honeypot within the honeynet is compromised, we have to contain the activity and ensure the honeypots are not used to harm non honeynet systems. There must be some means of controlling how traffic can flow in and out of the honeynet, without attackers detecting control activities. Data Control always takes priority over Data Capture.

II. Data Capture:

Capture all activity within the honeynet and the information that enters and leaves the honeynet, without attackers knowing they are being watched.

III. Data Collection

If the honeynet is part of a distributed environment, then that Honeynet must meet the third requirement of Data Collection. Once data is captured, it is securely forwarded to a centralized data collection point. This allows data captured from numerous honeynet sensors to be centrally collected for analysis and archiving.

REQUIREMENTS:

I. Data Control

This defines the specific requirements for data control:

a) Must have both automated and manual Data Control. In other words, Data Control can be implemented via an automated response or manual intervention.
b) At least two layers of data control to protect against failure.
c) Data Control failures should not leave the system in an open state. In case all layers of Data Control fail, the system should automatically prevent all accesses to and from the honeypot.
d) Be able to maintain state of all inbound and outbound connections.
e) Data Control enforcement must be must be configurable by the administrator at any time, including remote adminstration.
f) Control connections in a manner as difficult as possible to be detected by attackers.
g) Automated alerting of when honeypots are compromised.

Honeynet Project

II. Data Capture

This defines the specific requirements for data capture.

a) No honeynet captured data will be stored locally on the honeypot. Honeynet captured data is any logging or information capture that is not standard to the honeypots within the honeynet.
b) Data pollution can contaminate the Honeynet, invalidating data capture. Data pollution is any activity that is non-standard to the environment. An example would be an admin, testing a tool by attacking a honeypot.
c) The following activity must be captured and archived for one year.
    - Inbound/Outbound connections (firewall logs)
    - Network activity (full packet captures)
    - System activity
d) The ability to remotely view this activity in real time.
e) The automated archiving of this data for future analysis.
f) Maintain a standardized log of every honeypot deployed.
g) Refer to Appendix A (Honeypot Deployment) for template.
h) Maintain a standardized, detailed write-up of every honeypot compromised. Refer to Appendix B (Honeypot Compromise) for template.
i) Honeynet gateways' data capture must use the UCT time zone. Individual honeypots may use local time zones, but data will have to be later converted to UCT for analysis purposes.
j) Resources used to capture data must be secured against compromise to protect the integrity of the data.

III. Data Collection

If the Honeynet is to be part of a distributed network, then the following requirements must be met.

a) Honeynet naming convention and mapping so that the type of site and a unique identifier is maintained for each honeynet.
b) A means for transmitting this captured data from sensors to the collector in a secure fashion, ensuring the confidentiality, integrity and authenticity of the data.
c) Organizations have the option of anonymizing the data. This does not mean to anonymize the data of the attacker, rather it gives the source organization the option of anonymizing their source IP addresses or other information they feel is confidential to their

Honeynet Project
organization. d) Distributed honeynets are expected to standardize on NTP, ensuring all honeynet data capture is properly synched.

The policy statement for the Honeynet Project is not really a policy as many statements are technical in nature and are used more to describe standard procedures. They are definitely much more detailed then necessary for a policy. Not much of the policy can therefore be retrieved for the NoAH policy. However, the technical constraints can be adopted to the high-interaction components of the NoAH architecture.

7.3 Leurre.com

The LEURRE.COM project is an international project that operates a broad network of honeypots covering more than 20 countries and the 4 continents. Primary aim of the project is to gather data that allows to better understand the current malicious activity. Therefore, the aim of the project and the technical realisation is very similar in comparison with the eCSIRT project. As a consequence, the project does not focus on the in-detail analysis of attacks which is e.g. in contrast to the honeynet project. Anonymous statistical data is presented on a public web-server.

The project has triggered interest from many organizations (academic, industrial and governmental). A specific web interface has been built to help partners finding relevant information on the attacks they are facing.

LEURRE.COM
Public Data can be found on the Leurre.com Website[5]. You can find statistics of four different timeslots (day, week, month, semester) about the most attacking domains, most attacking countries, most attacked port sequences and most attacking clusters. The contract to become a member of LEURRE is very simple: Partners sign a non-disclosure agreement (NDA) and accept to install one platform. On the other side, they get access to the whole database and all the enriched information.

[5] http://www.leurre.com

The public policy statement for LEURRE.COM is very short covering only two issues of interest: What is provided? and How to become a member? However, a private NDA exist concerning the ownership, use and sharing of the captured data and concerning the information about the honeypot network that is likely relevant for the NoAH project.

7.4 NSP-SEC Forum and Mailing list

The nsp-security [NSP-SEC] forum is a volunteer incident response mailing list, which coordinates the interaction between ISPs and NSPs in near real-time and tracks exploits and compromised systems as well as mitigates the effects of those exploits on ISP networks. The list has the goal to help mitigate attacks.

NSP-SEC
NSP-SEC is a forum to get work done in the service of the community, so a person/ organization has to fulfil some expectations. These expectations are periodically reviewed by the NSP-SEC moderators to ensure that an individual's community membership is relevant, productive, and adds value to the mission of NSP-SEC. These expectations, which have evolved through active membership feedback include: • All posts to NSP-SEC must have an organizational affiliation via either a corporate email address that is identifiable as an ISP/NSP, or via a signature that includes an organizational affiliation. • Lurking and learning does not contribute to the community, there are other forums for that. Silence often indicates that people are not handling the information provided by the NSP-SEC community or that the information provided is of little relevance to the member. Acknowledgments of action (whether publicly on the mailing list or privately to the people involved) provides members of the community an indication that contributions are being made. Recognizing specific national laws, regulations, and/or corporate policies may prevent some members from posting on the public NSP-SEC alias; these limitations do not prevent private mitigation correspondence. • Taking information provided on the NSP-SEC forums and using it for commercial gain is not allowed. It is a violation of trust to the community.

NSP-SEC
• NSP-SEC's consultation on procedures, policies, tools, mitigation techniques, and other proactive activities take place on the discussion alias „NSP-SEC-DISCUSS“. It is natural online human behavior to digress into a dialog. This is encouraged and discussions of this nature are expected to move from NSP-SEC to NSP-SEC-DISCUSS. • NSP-SEC is built on trust. Therefore, reposting NSP-SEC communications to individuals inside or outside your organization is a violation of that trust. NSP-SEC members should have the span of control to take action on the information from an NSP-SEC correspondence without widely posting the information inside their organization. If forwarding inside the organization is required, permission of the posters must be sought. • NSP-SEC postings must not be CCed or BCCed to any other forum. Internal dialog must be re-crafted for internal use as mentioned in previous guidelines. • Membership in NSP-SEC is restricted to those actively involved in the mitigation of NSP security incidents within organizations in the IP transit, content, and service provider community. Therefore, it will be limited to operators, vendors, researchers, and people in the FIRST community working to stop NSP security incidents. That means no press and (hopefully) none of the "bad guys." • NSP-SEC will use a simple trust/peering relationship. This model is not as "secure" as an encrypted conversation, yet it is better than a wide-open public dialog. All applications must be accompanied by at least two existing members who will „vouch“ for the new applicant. Members of the list are asked to vouch for new subscriber requests. If the list administrators know the person, then they can vouch for them. No information presented in this list is allowed to be forwarded or shared outside the NSP-SEC community without specific permission from the poster. It is expected that members strictly adhere to this policy to ensure list confidentiality.

While the policy is very specific on some procedural aspects, it does not address a wide range of aspects to be expected in a well balanced policy. Given the strict focus of NSP-SEC and the closed community that has established a minimal policy only, this does not pose

a problem in their community. But due to this reason not much input for the NoAH policy can be derived from it.

7.5 A policy dimension for a honeypot infrastructure

If we look through the different policy statements from other relevant projects like we did in a previous sections it is obvious, that the various requirements fall into one of three main categories:

- **Technical Aspects**
  Describing in technical terms what is done and in some cases how it is done.
- **Organizational Aspects**
  Describing aspects which cannot be realized by technical means or that are directed towards the human users that are dealing with the information on a non-technical level.
- **Legal Aspects**
  As there are legal considerations that are enforced by the legal rules applicable for all parties involved, it is mandatory to cover these as well. Of overriding importance is the question how cross-border issues are addressed (components of NoAH will be operated in more then one country).

We will review each of these categories in more detail, especially concentrating on the main questions and provide first recommendations for a "NoAH Policy" which shall help to lead the further discussion esteaming from this report.

While trying to develop suitable policy statements it became obvious that some level of (mostly technical) details are yet unknown. Therefore, the final policy cannot be specified unless these details are known. However, in appendix A1 there is a first draft proposal for a NoAH policy document. This draft provides a list of building blocks that can be used as a starting point for defining an acceptable NoAH policy.

Technical Aspects

a) Which types of data are covered by the policy?

Actually it would be nice to explain in detail the data that is collected by the NoAH infrastructure. But this is neither practical – too

many changes – nor desired – providing hints to the "bad guys." But it is highly recommended to explain on a high level what kind of data is collected and how this data is categorized in terms that can be applied later in the policy to differentiate the various requirements to specific subsets of all the data only.

b) Which protection of NoAH partner interests is supported by the policy?

All data that points to one system of any NoAH partner might already be enough to be shared with others on a potential global scale. Therefore appropriate technical solutions to hide the identity of the systems involved needs to be utilized. The decision, what data to protect can only be made by the specific NoAH partner itself, as this decision needs to be based (and implement) the organizational policies that are applicable.

While technical anonymization and pseudonymization will solve the underlying problem – hiding once addresses – anonymization will not be considered for NoAH as it destroys the relationship among independent data entries that are routinely correlated based on the addresses. Therefore the use of pseudonymization is available that at least ensures the correlation of all data of any particular NoAH partner. The correlation between data of different NoAH partners will not be possible any longer, as this would enable any NoAH partner to look up in some sort of dictionary attack the address space of all other partners.

As the further analysis might be impacted by the pseudonymization, clear indication prior to the submission of any data is mandatory in all cases.

c) How long will the data be stored?

There must be a limit until the data collected and processed are actually stored according to good privacy rules. As the data collected is useful for research projects further on there is a conflict of interest. Even if the data pinpoints the source of attacks, this source can be a legitimate organization which has been victim of another attack earlier on – and such victims needs to be protected as well.

d) What services are provided?

Certainly there might be more services over time, but for now only processed summaries that are made available on a public web page are envisioned as public service.

Organizational Aspects

From the organizational point of view some questions also needs to be answered. These are especially related to the public visible interactions with NoAH and access to NoAH itself.

e) How to become a NoAH partner?

Organizations might wish to join NoAH and needs to understand the requirements they need to full fill in order to get access.

f) What rights does a NoAH partner have?

As soon as an organization has joined NoAH, they will have equal rights. These rights need to be communicated clearly to the public as well.

g) How does NoAH address its overall responsibilities?

As the NoAH partners have access to a wide range of information and as the components used for the purpose of NoAH itself might be targets of attacks some governing rules needs to be established defining the responsibilities that might drive decisions in specific severe situations.

Legal Aspects

This analysis will be important for creating the final policy, taking into consideration the international scope of the project, legal compliance might be difficult to achieve in some areas. Especially privacy will be an important issue.

h) What rules are enforced regarding the Copyright?

The use of the results of the data processing is much related to the public services and certainly to the desired integration by the NoAH partners as well. To be most flexible, any reproduction outside the scope of the policy is prohibited.

i) What permissions are granted?

More specifically as the copyright the permissions given to other parties must be defined in accordance with the desired outcome. As always this statement will list the rights of others and define any other requirement that needs to be fulfilled in order to have legitimate rights.

8. Conclusions

Along with the existence of the questionnaire, there was a discussion both via email and teleconference, about the objectives that NoAH project should focus on. All the partners had the opportunity to state their opinion on what should be the focus of NoAH project.

The following overall conclusions can be drawn both from the received responses on the questionnaire and from the discussion between consortium members, as well as on the survey on projects related to NoAH:

- NoAH's platform should be easy to install, configure and update. The installation and configuration process should be as self – explanatory and easy to follow by anyone. Expansions of the infrastructure with new features at low cost must be predicted.

- NoAH's honeypots may be implemented to support various operating systems. This variety of operating systems should not cause any malfunction to the honeypot infrastructure.

- The administrator of a honeypot should be able to define the level of interaction for the specific honeypot, as well as its security level.

- NoAH's honeypots should not interfere with the organization's network resources and should not in any case affect their network's bandwidth and introduce extra unnecessary traffic.

  They should also not attack to other honeypots or cause any malfunction to other network facilities within an organization or to an outsider. However they should be easy to install/disconnect to one's network (portability).

- In case of a hardware malfunction on the honeypot's resources, the honeypot should be isolated so as not to produce any kind of problem to the network that it is connected to.

- NoAH's infrastructure should be able to detect various kinds of attacks, such as virus/worms spread, intrusions attempts, bots attacks, etc. It should also be able to recognize new threats at the beginning of their spread, such as polymorphic and metamorphic virus, or new critical vulnerabilities that come up, for various resources.

- The reaction of NoAH's infrastructure in case of an attack detected should be quick and accurate. The number of false positives should be minimized, if not zeroed, in order the system to be trust-worthy.

- Honeypots may need to communicate with each other in order to produce valid alerts quickly and to reduce false positives at minimum.

- NoAH's infrastructure should produce well formatted signatures that are clear to various recipients (network technicians / administrators).

- Information that should provide is: IP/DNS of the attacker, geographical information about them, information on the methods used by the attacker and the kind of the application/service exploited by the attacker.

- Once an attack has been detected, NoAH should send an inform alert on the specific attack. Also, a web site with information about those attacks should be developed. A mailing list might need to be developed, as well. Other potential actions that can be taken by the infrastructure should be described by a NoAH's policy.

- A policy for the co-operation between NoAH and external partners should be clarified (requirements for becoming a partner, the rights/obligations for each partner), as well as for the actions that should be taken in case of misuse or abuse of the infrastructure by any NoAH partner.

- A policy for the usage of the produced data should be clarified. A policy should also exist concerning the data that every

participating organization that hosts a honeypot can provide and can have access to.

- A policy for the data export of the honeypot nodes should exist, defining which data can be export from the nodes and the various protection options for it.

- The NoAH infrastructure should take into account issues about data logging/user's privacy. Logging is risky with various data protection acts in different constituencies. It's extremely dangerous for any third parties to retain this data without tight restrictions on use and access.

- NoAH's honeypots should not reveal themselves to the attackers. Mechanisms should exist for self-protection of a honeypot in case an intruder understands a honeypot.

- In case attackers realize that they are in a honeypot, it should become difficult or even impossible for them to take over and control the honeypot.

9. Appendix

A1. Building blocks for the draft NoAH Policy

In appendix A1, a list of building blocks is presented which is intended as a first proposal for a NoAH policy. Each building block corresponds to a requirement as described in section 7.5 a) to i). Since the policy is closely related to details which are not completely known at this state of the project, the building blocks have to be adopted to the final policy and are very likely to change.

NoAH Policy Proposal
Provide a detailed description of what the NoAH project is all about. It should be accurate and careful enough to provide a well-defined overview of the service that is provided.
Example: NoAH is a three-year project to gather and analyse information about the nature of Internet cyberattacks. It will also develop an infrastructure to detect and provide early warning of such attacks, so that appropriate countermeasures may be taken to combat them.
Describe the context and scope of this policy (with respect to participation and data sharing) establish the right to review the policy:
Example: To communicate on the established policies governing the NoAH infrastructure as well as the data collected and the information provided to others, this policy was developed. This policy defines expectations both in regard to the NoAH infrastructure and its service to the community and the NoAH partners, but also towards the NoAH partners themselves, that are participating in this effort. This policy statement as the expectations defined within will be periodically reviewed by the NoAH partners to ensure that it is relevant and appropriate as defined by the mission of the NoAH infrastructure.

NoAH Policy Proposal
Distinguish between different types of data that might be governed by different usage and sharing rules: Example: All data which is collected by the NoAH infrastructure is covered by this policy, to which the NoAH partners adhere. Specific subsets of data might be handled differently from the whole set or other subsets as defined by this policy. For the purpose of the NoAH infrastructure the following subsets are defined: • Public data – this data is designated for public consumption, for example for graphical visualization on a public web server informing about NoAH. This includes aggregated statistics and data that is deemed by NoAH to be consistent with privacy rules and regulations. • Private data – this data is designated for consumption by NoAH partners only. No publication of this data or work derived from this data revealing the identity of any NoAH partner or its systems is allowed. • Data governed by special rules – special cases can be established in an ad-hoc manner by NoAH partners and are subject to opt-in participation by other participants.
Establish non-disclosure rules about auxiliary data besides the data generated by the NoAH infrastructure itself: Example: In addition other types of information are handled and covered by this policy, most notably the following: • Data about NoAH partners including the position of any NoAH device operated on the partner site – this data belongs to the individual NoAH partner and is not designated for publication or use outside the scope of NoAH. Each NoAH partner might decide, which data about himself as well as NoAH components under his administrative control, is published and where. • Data about NoAH infrastructure including all components not designated to be part of the local infrastructure of a NoAH partner – this data does not belong to any specific NoAH partner and is not designated for publication without consent by the NoAH partners. While the NoAH partners agree on making information as widely available as possible, sensitive as well as critical details especially addressing operational concerns must be protected.

NoAH Policy Proposal
Provide details on the types of post processing to be performed and data retention limits to be established for ensuring privacy, especially with respect to public data Example: To protect their interests NoAH partners might choose to submit data only in a pseudonymized format not revealing the destination addresses that are pointing to own systems. This might include searching and replacing for host names and domain names inside any payload as well. Any partner that wishes to use pseudonymization must clearly indicate this and use methods that have been agreed upon by all NoAH partners to ensure compatibility and interoperability. All NoAH partners will accept the agreed upon name space to avoid overlaps in the address spaced used, as this otherwise might impact the quality or correctness of any further analysis taken out on the available data. All data collected and processed by NoAH will be stored up to a maximum of 14 days without further measures. After that period all data will be used only for further research, with identifying data pseudonymized to protect parties involved and found in the original data.

NoAH Policy Proposal

Establish common rules of participation and mutual trust

Example:
To become a NoAH partner an organization needs to fulfil the following requirements:

- Report regularly (at least biannually) about the results of running the service
- Provide a technical support contact for coordinating the operation of the NoAH system(s) and resolving technical problems.

Any organization that has fulfilled the requirements above needs to accept the following code of conduct and present a membership application to the NoAH partners. Only then the NoAH partners will decide on the membership application and inform the applying organization appropriately. There is no legal right to become a NoAH partner for anybody.
The code of conduct comprises the following rules:

- The co-operation is voluntary and can be terminated at any time by any NoAH partner.
- Co-operation within the project will not infringe on partners business.
- Information and intellectual property rights of all partners must be protected.
- Services provided by the partners should steadily improve.
- Policies, procedures and work flows of all partners should be optimized by the exchange of knowledge and practice within the partner community.
- The partners will develop and enable means for an improved exchange of knowledge and practices.
- Misuse or abuse can give reason to exclude any NoAH partner by decision of the other partners at any time.

Explicitly establish the rights of NoAH partners, once the membership application has been accepted

Example:
After the membership application was accepted, the NoAH partners have the following rights:

- To decide about future membership applications
- To have access to the reports of all NoAH partners
- To have access to the internal communication infrastructure
- To have access to the internal databases through the established interfaces
- To make use of the internal available information for internal purposes
- To make use of the public available information for all purposes
- To been listed – or not – on the NoAH public web site

NoAH Policy Proposal
Explicitly list the responsibilities of the NoAH partners with respect to security incidents, including those affecting the NoAH infrastructure Example: As the NoAH partners are responsible users of the Internet and recognize their unique position in regard to having access to real life information they agree to: • Inform other entities, most notably CERTs, if data suggest a new threat or widespread attacks that have the potential to threaten the Internet or large parts of this infrastructure • Mitigate any compromise of the NoAH infrastructure to avoid damages caused by wrong or falsified data • Keep a high level of IT security in regard to the NoAH infrastructure

NoAH Policy Proposal

Copyright:

Example:

All documents and other material publicly available from the NoAH infrastructure are protected by national laws. Permission for any reproduction must be required unless permission is granted explicitly in this policy statement.

Permission to Use:

Example**:**

Permission is granted to any none NoAH partner for any non-commercial use:

- to reproduce the graphics and documents of the public NoAH data as obtainable through this public web site and
- to prepare derivative works from these
- provided the URL http://www.fp6-noah.org/ the disclaimer and the copyright notice are included with **all** reproductions and derivative works

It is recommended that graphics for reproduction on other web sites are not copied but included as links to the specific web page.
It is also recommended that you provide us a short information about reproductions and derivative works by sending email to pr@fp6-noah.org

Permission is granted to any NoAH partner for any other use in accordance with this policy.

A2. NoAH Questionnaire

PART A - General organization information

This part contains questions relevant to your organization.

1. Organization/company

2. What category best describes your organization?

Please choose **only one** of the following:

- NREN
- ISP
- Security firm
- Research/Education
- Government
- Commercial
- Other

3. Interviewed person contact details

Please write your answer(s) here:

- Name:
- Address:
- Email:

4. Other information

PART B - Organization Infrastructure

This part contains questions relevant to your organization infrastructure.

1. Number of hosts of your organization

Please choose **only one** of the following:
- 1-10
- 11-20
- 21-50
- >50
- Other

2. Internal Organization's network

Please choose **all** that apply
- LAN

- MAN
- WAN
- Other

3. Operating system(s) used within your organization

Please choose all that apply and provide a comment
- Unix
- Linux
- MS Windows
- Other

4. Does your organization have a security department/NOC?

Please choose **only one** of the following
- Yes
- No

5. Other information

PART C - Monitoring issues

This section contains questions to investigate the state of the art about system security monitoring and cyber threats.

1. How important is system monitoring for your organization?

Please choose **only one** of the following:
- Not so important
- Important
- Very important
- Crucial

2. Security/monitoring mechanisms/tools currently used by your organization

Please choose all that apply and provide a comment

- Firewalls
- Antivirus
- Passive Network Monitoring Tools
- Active Network Monitoring Tools
- Honeypots
- Other

3. What kind of attacks against your infrastructure do you usually detect?
Please choose **all** that apply

- Virus/Worms
- DDoS
- Intrusion attacks

- Sniffing network traffic
- Spamming
- Other

4. What kind of services do you usually operate within your organization?

Please choose all that apply and provide a comment

- peer-to-peer applications
- FTP services
- SNMP services
- ssh / Telnet
- E-mail services
- WWW services
- DNS
- ERP
- CRM
- Other

5. System monitoring objectives
Please choose all that apply
- Intrusion detection
- Debugging performance problems
- Failure diagnostic
- Other

6. NoAH will contribute towards building an early warning system to alert organizations of cyberattacks spreading on the Internet. What would you consider as satisfying response time for such a system?

Please choose **only one** of the following:
- <10 minutes
- 10 - 30 minutes
- >30 minutes
- Other

7. Potential recipients of the security monitoring data in your organization

Please choose **all** that apply
- Network engineer
- Network operator/administrator
- System administrator
- Corporate Manager
- Other

8. How many honeypots do you think are necessary in order to produce a valid alert on a potential attack?

Please choose **only one** of the following:
- 1-5 honeypots

- 6-10 honeypots
- 11-20 honeypots
- >20 honeypots
- Other

9. Other information

PART D - NoAH Operation

This part contains questions to investigate the desired operation of NoAH infrastructure.

1. What purposes, do you think, the data provided by an early warning detection system like NoAH, should be used for?

Please choose **all** that apply
- Education
- Research
- Commercial
- Other

2. What actions, do you think, should be taken by NoAH in case of a detected attack?

Please choose **all** that apply
- Log all Internet traffic
- Alert all project participants immediately
- Provide guidelines/hints in order to face the attack
- Other

3. Have you ever used, or are you currently using honeypots?

Please choose **only one** of the following:
- Yes
- No

3.1. What was the level of interaction?

Please choose **only one** of the following:
- High
- Medium
- Low

3.2. Which of the following have you used?

Please choose **only one** of the following:
- Honeynet
- ECSIRT
- DeepSight
- Other

4. Would you agree to have a honeypot in your organization?

Please choose **only one** of the following:
- Yes
- No

4.1. Which are the reasons?
Please choose **only one** of the following:
- it is too expensive
- I do not trust them
- I do not need one
- I do not know anything about honeypots
- I do not know how to use one
- I do not know what to do with the information from a honeypot
- Other

4.2. Which of the following would possibly convince you to use a honeypot ?

Please choose **only one** of the following:
- provision of honeypot equipment
- get some training
- change of legal framework
- Other

5. If you installed NoAH honeypots in your organization, who would you like to be responsible for their installation / configuration in your organization?
Please choose **all** that apply
- Your organization
- Remote installation / configuration
- Central help-desk for installation / configuration
- Other

6. If you installed NoAH honeypots in your organization, who do you think should maintain and manage them within your organization?

Please choose **all** that apply
- Your organization
- Independent consortium
- Other

7. If you installed a honeypot in your organization would you be willing to share (give/receive) any attack information (alerts/signatures, etc) with other organizations?

Please choose **only one** of the following:
- Yes
- No

7.1. Are there any specific conditions for changing your mind.

Please choose **only one** of the following:
- anonymized data
- only alerts

8. Other Information

PART E - Cooperation with NoAH

This section contains questions to investigate the output that NoAH's users would prefer.

1. Interest for cooperation with early warning systems, like NoAH, for various kinds of attacks

Please choose the appropriate response for each item

- DDoS attacks	1	2	3	4	5
- Virus/Worms	1	2	3	4	5
- Intrusion attacks	1	2	3	4	5
- Spamming	1	2	3	4	5
- Sniffing traffic	1	2	3	4	5

2. What information about the attack would you consider as helpful?

Please choose **all** that apply
- Type of attack(virus,worm,intrusion,etc)
- Attacker's sophistication (low,middle,high)
- Attack signature
- Methods used by the attacker
- Tools used by the attacker
- Other

3. What would you like to know about the attack's origin?

Please choose **all** that apply
- IP/DNS address
- Geographical information
- Other

4. What kind of alert would you prefer in case of a detected attack?

Please choose **all** that apply
- Email alert
- SMS alert
- Web site update
- Logging
- Other

5. What kind of attack signatures will be of use to you?

Please choose **all** that apply
- IP packet-based

- composed of a series of system calls
- None
- Other

6. What would you consider as tolerated rate of false positives?

Please choose **only one** of the following:
- 0-2 false positives per day
- 3-5 false positives per day
- 6-10 false positives per day
- >10 false positives per day
- Other

7. Are you interested in cooperating with NoAH in the future ?

Please choose **only one** of the following:
- Yes
- No

8. Other Information