‘THE PSG VISION FOR ENISA’

Permanent Stakeholders Group (PSG)

Rapporteur: Urho Ilmonen
Co-editors: Paul Dorey and Simon Perry

Adopted version
May 2006

1. Contents

2. Executive Summary

ENISA position in 2008

ENISA should be one of the highly respected European centres of excellence in Network and Information Security, and a trusted expert body whose opinion is sought in key projects of both the public and private sectors.

ENISA should be the recognized spokesperson of European NIS interests in global cooperation, seeking to develop necessary relationships to forward European interests, with a clearly defined role relative to the Commission and individual Member States

ENISA should be the advanced driving force behind the creation, development and dissemination of trusted, secure Information Security technology; thus enabling the consumers in both the public and private sectors to use digital technology without undue security risks.

ENISA should be a recognized consultation centre for the European Union bodies and Member States as well as other international standardization and legislative bodies

ENISA should not:

- redo work done elsewhere,
- compete with commercial organizations,
- stay only at the "best practices" level, but instead have a holistic vision which can be worked towards, and for which the best practices becomes only a stepping stone.

Target deliverables for 2008

The following are the target deliverables that ENISA should work towards for delivery by the end of 2008. This list is indicative only as there may be other important work items not yet listed here.

- ✓ Create a roundtable forum for the NIS stakeholders to discuss and agree on solutions to the recognized threats in this Vision
- ✓ Publish an annual NIS status report free of commercial and political ties
- ✓ Publish an annual or quarterly "Internet Insecurity Index" to monitor development and report progress in NIS. (ENISA should handle such a tool with special care and perform a proper study of the political implications of the index, especially when it comes to required action in case of fault or mistakes).
- ✓ Be a co-promoter of very high-level NIS conferences to forward the development of "NIS without frontiers". ENISA should not produce such conferences itself, but instead select 1-2 annual conferences and co-promote them with publicity and high-level contributions.
- ✓ Select and promote clear and practical end-user guidance material for NIS. ENISA should not draft or produce such material but support existing work.
- ✓ Drive security awareness to all EU citizens. Consumers and end users all have to cope with securing more devices, updating their systems to ensure they are protected - and many have a limited awareness of what security really is, why it

matters, and how to know if they have a problem. By 2008 part of the vision of ENISA should be that every European citizen understand the benefits of information security, and understand how they need it to operate as electronic citizens in the 21st century

3. Introduction

This report has been collectively produced by the members of the Permanent Stakeholders Group (PSG) that has been established by European Network and Information Security Agency (ENISA). The objective of this report is to present the PSG members' collective Vision on the mid-term evolution of security issues from both a technical and non-technical perspective. This report also presents the Stakeholders view of the role envisaged for ENISA in answer to the foreseen security issues.

It is the intention that this report serves as input from the Stakeholders to ENISA towards the establishment of its long term vision and mission statements, in order to contribute towards the development of a culture of network and information security.

PSG Role and Composition

The Permanent Stakeholders' Group (PSG) has clearly defined roles:

- to advise the ENISA's Executive Director in the performance of his/her duties on scientific matters,
- to provide input in drawing up a proposal for the ENISA's annual Work Programme,
- to be a constantly open communication link between ENISA to the rest of the network and information security stakeholders community, and
- to advise ENISA on setting up of new ad-hoc Working Groups, purpose of which are to address specific technical and scientific matters.

The PSG is set up under the responsibility of the ENISA Executive Director and is composed of 30 leading experts (see Annex A) representing the relevant users and suppliers from the Information and Communication Technologies industry, consumers and academia. The PSG members are nominated for a two and a half-year term.

4. Current and Foreseen Security Issues

In this section we elaborate on issues related to network and information security both those which are currently visible, as well as those which are more likely to be the centre of focus during the coming years. The purpose of this section is not to be exhaustive but to provide indicative insight on potential threats based on the current knowledge, trends and predictions.

Focus will not only be on technology-related issues, such as malware, but also on security issues that arise from human-related factors, such as lack of security awareness.

4.1 Technology-related Risks and Threats

In this section we will discuss current and emerging threats and risks which are related to information and communication technology (ICT) that currently in use and is expected to grow in the future. Our discussion includes various forms of malware (such as worms, rootkits, and botnets), identity theft, such as phishing attacks, security issues related to wireless, mobile and peer-to-peer networks, spam and denial of service attacks.

4.1.1 Various forms of malware

Malware is a general term that is used to denote any kind of malicious software. More and more sophisticated malware and spyware is going to be widely available for free on the internet, making it possible for large numbers of amateur hackers to penetrate and control badly protected personal computers connected via *always-on* broadband connections. This trend is exacerbated by the appearance of "script-kiddie" tools which enable amateur or novice users to generate complex attacks via a simple-to-use interface.

In addition to amateur attackers, professional hackers and organized crime are starting to use highly sophisticated attack tools to access private and otherwise valuable information, or gain control of the computer itself, forming the so called "botnets". The controllers of "botnets" will offer organised attack services for money. This is a particularly worrying evolution whereby criminal organisations rely on hackers to facilitate criminal activities such as fraud and extortion. Organised cyber-crime also includes attacks such as theft of trade secrets, phishing (theft of identity data), etc.

4.1.2 Future advances in worms and their potential effects

In the future, worms are expected to become more *targeted* and *stealthier*: the authors of such worms intend to use the compromised computers; therefore it is in their interests to avoid detection for as long as possible. It is unlikely that we will see again the sort of massive, easy to spot, flows that characterised worms like SQL.Slammer. The longer-term impact of the abuse of worm compromised hosts (whether managed by botnets or some other means) is likely to be greater in total than at present. That impact will include a degree of loss of confidence in the Internet (and the information society that relies on it).

Though we have not seen really devastating worms more recently, and the likelihood of seeing one in the near future is low, it may be wise to prepare for one as the consequences from a destructive worm may be significant. Also it is surprising that up to today we have

not seen worms that really destroy data on a system whilst propagating (e.g., those with a kind of “terre brulee” policy). So far, worms have been merely devastating for network resources, but it is not unlikely that someone will write a worm that really destroys useful information on the targeted systems.

If such a worm does happen, it most likely would be the single most destructive data security event in history. Lack of any occurrence to date can give us no confidence as it only takes one competent person to create and release such an attack.

The likelihood of the release of an effective and destructive network worm may be very low, but the destructive consequences of such a release extremely high. The likelihood of the release of an effective non-destructive worm is much higher and it can still cause a lot of collateral damage.

It is expected that massively distributed attacks (like SQL.Slammer) that attack overtly and with immediate destructiveness are becoming less fashionable amongst the writers of such attacks. A compromised machine now has agreed value (botnets are for hire) and it is now recognised amongst the attacker community that a mole machine is more valuable long term than a machine that is infected and then acts as a short lived guns-blazing attacker as it propagates as quickly as possible. Infected machines will only last as a long term asset if their infected nature can either be hidden or the infection can be adaptive and self repairing.

4.1.3 Rootkits and botnet software

The certain class of malware, sometimes misnamed as ‘spyware', is very adept at deeply penetrating a machine, and pernicious in its ability to avoid complete removal – leave just one loader item left on the machine and the spyware will completely and silently reinstall next time you connect online.

“Rootkits” are the other area of concern. These have been around for a while, but some recent incidents have raised the profile of ‘rootkiting’ as a successful technique. What tends to happen is that once a technique has proven to be successful we then see it aped by other writers.

We therefore expect that we will see more techniques borrowed from spyware and rootkit writers by the virus/worm authors. Such attacks would combine the effective methods of *widespread propagation* from the worm/virus community, with the *self-healing* and *camouflage* techniques of the spyware and rootkit writers; with the intent of building and sustaining a network of infected machines that provides a platform for additional attacks in the longer term.

This is one of the biggest concerns, and it may well be that the overall prolonged economic damage of such attacks outweighs that of a single "devastating worm" event.

In addition, we are seeing more targeted attacks in general against selected organisations. Included in that category are the so-called 'spear-phishing' attacks of targeted malware. Common to all these targeted attacks is the fact that the motivation is primarily monetary – a fact which supports the theory of 'malware as a platform for economic enrichment'.

4.1.4 Distributed Denial of Service (DDoS) attacks

Although DDoS is not a new type of threat, we can expect it to rise in the coming years, especially with the set up of botnets by hackers. Another factor pushing for more DDoS is adoption by criminal organisations using such techniques for extortion.

4.1.5 Identity Theft

Currently an increasing amount of credit card and other personal data are being stolen or lost. Such data is now available at certain websites for purchase at a reasonably low price. Authorities and commercial companies currently hold such data with poor security and the compromising of such data may become valid grounds for legal liability and damage claims.

The so-called Phishing attacks, where perpetrators try to make users reveal credentials that will enable the attackers to impersonate them, e.g. theft from online banks are of an increasing concern and may, if not effectively hindered, reduce trust in the Internet as a viable medium for eCommerce.

The anonymity of the Internet is the fundamental problem here and there is no widely adopted method for authenticating identity. In the short-term some banks may adopt 2-factor authentication (password plus physical token) or other techniques, but solutions may well be piecemeal and reduce user acceptance.

4.1.6 Increased level of Vulnerabilities in Software

As software becomes more complex and the timetables for releasing new versions of software are becoming increasingly shorter due to market pressure, software products are prone to have more vulnerabilities and thus become more exposed to all kinds of attacks.

Such vulnerabilities are a typical target of the hacking community that requires the response of appropriate solutions from the ICT industry, both in terms of development process methodologies for reliable and secure technology and efficient reactive processes when vulnerabilities are actually discovered.

4.1.7 Attacks on Mobile and Wireless Networks

In general mobile technologies should not be regarded as being more insecure than fixed network technology. Most threats are not mobile specific and it is a fact that some mobile network security, e.g., in GSM, is very much stronger than fixed network security (with no encryption at all). However, it is clear that when the security features of mobile and wireless technologies are not used, they become even more insecure than wired technologies, due to the simple fact that the communication medium is accessible by everyone.

- Increasing use of SMS and MMS as vectors for SPAM and also malware.
- As mobile network infrastructures and service applications migrate towards IP-based technologies, many threats and attacks today seen on “fixed” Internet-like networks are also becoming applicable in such mobile environments. This trend is re-enforced by the convergence between fixed and mobile network accesses, whereby consumers can access network-based services using the same devices over fixed and wireless infrastructures.

- Increasing connectivity between end-users (including creation of spontaneous proximity networks) will bring extra risks for propagation of viruses and worms.
- The lack of inherent traceability of wireless access leads to the need for wireless installations that follow good practice with access control and logging.
- The lack of good practice for organisations and home users using WiFi, leads to risks such as theft of service and exposure of internal network traffic.
- Related new technologies and architectures, like WiFi, ad-hoc, mesh, sensor networks, ambient networks etc., are all creating new challenges that require special attention to security.

4.1.8 Security Issues with Peer-to-peer Networks

Peer-to-peer networks usually rely on end-users sharing part of their storage space and/or computer resources in general with remote peers. This is an open door for remote hackers to hack into end-users' systems and also to distribute some form of malware. Our focus here is on the security problems linked to the use of peer-to-peer networks, but not with the problem of illegal content sharing. (The first is part of the scope of ENISA, while the latter it is not).

4.1.9 SPAM and SPIT

SPAM (unsolicited mass email) is a well-known annoyance for which both legislative and technical solutions are being developed. But despite the development of countermeasures, SPAM continues to evolve, with more and more sophisticated techniques to escape detection mechanisms put in place in anti-spam solutions. What is even more worrying is the perceived migration of spam into VoIP-based networks, so-called SPIT (SPAM over Internet Telephony). A successful deployment of future VoIP-based services will depend on efficient solutions to counter SPIT, as the level of annoyance for end-users gets much higher with phone than with e-mail.

4.2. Security Issues not Related to Technology

In addition to the risks and threats which are related to technology, there are very important non-technical issues which are key to good security. These issues are mainly concentrated around human factors, and include concerns such as lack of security awareness, increased professionalism of cyber-criminals, increased reliance on the Internet, and industrial espionage.

4.2.1 Lack of Security Awareness

The desired outcome of raising security awareness is to make the consumer aware of security concerns and options. It would be foolish to argue against the merits of better educated citizens. Not only educated in order to know the security issues, but also as educated ICT consumers. This will increase the chances of profoundly improved information security.

According to a somewhat old analogy, it not clear that today's citizens are that much better at driving motor cars than the citizens of 30 years ago, but cars are definitely a lot safer. This is because the cost to society due to deaths and traffic-related injuries became too

high, and it was realized that the cars had to be made safer. Through a combination of legislative actions, such as mandating safety belts, and vendors' realization that safety actually could be a sales proposition, we ended up in today's situation with safer cars.

Although legislation was important, the most important achievement in the motor car example was to make safety something that purchasers asked for, so that manufacturers competed to add genuine safety features to meet that customer demand. Many brands of car now base their advertising on safety, and even the base models now come with advanced security features, such as airbags, as standard fittings.

Improving the security of ICT products by motivating purchasers to ask for security features will lead to a virtuous spiral and to be preferable to the alternative of mandating security measures only by legislation. Legislation tends to lead to combative relationships and minimum compliance whilst market pressure leads to mutual benefit.

The solution for a more secure future should therefore be based on well educated users and consumers with supported by only “light touch” legislation, underpinned by better informed procurement. The combination of awareness and legislation requiring transparency on security will create forces to software and hardware vendors in a more security oriented direction.

4.2.2 Professionalism of Cyber-criminals

The preceding section of this paper outlines the risks of malware and the growing sophistication of attack. The professionalism of this attack and the resulting motivation is worthy of further discussion. It is a fact that more and more of the advanced malware that we see are created by professional criminals. They are motivated by financial return from targeted victims and they will not profit from creating a widespread destructive worm. In fact the public scrutiny following the release of a destructive worm would greatly increase the risk of a fraudster being caught. The need for stealth is even more important in the case of information theft and cyber attacks aimed at the theft of intellectual property by industrial espionage are increasingly common.

It is clear that monetary benefit is one driver which leads criminals to be stealthy. Political ambitions (e.g., terrorism) may have another dimension. In this case publicity and level of havoc caused is a more important outcome for the attacker.

At present there is much evidence for organised crime sponsored attacks. But terrorists currently prefer physical weapons of terror such as bombs. Both groups do however introduce a level of sophistication and funding of attacks that is far beyond what we have commonly seen in the previous 20 years of cyber security.

4.2.3 Increased Reliance on the Internet and Networked Resources

In the midst of general ICT systems development and adoption another trend of widespread digitisation of physical infrastructure, industrial plants and consumer goods has been happening. This dependence on digital infrastructure has occurred with little focus or attention but does lead ENISA’s work to be relevant to critical national infrastructure even though this is currently out of the scope of the agency.

In our view the reality of significant business dependency on the Internet and adoption of Commercial Off the Shelf (COTS) technologies within critical infrastructure will make

future attacks on ICT services have a much wider consequential disruption to other services. The distinction between the types of systems will soon be academic and solutions taken forward by ENISA will be applicable to the broader protection of society.

It has to be noted that *all-IP* is not always good. The idea of connecting the hospital Emergency Room computers and even door operation to a system with a less than perfectly protected link to the Internet proved to be vulnerable. In a recent hacker attack the computers crashed and the doors did not function.

5. Long-term Actions for ENISA

The Permanent Stakeholders Group feels that ENISA should have a role as a catalyst. To draw an example from the military ranking, ENISA should play the role of the general rather than a soldier in the fight towards a secure world.

The target groups of the outcome of ENISA's activities should be large Businesses, SMEs, Consumers and Member State agencies, etc. In addition ENISA should maintain cooperation and exchange of information with organizations where the large businesses are involved.

5.1 Cooperate and coordinate Member States' national network and information security authorities

ENISA can do most good by facilitating, through all possible means, cooperation between national Network Security agencies and actors. This is because ENISA's resources are very low for the duration of the first budget period. The existing Member State national resources are significantly greater. Cooperation between national agencies is very low at the moment. Much good can be done by fostering increasing communication and cooperation between the national agencies, particularly in sharing best practice from advanced agencies to those who are just starting.

5.2 Cooperate with research institutes

ENISA's purpose should be to direct basic research and targeted technical development in order to focus on the areas of greatest benefit to managing actual security risk in real-world systems. ENISA should not support research agendas by itself, but rather work on aligning the existing processes and priorities of existing programmes.

ENISA should become a trusted discussion and planning partner for the leading research institutes in selecting and evaluating papers and research projects. (But care should be taken in focusing effort as such activity may be time-consuming due to the large number of research institutes and the current staffing plan of ENISA is quite limited).

5.3 Cooperate with software and hardware vendors

Vendors of software and hardware are by definition competitors and can be difficult for them to openly agree on mutual practices. ENISA could provide unbiased opinion and a forum for sensitive discussions, while maintaining the necessary hygiene against anti-competitive behaviour.

ENISA's long-term vision should focus more on creating reliable network and information technologies that are resistant to worms and other problems, instead of extending current incremental security trends. This could be achieved with the promotion of techniques for developing correct, secure and reliable architectures and software.

ENISA should make recommendations to improve certifications and standardizations, such as 'Common Criteria'-based evaluation processes. ENISA should further seek to make these processes less expensive and faster, which will help with their implementation.

5.4 Participate in standard-setting bodies

With an eye to identifying and publicising initiatives or greatest value, ENISA should track and monitor NIS-related topics in standards-setting bodies, including following up the works of various available security certification and accreditation bodies.

5.5 Participate in legislative process through lobbying and opinions

ENISA should work to gain the position of a trusted consultant body to be heard early in the process of drafting and proposing directives and other legislation in NIS-related issues.

Before lobbying is performed, ENISA should clearly document the position and goals of such lobbying.

Through its links with the stakeholders (industry, users, academia), ENISA can also play an important liaison role between the stakeholders and the legislative/regulation institutions.

5.6 Work with user organizations

Often user organizations are not as well represented in legislative and standard-setting bodies as are vendors. ENISA could provide end user groups with an insight into standards work and an opportunity to influence such work.

5.7 Identify and promote best practises to Member States to end user industry

ENISA should not only protect business interests, but must also enhance end users' confidence in the use of the Internet and digital media. This confidence needs to be built at all levels so, for example DRM technologies must not cause technological instabilities, and must not be used to enforce rights that are not considered reasonable by the broad base of users.

5.8 Work for a technical and political solution for identity management

Lack of confidence in the Internet is the main obstacle to large-scale consumer-oriented e-business. To be able to accurately check the identity of an owner of a site, an email address, or some online service a user communicates with, would be a huge step to renew and increase the trust of the common users in the Internet. Technical solutions in this area should be sought through industry-led processes, but ENISA could work towards EU-wide policies for authentication of online entities.

Interoperability is one of the main challenges for success in the field of identity management; therefore this work should be done at pan-European, or even global level, since it is virtually impossible to promote development of sustainable local solutions.

5.9 Balance the efforts to both “Information” and “Network” security issues

ENISA should communicate with the largest Internet and Network Service Providers ISPs/NSPs to help them identify best practises for the benefit of businesses and consumers across Europe. This is important because ISPs/NSPs can play a key role to improve security in the Internet at large. Sufficient co-operation and coordination between the actions ISPs are taking is lacking at the moment.

We acknowledge that ENISA has limited resources. Therefore in order to perform all or some of the suggested actions outlined in this Vision Paper it might be necessary for ENISA to grow by recruiting and maintaining a sufficiently large number of well-respected staff.

6. Annex A: Members of the PSG

Name	Country	Organisation
Jaap Akkerhuis	Dutch	NLnetLabs
Charles Brookson	British	Department of Trade and Industry, UK
Giuseppe Carducci Artenisio	Italian	Securteam (Marconi)
Nick Coleman	British	IBM Europe
Andrew Cormack	British	UKERNA
Paul Dorey	British	BP
Philippe Duluc	French	France Telecom
Andreas Ebert	Austrian	Microsoft
Kurt Einzinger	Austrian	ISPA Austria
Cecile Gregoire	Belgian	EuroCommerce
Wim Hafkamp	Dutch	Rabobank
Urho Ilmonen	Finnish	Nokia
Andrzej Kaczmarek	Polish	Polish Data Protection Authority
Sandor Kurti	Hungarian	Kuert Information SecurityGroup
Stephan Lechner	German	Siemens
Petri Lillberg	Finnish	SSH Communications Security
Evangelos Markatos	Greek	ICS - FORTH
Vilma Misiukoniene	Lithuanian	Infobalt Association
Sead Muftic	Swedish	Royal Institute of Technology Stockholm
Magnus Nyström	Swedish	RSA Security
Olivier Paridaens	Belgian	Alcatel
Simon Perry	British	Computer Associates
Norbert Pohlmann	German	University of Applied Sciences Gelsenkirchen
Sachar Paulus	German	SAP
Risto Siilasmaa	Finnish	F-secure
Marta Villen Sotomayor	Spanish	Telefonica
Jacques Stern	French	ENS
Robert Temple	British	BT
Giuseppe Verrini	Italian	Adobe Systems
Anton Zajac	Slovakian	ESET