enisa European Network and Information Security Agency

Quarterly

10/2005

IN THIS EDITION

A WORD FROM THE EXECUTIVE DIRECTOR

It's been a very busy summer for ENISA. Dominated by our move to Heraklion, I am proud to say that ENISA is now fully up and running in our new base. Boxes have been moved, offices set up, and by planes, ferries, and automobiles the staff has arrived. And at the end of it all, I am delighted to let you know that ENISA is open for business.

Looking for housing, learning basic Greek, and finding the best place for a meal – it has been a challenging and fascinating learning experience for all of us.

When our last newsletter came out, we were working with a team of 7 seconded national experts interfacing with the whole of Europe. As ENISA is now almost at its cruising altitude of 44 full time staff, just imagine the possibilities! We are excited about our activities and hope this publication will give you the inside scoop on what we've been doing.

ENISA now has three departments – the Technical Department, led by Alain Esterle, the Cooperation and Support Department, led by Ronald de Bruin, and the Administration Department headed by José Carreira. I have full confidence that with the hard efforts of our entire team we will be able to fully tackle the challenges ahead of us.

Recently we had a great conference in Budapest at ISSE 2005. ENISA was a co-organizer of this event together with our partners eema and Teletrust.

This was a very important event for ENISA, as it was our first major event in which we took a core organizational role. ENISA played a very active role in the Program Committee and Steering Committee where we were represented by our own Boaz Gelbord.

And the great news is that eema, Teletrust, and ENISA are teaming up again next year for ISSE 2006. This event will take place in Rome, where we will be hosted by the Italian Ministry of Communications.

Where to now? With ISSE and our 6th Management Board meeting behind us, ENISA is pushing ahead full throttle. We look forward to continue to work with you in the exciting areas of our mandate, including CERT cooperation, awareness raising, and different technical aspects of information

➲

ISSN 1830-3609

security. We have many new ambitious goals in our 2006 work program.

ENISA will also continue to build upon the great network that was put together of National Liaison Officers, with the torch being officially passed on to Tim Mertens, our new Senior Expert for Coordination of Activities with Member States and European Bodies.

With an ever changing technological landscape, information exchange on today's security challenges is more vital than ever. We hope this publication can make a small contribution to this effort.

Happy reading!

Yours truly,

Andrea Pirotti.
Executive Director, ENISA |

A WORD FROM THE EDITOR

Welcome to this, the second edition of the ENISA Quarterly. After a hectic move to Heraklion and a busy September that culminated in the ISSE conference, we are happy to bring you another version of our quarterly publication.

You will notice that this publication has grown and has expanded in scope with this new edition. We hope that it will provide you with a valuable resource and we very much encourage you to share the publication with your respective communities who may be interested.

I would like to personally thank everyone who contributed to this edition. We are very flattered by the many articles that people offered, and we appreciate very much your continued support and participation in this endeavour.

We received a lot of positive feedback from you about our first edition. With this edition we have expanded the menu and nearly doubled the size of the publication (as well as reverted to the name ENISA Quarterly, since it will come out once each quarter). It is chock full of the latest news in information security and on our activities.

We have dedicated a number of pages to ISSE 2005, which is not surprising since this was the first major event ENISA has co-organized. The conference was a big success by any measure and we hope to give you a taste of the important discussions in the coming pages.

In this edition, we bring you a wide range of views from across the information security community. We also bring you two contributions from our own staff. Marco Thorbruegge brings us a report from the GOVCERT conference in the Netherlands, and Carsten Casper takes us into the fascinating world of network security policies.

The technical articles can at times be quite... well, technical. But for everyone working in the information security area, it is important to understand the latest developments in the field. In this edition we try to bring a few of the most important technical issues to the fore, in plain and easy to read language that is easily accessible to non-technical audiences as well. For this edition, we have chosen two particularly hot topics – security developments in both Internet architecture (DNS) and in so-called hash functions.

Many of us have probably heard about DNS in the press (particularly with ICANN being in the news and with the upcoming World Summit on the Information Society in Tunis), but may not have been sure what exactly this means or what the security implications are. In a thorough yet accessible article on this topic, Jaap Akkerhuis and Peter Koch provide us with a great primer on this area.

Also on the topic of technical developments in the news, anyone reading this publication probably knows that a hash function is not a drug party, but rather a critical component of digital signatures. The last year has seen some startling developments in the security of hash functions, with serious implications for the security of the corresponding digital signatures. Stephan Lechner of Siemens has written a great piece for us giving the lowdown on what all these developments mean for digital signatures. Definitely recommended reading even for the technophobes in the crowd!

In this edition we also give you an eye on our previous and upcoming events. These include the Polish SECURE conference that will be taking place very shortly after publication and the "Network and Information Security: Political and Technical Challenges" workshop that will take place in early November in Rome.

Last, but certainly not least, we have a look at information security in Member States. In this edition we have a feature on an interesting training program in Lithuania and bring you some of the many important developments occurring in information security in Germany.

I very much encourage all of you to provide feedback on what you have read and please do not hesitate to contact me if you would like to make a contribution. We hope that through such information exchanges, we will be able to do our part for a culture of network and information security.

I hope you enjoy reading our Quarterly as much as we enjoyed putting it together.

Sincerely Yours,

Boaz Gelbord,
Editor-in-Chief, ENISA Quarterly

Boaz is a Senior Expert in Security Technologies at ENISA |

ISSE CONFERENCE 2005

Our first major conference, ISSE 2005 gave ENISA the chance to both listen to and learn from international experts, as well as the opportunity to showcase our own activities and vision.

Before giving you a round-up of some of the highlights of this event, we would be amiss if we did not mention the incredible cooperation and help we got from our partners in this endeavour – eema and Teletrust, and our hosts, the Hungarian Ministry of Informatics and Communications.

The Executive Director Mr. Andrea Pirotti and the Hungarian Minister of Informatics and Communications, Mr. Kálmán Kovács

It's been a few weeks since Budapest, but most of us here at ENISA are still on a high. 400 people, 3 days, and dozens and dozens of talks loaded with trends and developments in information security. We couldn't even begin to summarize the content of the conference in these pages, so instead we just skim the surface with a few highlights and also give you a brief overview of our ENISA session which was held on the first day.

The conference was opened by Frank Jorissen, the chairman of eema, who introduced the Executive Director of ENISA, Andrea Pirotti, and the Hungarian Minister of Informatics and Communications, Kálmán Kovács.

Our Executive Director Andrea Pirotti gave a warm welcome to the conference. He underlined the goals of ENISA and its objectives for the coming year. He emphasized the need for cooperation and support from all actors and said that ENISA was delighted to be part of that process by co-organizing ISSE 2005. The Hungarian Minister Mr. Kálmán Kovács spoke of the need to achieve knowledge transfer in the area of information security and the possibility of regional transfer centres to achieve this aim.

The next keynote was by Howard Schmidt, a leading American information security expert. Mr. Schmidt has held numerous top positions in information security – including the positions of cybersecurity advisor to President Bush and Chief Security Officer of E-Bay and Microsoft - but is very down to earth and seems to prefer to be called Howard than Mr. Schmidt. Howard delivered an electrifying and fascinating speech on the various international developments in information security. His wide experience meant that there was always an interesting anecdote on information security peppered in between the slides.

Howard's participation further underlines ENISA's view that information security is a global issue. ENISA is especially keen to learn from best practices in leading information security countries like the US, and that's why Howard's participation was particularly valuable to us.

In the afternoon ENISA held its own session, with a panel discussion with four leading experts from diverse backgrounds. This panel was chaired by Boaz Gelbord, the Senior Expert in Security Technologies at ENISA.

After the introductions, Boaz explained the voting system that was used for audience participation. By asking questions at regular intervals, the panellists were kept on their feet and had to contend with unexpected results from the public. The interesting results of this experiment in direct democracy can be seen in the coming pages.

The ENISA session provided a tour through the important issues of emerging technologies and the public response to their security challenges. Howard was back at the podium for the ENISA panel, where he got a chance to further expand his views and in particular to outline his vision of three key components in security success – people, processes, and technology.

➲

The Panel Discussion at the ENISA Session at ISSE 2005

The next speaker was Jacques Stern, a renowned expert on security and cryptology from the Ecole Normale Supérieure in Paris. Professor Stern gave a very accessible overview of issues related to managing and protecting identities. He also gave an insight into the wide range of technical possibilities such as "traitor tracing" that can be used in the online environment.

The main issue, in his view was non-technical: namely to find innovative business models for content distribution. Such models could take advantage of the numerous cryptographic protocols which have been developed.

Next came Risto Siilasmaa, the CEO and founder of one of Europe's leading security technology companies, F-Secure. Mr. Siilasmaa has been an active contributor to European initiatives, being a member of the eEurope 2005 Steering Committee and a member of the ENISA Permanent Stakeholders' Group.

Mr. Siilasmaa gave a comprehensive look at the state of viruses and security, with a particular emphasis on the threats wireless technologies pose to users (in fact, he warned 5 participants in the front rows to check their Bluetooth settings as they were exposed!).

Last but certainly not least came Francisco Garcia Moran. Mr. Garcia Moran has a tough job. As acting Director General of the European Commission's DG Digit, he has the formidable task of making sure that the EC's IT systems are up and running all the time. And security, it goes without saying, is one of the major challenges in this arena. Mr. Garcia Moran gave a thorough overview of the challenges faced by security professionals, as well as a nice example of how spammers avoid spam filters by cleverly masking their content.

Mingling with the Students – ISSE 2005 was held in the beautiful environment of the Budapest University of Technology and Economics. Some PhD students attended sessions that interested them, while other students mingled with the hundreds of delegates who had converged on their institution. Housed in a classical building with a beautiful view of the River Danube, many participants expressed their delight at being in such nice surroundings rather than in the usual hotel conference room.

All in all the audience seemed to greatly enjoy the panel discussion, with the voting system being a particular hit. Boaz promised that ENISA would carefully digest the important discussions that had taken place.

Following the panel discussion, ENISA's newly minted Head of Cooperation and Support Department, Ronald de Bruin, led a discussion by the three Working Groups of ENISA. Janice Richardson presented results on Awareness Raising, Miroslaw Maj on CERT cooperation, and Serge Lebel on Risk Management. It was clear that these groups were bringing together some of the best expertise in Europe to help ENISA achieve its mandate in these important areas.

Over the next three days before the closing plenary, there were dozens and dozens of other great speeches and presentations. For those of you who missed these, check out

Ronald de Bruin, Head of Cooperation and Support Department, introducing the chairpersons of the ENISA Working Groups.

Networking at ISSE 2005

the eema website, or better yet, make sure to pencil in ISSE 2006 into your diaries!

The conference ended with a bang with two heavy hitter speakers – Fabio Colasanti, Director General of Information Society, and Prof. Ross Anderson of Cambridge University.

Mr. Colasanti gave an overview of the developments in information security and gave an in depth overview of the European Commission's activities and strategies in this area. He pointed out the call for action contained in the voting results from the day before, whereby participants certainly felt that public authorities should play an important role in network and information security matters, but did not rate their performance as satisfactory to date.

Prof. Ross Anderson requires no introduction to anyone even vaguely involved in information security. The Cambridge Professor is one of Europe's information security stars, having published countless articles in fields as diverse as the economics of security to cryptography. His fascinating speech on the economics of security made sure that even after three days of intense talks, people stayed alert and attentive to the very end. He emphasized that the economics of security were just as important as the technology, and he gave numerous real life examples of this.

Finally, the plenary ended with what was by then an open secret – ISSE 2006 will be held in Rome! ISSE 2005 is just behind us, but we are already working hard at ISSE 2006. |

Enjoying Ballet at the Gala Dinner at the Gundel Restaurant

Raising a glass to the success of ISSE 2005 – The Gala Dinner at the spectacular Gundel Restaurant

THE PUBLIC VOICE – WHAT **YOU** HAD TO SAY

The ENISA session featured an exciting e-voting system to involve the audience, rather than just listening to the panel give their views.

The topics voted on did not steer away from controversy, with questions about open source vs. proprietary software and an evaluation of the performance of public bodies.

The results are fascinating – at times predictable, at times unexpected, and at times seemingly contradictory. Turn the page for a slice of what European information security professionals think about a range of important issues... |

ISSE 2005 voting results

The state of Internet security is…

1. Pretty good – the threats have been exaggerated by interested parties and user paranoia. **7%**
2. So-so – there are threats but with some precautions users can feel secure. **41%**
3. Pretty bad – urgent action is necessary so that security concerns do not further stifle the growth of the Information Society. **48%**
4. Completely *#%$#%#. I have moved to a forest in Montana and cut off all communication with the outside world. **4%**

In the next 5 years, the major threat to the Internet will be…

1. Identity theft and phishing scams **21%**
2. Hackers **2%**
3. Denial of Service attacks **12%**
4. Mobile security threats **38%**
5. None of the above **27%**

Who is most responsible for the current problems in online security?

1. Software producers **51%**
2. Hardware manufacturers **0%**
3. Public bodies **2%**
4. Network operators **4%**
5. ISP's **4%**
6. Users – when will they learn??? **8%**
7. No one party is to blame **31%**

Who do you most trust to solve the security problems on the Internet?

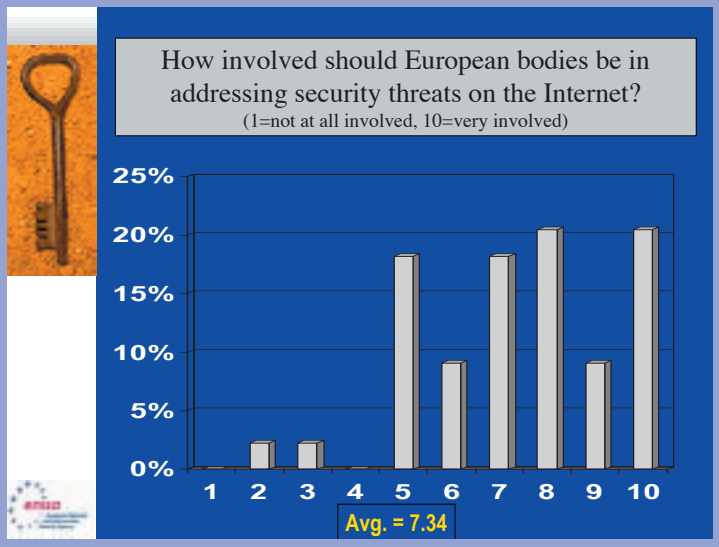
1. Software producers **23%**
2. Hardware manufacturers **0%**
3. Public bodies **25%**
4. Network operators **0%**
5. ISP's **2%**
6. Users **11%**
7. None of the above **40%**

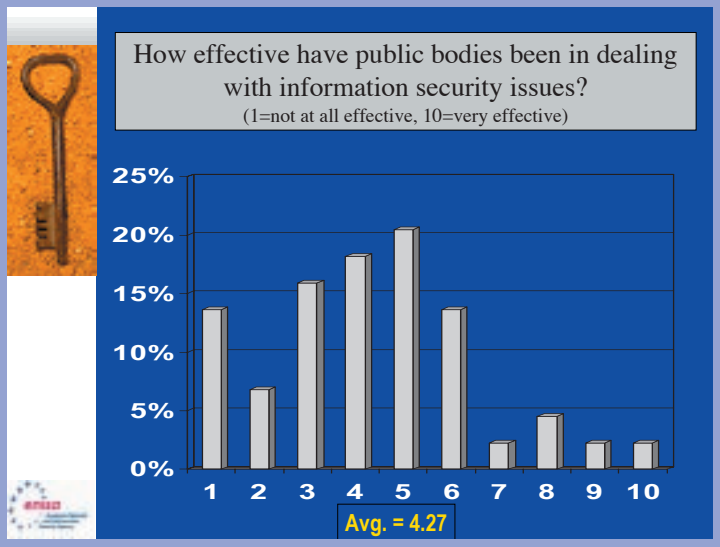
The best way to produce secure products is through…

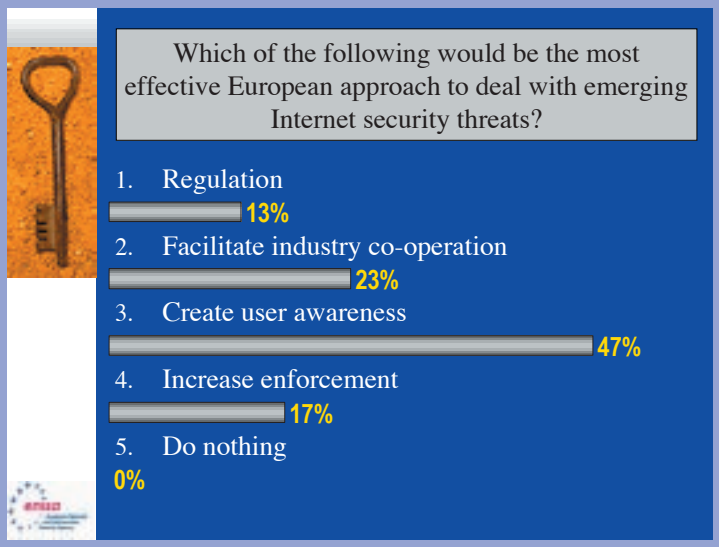
1. Open source collaboration **39%**
2. Standardization **11%**
3. Industry collaboration **37%**
4. Proprietary software **7%**
5. Government regulation **6%**

Convergence of technologies and the move towards an IP backbone will make us

1. More secure **10%**
2. Less secure **90%**







From the World of Security - A Word from the Experts

Securing the Internet's Largest Distributed Lookup Service - DNSSEC Deployment Issues

Jaap Akkerhuis, Peter Koch

Background

The DNS (Domain Name System) serves as one of the Internet's most important basic technologies. The hierarchical, redundant distributed data repository is used to translate human readable domain names into host addresses and other infrastructure elements. The system has been working well for almost 20 years and has proved to not only scale well but also to be flexible enough to address new and emerging technologies, e.g. IPv6 and VoIP (through ENUM).

Another aspect that changed dramatically during the evolution of the Internet is the nature and extent of security threats. Here the DNS shows its age by assuming a level of trust that was appropriate in the early days of the net but unfortunately no longer is today. Responses coming from the DNS are taken for granted without cryptographic authentication, opening it to various vulnerabilities. Attacks like DNS message spoofing and cache poisoning were documented in the early 1990s and while some intelligence has been built into DNS software to mitigate the most obvious paths of unauthorized data manipulation, the inherent weakness of the protocol remains.

DNS weaknesses have not yet been widely exploited for various reasons. First, a successful attack not only needs sophisticated preparation but also might produce enough traffic not to remain unnoticed. Second, the DNS usually provides only for a layer of indirection, i.e. manipulating DNS information may redirect upper layer communication which in turn may employ its own security mechanisms. Third, the incentive, other than "proof of concept" might not have been big enough compared to other, more direct attacks on systems and communication.

To emphasize the second point above, most web communication involving sensitive data today is expected to be secured by TLS, signaled by the https in the URL or by the little lock displayed in the browser's window. TLS provides for endpoint authentication in addition to channel security, so even if one were able to map a domain name to a wrong IP address, the subsequent http/TLS communication would fail since the attacker

➲

would not be able to present the correct certificate belonging to the domain name so misdirected. Similar reasoning applies to SSH based remote login which gives a cautious user the opportunity to check a target host's fingerprint.

DNS Protocol Enhancements

So, when we have been living well with this alleged DNS weakness for more than a decade, why is there a need for a change?

The Internet Engineering Task Force (IETF) published a first version of DNS security extensions (DNSSEC) as early as 1997, close to when the first major cache poisoning attack received wider attention. However, a protocol specification is just a piece in a larger puzzle. Interoperable implementations, operational procedures, tools, documentation and tutorials, and finally a demand driven deployment are all crucial to the success. It turned out that the first and the second version of DNSSEC had technical issues demanding a refinement of the protocol specification. In March 2005, a set of three RFCs (Request for Comments) were published as IETF Proposed Standard. The situation is much more promising than 1997, though, since today we do not only have a well designed and tested protocol but also support from at least two major DNS software implementations as well as helpful tools and operational experience from a variety of testbeds and workshops.

In addition, the DNS has become much more than a system translating names into IP addresses. A variety of new applications make use of the DNS infrastructure, telephone number mapping (ENUM) and mail sender authentication to name a few. One difference is that e.g. ENUM implements an indirection that cannot easily be verified when the subsequent communication is initiated. It is therefore important to ensure authenticity and integrity of the ENUM information to avoid malicious VoIP call redirection. Similarly, DNS based methods in the anti spam arena provide an incentive for already criminal subjects to modify DNS information.

Both the availability of the technology as well as the new challenges for the DNS suggest that now is the time to start Internet scale deployment of DNSSEC.

Deployment

The DNS namespace is hierarchically organized and uses different levels of this hierarchy to distribute the management and operational responsibilities to a large number of different entities down to organizational, departmental or even office level. DNSSEC leverages on this hierarchical model taking advantage of the proven scalability and the distributed management model. However, the hierarchical model does not support early adopters very well. In contrast to, say secured websites or digitally signed electronic mail, there is not much opportunity to just start using DNSSEC between an ever growing group of interested parties. To verify authenticity of DNSSEC information it is necessary to have signed all DNS zones starting at the root all the way down the trust chain to the node in question. While at the top of the DNS hierarchy (that is, the root zone and the toplevel domains (TLDs)) there has already been some discussion and coordination, more work needs to be done on the receiving end. Here is an overview of current areas of interest:

Validators are needed on the consumer side that can fetch, interpret and cryptographically verify DNSSEC signatures on the DNS data. They also need to follow the trust chain up to a trust anchor, which will at the end be associated with the DNS root zone key. Dedicated software for this task is currently under development.

User Interface issues are dealt with at different levels. First, applications need a modified, DNSSEC aware API that allows them to specify their security needs and to react to signature verification success or failure. Second, application programs like web browsers or VoIP soft phones need to communicate to the user that a name lookup did or did not succeed securely.

Key Management for the DNS root key is crucial to DNSSEC deployment. Since the root key will have to be distributed to millions of validating resolvers, extreme care must be taken during both generation and handling of the key. A root key compromise would jeopardize the whole DNSSEC effort. Interested parties are working on appropriate procedures as well as on automated key rollover mechanisms.

Politics are involved when it comes to signing the DNS root zone and thus to securing and controlling the trust anchor due to the international nature of the Internet. Currently changes to the root zone are dealt with by the ICANN IANA, the US Department of Commerce and VeriSign in their function as technical editor of the root zone. However, this is under discussion at WSIS (World Summit on the Information Society), and the perception that any one entity holding the DNS root key "controls" the Internet needs to be dealt with not to further delay DNSSEC deployment.

Cost of initial deployment of DNSSEC may be considered high on the server side. Large zones, especially TLD zones will grow significantly and although that is no longer a technical barrier, DNSSEC is currently a binary thing. If a TLD zone is to be secured, it will require signatures (and thus memory, CPU, and bandwidth) for all of its children, even the unsecured ones – to be able to prove they are unsecured. It is thus important to acquire a critical mass of second level domains to be signed. In addition, the IETF is currently working on a protocol addition that could allow for a smoother phase-in.

Privacy and security are related, but sometimes there are trade-offs. As a side effect of DNSSEC all names in a secured zone may be disclosed. The so called zone walking problem is unacceptable to many TLD registries for legal and contractual reasons, since it may be abused by address harvesters or domain grabbers. Again, the IETF is working on a protocol enhancement to avoid this undesired disclosure.

Conclusion

The security extensions to the Internet's Domain Name System have recently been published as an IETF Proposed Standard. While the protocol is believed to be mature

and interoperable implementations exist, DNSSEC has not yet been widely deployed. We have demonstrated some of the operational and organizational challenges and the ongoing efforts to deal with these. DNSSEC has been waiting for the killer application for years, but rather recently several new technologies have been proposed or deployed on top of DNS which need secure name resolution. Anyone considering those new applications like ENUM or DNS based anti spam systems should have DNSSEC on their radar screen and become familiar with itrs concepts and implementation.

Jaap Akkerhuis works at NLnet Labs, a small non-profit research facility dedicated to the evolution of the Internet. He is a member of the ICANN Security and Stability committee.

Peter Koch is a Senior Researcher with DENIC, the toplevel domain registry for Germany (DE).

Hash functions broken - are our digital signatures still secure?

Stephan Lechner

Summary

This article explains in an understandable way the implications of recent results on "breaking" hash functions. The mathematical results shown since the CRYPTO 2004 conference imply that the strength of certain hash functions (MD4, MD5, RIPEMD, HAVAL-128, SHA0, SHA1 with a reduced number of rounds) is not appropriate any more. For the future one can expect that those attacks might carry over to SHA 1, one of the most popular hash functions. Thus, in the long run, SHA 1 should not be first choice for any new product development any more. The attacks do not transfer to all hash functions (e.g. not to SHA128, SHA224, SHA 256, SHA384, SHA512).

In 2004, the US American National Institute of Standards and Technology (NIST) issued a statement that they are planning to phase out their recommendation of SHA1 in favour of other hash functions by the year 2010. This seems ambitious, as with respect to more recent results SHA 1 might become shaky before.

Hash functions

Hash functions are specific functions in a cryptographic context that are used to map large (encrypted) texts to short texts. They provide a significant basis for digital signatures; usually one does not want to have a full document being encrypted by a sender's private key for showing its authenticity but rather just takes a digest of the document and encrypts it. Therefore so-called hash functions are used that, of course, have to meet certain mathematical requirements.

A hash function basically has one "big" input channel and one "small" output channel only. It "compresses" large input to small output text of always the same size. The most important requirement on hash functions is that there are no collisions, i.e. two different inputs (e.g. documents) must not produce the same output. This is easily understood in the context of electronic signatures, where only the hash value of a document is signed and therefore must be unique across all possible documents. (Otherwise the digital signature could legally be challenged for not originating from the attached document!).

Creating a collision-free hash function is really tough, as there are much more theoretical input values to a hash function than possible outputs, though the number of possible hash outputs usually significantly exceeds a billion billions. As the number of input values exceeds the number of output values, theoretically, there always are collisions. The problem to find any of them therefore must be mathematically hard!

What happened since CRYPTO 2004?

Recent mathematical results showed that there are practical possibilities to generate "near-collisions" on some hash functions much faster than before. Whereas the best results in attacking up-to-date hash functions this way used to require 2 to the 64th operations before, the new approach reduced the number of operations to 2 to the 43rd. This means that an attack that by far exceeded 10 billion billion operations now can be performed more than a million times faster! This comes close to being computationally feasible.

One has to admit, that "near-collisions" are not exact collisions but there are mathematical connections between both structures that ease concluding from one to the other.

With the 2004 results a set of hash functions has been moved from the category "computationally infeasible to be broken" to the category "computationally almost feasible to be broken soon". At the EUROCRYPT conference (May 2005) there was even presented a collision for the MD5 algorithm involving an effort of 2 to the 39th. Later in 2005, Professor Lenstra from Eindhoven University demonstrated how MD5 based X.509 certificates – a basis for digital signatures - can be forged if they are based on MD5. The MD5 hash function therefore can be considered broken and should not be used any more.

In general, the results shake the trust in digital signatures based on the affected hash functions.

What algorithms are affected?

Affected algorithms are MD4, MD5, RIPEMD, HAVAL-128, and SHA0 (A word on acronyms - SHA stands for a family of "secure hash algorithms" whereas MD denotes "message digest"). SHA 1, one of the most popular hash functions, is not directly affected yet, but moving closer to being affected.

The results shown do not directly transfer to SHA128, SHA224, SHA 256, SHA384, SHA512 as other members of the SHA family.

What are the implications?

Practically, not much happened. Yet.

All basic principles of digital signatures and PKI (Public Key Infrastructures) are still valid. There has been no world shaking quantum leap, nor has there been any breakthrough result that compromises PKI, asymmetric cryptography or digital signatures as a whole. But the progress since 2004 is so significant, that the future of certain hash functions is not at all bright any more.

This, by the way, is a natural process in cryptography, where over the years new ideas and attacks come up and eventually weaken the well known algorithms that have been around a long time - one of the victims now is MD5. New and stronger algorithms usually are put in place easily (e.g. triple DES instead of the broken data encryption standard DES), but those again are subject to attacks of the mathematical community. One of the philosophical ways out of the dilemma is to never publish an algorithm's details, but applying this principle of "security by obscurity" on the other hand spoils the opportunity of having an algorithm

approved by the "test of time" (e.g. all the attacks from the mathematical community described above).

In the year 2004 the US National Institute of Standards and Technology rethought their recommendation for SHA1, as future mathematical or cryptographic results might put more pressure on the algorithm. NIST therefore have issued a statement that they plan to phase out SHA1 and replace their recommendation by other hash functions (e.g. SHA128, SHA224, SHA 256, SHA384, SHA512) by the year 2010. This is ambitious, as SHA1 might come into trouble before: Already at the CRYPTO 2005 conference, a Chinese research team showed ideas to reduce the effort for SHA1 collisions to 2 to the 63rd operations – which, admittedly, is still computationally infeasible today but is nonetheless 64 times faster than any result before. If new products to create digital signatures are developed, there should be a thorough investigation of hash algorithms beforehand. Digital signature schemes usually cannot easily be updated to a different algorithm, as a new hash function would not be "downward compatible".

Thus, once a far distributed and well-known hash algorithm is broken completely (for full length SHA1 this is NOT the case today), all digital signatures produced on the basis of that algorithm are at stake. There is no clear guess if and when this might be the case, but the recent results from the cryptographic community imply that one better should use one of the more future-proof, longer SHA versions for new product development.

Stephan Lechner is head of central security R&D at Siemens |

Upcoming ENISA events

ENISA, ISCOM and FUB are proud to announce the "Network and Information Security: Political and Technical Challenges" workshop

ENISA will be co-organizing, together with ISCOM (Istituto Superiore delle Comunicazioni) and FUB (Fondazione Ugo Bordoni), the "Network and Information Security: Political and Technical Challenges" workshop in Rome (Italy), from 2 to 3 November 2005.

The workshop comes in reaction to recent worldwide developments in the area of information security. During recent years all the public and private stakeholders have experienced that the actual level of communication network security strongly impacts on the development of modern Information Societies. This impact is perceived both at political and technological levels.

Indeed, many innovative political and business-related initiatives (such as e-commerce and more recently t-commerce) are not fully exploited because of, amongst other factors, the perceived poor security granted by the actual communication networks.

Even the emerging broadcasting technology of digital TV exploits the attraction of interactive services and, hence, needs network security in the information exchange process.

The implementation of a high level of communication network security is even more important when the focus is to ensure an adequate level of quality of service for the security functionalities of infrastructures that are critical for everyday life in a modern country (e.g., business related services and critical infrastructures operations).

Sometimes, the approach followed to gain more network security is to unnecessarily implement very strong (and expensive) countermeasures, wasting resources. Sometimes, we prefer "hiding" problems, hoping for "good luck". Both approaches are inappropriate in the medium-long term, having as their main effects the discouragement of investments and the lowering of end user confidence, respectively.

The workshop aims to give government experts and top level technologists the opportunity to share good and bad experiences, based on the principle that in the network security world the main way to reach your own security is to share proper information and to enhance effective cooperation with all the players. The main goal

of the workshop is to help increase the awareness and information sharing on network security, trying both to highlight false network security myths (both positive and negative ones) and to effectively apply the "try and fail" and the "lesson learnt" approaches on a worldwide basis, involving both political and technological experts.

The need to organize the workshop was identified by Ms. Luisa Franchina, Director of ISCOM and ENISA Management Board Member: "During the activities of the Italian Ministry of Communications mainly devoted to build up a 'bridge' between Italian public and private sectors, we realized that the information sharing 'best practice' is indeed a key point to fully manage political challenges in the network security field, and that this information sharing must be effectively extended, as far as possible, on a worldwide basis. The most important 'added value' that we experienced in our job is that we have to share not only fully positive experience but also partly negative ones. This process greatly enhances the interaction and the confidence between political and technical decision makers, resulting in more effective strategic choices".

The important results of the aforementioned Italian information sharing activities are summarized in three published guidelines jointly developed by about 50 public and private organizations. These first three guidelines deal with risk analysis methodologies, communications network quality of service and network security in CIIP (Critical Information Infrastructure Protection), respectively. At present they are available in Italian only at www.iscom.gov.it. They will be translated into English and will be officially presented during the workshop.

Stating the success of the Italian information sharing approach, the same organizations that developed the first three ones asked for four new guidelines that, at present, are in an advanced status of development.

Ms Luisa Franchina, on behalf of the Ministry of Communications and FUB, is delighted to host this workshop together with Mr. Andrea Pirotti and the team at ENISA. All parties expect a great exchange of ideas and experiences, ensured by the high profile of the international participants in attendance.

We look forward to welcoming all of you to the beautiful city of Rome.

For further information and for the workshop agenda please contact segreteria.conv@comunicazioni.it |

SECURE 2005 Conference Security – Who is Responsible?

25-26 October 2005

NASK and its CERT Polska affiliate, with the official support of ENISA and the honorary patronage of the Minister of Science and Information Society Technologies of Poland are organizing the 9th conference of the "SECURE" cycle dedicated to network and ICT systems security.

SECURE is a conference propagating knowledge on security of networks and computer systems, dating back to 1997 and holds a reputation as the most important event of its kind in Poland. The SECURE 2005 agenda is based on the knowledge and experience of CERT Polska, other response teams and a group of various computer security experts. Moreover, the agenda includes a number of presentations selected in this year's call for papers. ENISA is taking an active, essential role in this event and is preparing a part of the presentations.

Objective of the conference

The main objective is an attempt to define the roles and responsibilities of manufacturers, operators and Internet users for IT security in view of growing threats from underground elements in the network.

Main topics of the conference

With the growth and popularization of new data transmission technologies, such as wireless or peer-to-peer networks, and given the indisputable strength of the underground economy, the canon of security worked-out for years is merely a protection against certain types of attacks and threats. Paradoxically, solutions such as firewalls, anti-virus software or intrusion detection systems are used almost everywhere, yet almost everywhere users have to face hacks, virus invasions and attacks on a large scale.

It has been repeated for years that with technology only, the enormous wave of attacks, spam and other form of illegal network use cannot be stopped. Real life experience underscores this observation. So, which direction should we choose in order to influence a breakthrough in the vicious circle of ICT security we are now facing? Who should be concerned with network security, and who should be responsible for its individual aspects? To help us grapple with these questions, the following topics will be addressed during SECURE 2005:

- The role of manufacturers, operators, public administrations and network users in the improvement of IT security
- Practical methods of security improvement developed by organizations dealing with prevention of network threats (CERTs, state administration centers, international institutions, etc.)
- Security of new communication tools such as wireless or peer-to-peer networks
- Criminal activity on the Internet, the breadth of the problem and preventive measures

Within the framework of these topics, detailed issues will be presented concerning the characteristics of threats, their growth, and the level of complexity of legal and organizational aspects of IT security, as well as IT security systems and technologies such as:

- threat detection and response systems (IDS, IPS, honeypots, anomaly detection),
- protection systems for home computers,
- forensics.

The conference will also provide a forum for the discussion of how to respond to network threats and security violations, as well as illegal content (e.g. hotlines) published online.

Target audience of the conference

The conference is addressed mainly to:

- Representatives of governmental and self – governmental institutions
- Company directors
- IT managers
- Specialists responsible for the security of IT systems, networks and databases
- Users of networks and IT systems interested in security issues.

Date and location of the conference

The conference will be held on 25 and 26 October 2005 in Warsaw, Poland.

Contact

www.secure2005.pl

As in the previous conferences of the SECURE cycle, about 200 people will take part in SECURE 2005. And by tradition, the first day of the conference will be accompanied by an evening celebration where awards will be presented for contributing to the building of the information society, with journalists, mass-media coverage and VIPs. The event will take place in one of the new clubs in Warsaw. |

Past ENISA events

ENISA AT GOVCERT.NL IN THE HAGUE

Marco Thorbruegge, Senior Expert CERT cooperation, ENISA.

Computer Emergency Response Teams (CERTs) are something of a fire brigade for the Internet. Like their real life red and yellow counterparts, their main duty is to step in when an incident happens. But while fire brigades rush out to fight a fire and rescue victims, CERTS have a bit more of a behind the scenes role; CERTs combat to mitigate the effects of Internet attacks like worms or denial-of-service and they enable the victims to quickly recover from those incidents.

This was also the main task for the very first CERT, the CERT Coordination Centre (CERT/CC), established back in 1988 at the Carnegie Mellon University in Pittsburgh. The establishment took place as a response to the very first automated Internet attack, the so called Morris worm. Since then, a steadily growing number of CERTs face ever changing challenges to make the Internet a safer place. To be able to protect their constituencies better, CERTs evolved from solely reactive institutions into more complete protection facilities. Indeed, today's CERTS also provide preventive services like warning and alarming about new threats, security education, and much more.

Very early on, the CERTs realized that only through co-operation, information sharing and covering as much of the Internet as possible would CERTs be able to fulfill those tasks and to fully protect users. This led to self organization of CERTs and to the creation of entities like the European Government CERT group (EGC) or the international umbrella organization for CERTs, FIRST.

A long time member of the European and international CERT-community is GOVCERT.NL, the Computer Emergency Response Team for the Dutch Government. The annual GOVCERT.NL security symposium in The Hague brings together every year government representatives from Asia-Pacific, Northern America and Europe. In 2005 this event was organized in association with ENISA, and as in 2004 the Executive Director, Mr. Andrea Pirotti, was kindly invited to deliver a keynote. Joining him at the conference was a delegation of staff who had just established themselves in Heraklion, Crete a few days earlier.

> "Only through co-operation, information sharing, and covering as much of the Internet as possible will CERTs be able to fully protect users"

Mr. Pirotti opened his keynote with some stories related to the establishment process on Crete. To set the tone for the next two days and the discussions moderated by the Head of Department for Cooperation and Support, Ronald De Bruin, Mr. Pirotti raised four questions concerning the future of computer and network security:

- Which are the tools to be used to reach the goal of making the Internet a safer place?
- What will be tomorrow's questions about computer security, asked 2 to 3 years from now?
- What can ENISA do to help the Member States to set up CERTs?
- What can ENISA do to facilitate cooperation between CERTs?

These were the questions to be answered in the ENISA workshops to take place on the two days of the symposium.

The first day covered Mr. Pirotti's question: what can ENISA do to help Member States to set up CERTs. To prepare the discussion, ENISA invited three speakers to give presentations about provisions in their field of interest.

Peter Burnett from the UK National Infrastructure Security Co-ordination Centre (NISCC) presented the WARP idea. WARPs (Warning, Advice and Reporting Points) are set up by a community of people sharing the same needs for information security and shall stimulate better communication of alerts and warnings, improve awareness and encourage incident reporting. Designed as a user friendly and low priced solution, a WARP can cover groups of Internet users, for whom a complete CERT would be overkill.

To discourage the widespread opinion that CERTs have to be big and expensive to be successful, Henk Bronk from the hosting GOVCERT.NL presented the 'CERT-in-a-box' and 'Alerting service-in-a-Box' concepts. These projects shall preserve the lessons learned from setting up GOVCERT.NL and 'De Waarschuwingsdienst', the Dutch National

Alerting Service. They also aim at helping others starting a CERT or just an alerting service by getting them up to speed faster and taking the benefits and not making the same mistakes again.

Both NISCC's and GOVCERT.NL's concepts were subsequently analyzed and compared to each other by Andrew Cormack, Chief Security Advisor of UKERNA, the United Kingdom Education and Research Networking Association. His aim was to find areas where CERTs and WARPs can gain benefit by working together, like for example by information sharing.

The following discussion about the initial question was followed by an attentive audience, and the results comprise an overview of the current situation and ENISA's potential role. The coverage of relevant security services provided by CERTs and similar facilities in Europe is insufficient, this is the unanimous opinion of the audience. The coverage should be improved bottom-up, starting with a basic level of protection. Therefore ENISA could provide an overview of existing CERT facilities and services.

This inventory, on the one hand, is considered useful for new teams to find their way, and on the other hand it can help ENISA to locate further gaps in the coverage of the European Internet with CERT-services. ENISA should work on filling these gaps by promoting best practices for setting up CERTs and, as a first practical step, ENISA should facilitate trainings on the setting up of CERTs and similar facilities.

The second day addressed another of the questions from the keynote: what can ENISA do to facilitate cooperation between CERTs. Again experienced speakers where invited to foster the discussion. Klaus-Peter Kossakowski, founder of the well known DFN-CERT, the CERT for the German research network, presented his ideas about security management cycles and the gaps within to be filled by ENISA. At the moment a fraction of the CERT-community makes an effort to redefine security processes and CERT-involvement, which leads to a shift in focus from the facilities like CERTs and WARPs to the services they provide.

Graham Ingram, general manager of The University of Queensland-based AusCERT, gave a presentation about APCERT, a coalition of CERTs from 13 economies across the Asia Pacific region. APCERT was initiated in 2001 and, at the moment, affiliated fifteen Teams as a full member. APCERTs main goal is the facilitation of co-operation, education and accreditation.

Again a very fruitful discussion took place afterwards and produced clearer visions for ENISA's future role in facilitating CERT cooperation in Europe. No one questioned that the level of co-operation between CERTs in Europe can be improved. ENISA should find possibilities to promote best practices in that field. All participants also agreed that one of ENISA's main tasks should be to close the gap between the policy makers and the operational CERT community and to facilitate the communication between them.

Thanks to GOVCERT.NL, who arranged the symposium in a very professional way in all respects, this event can be considered an overall success and produced valuable insight into the needs of the stakeholders and the gaps to be filled by ENISA in the CERT context.

ENISA already had identified CERTs as a vital part of the network security infrastructure. The event in The Hague strengthened the opinion that one of ENISAs tasks is to promote best practices for setting up new CERTs and enhancing the co-operation between them, and that ENISA shall encourage and facilitate the work of the relevant co-operation organizations.

ENISA staff will continue to build up its own expertise in all fields of computer and network security and to develop a vision on how ENISA can add value through a continuous dialogue with industry and CERT community. Thanks to the GOVCERT.NL security symposium this vision has become clearer. |

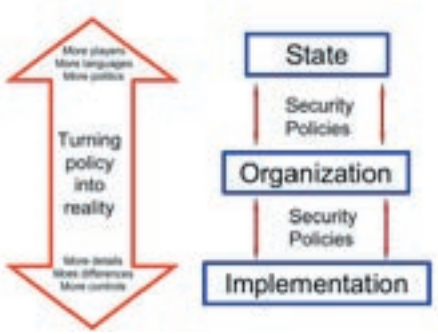
From our Own Experts

Where do organizational and technical security policies stand in the real world?

Carsten Casper, Senior Expert Network Security Policy, ENISA

Everybody knows what a security policy is. Unfortunately, not everybody means the same thing when talking about security policies. Is it the way a government designs laws for the secure life of its people? Is it the 200-page handbook that companies have written over the past ten years, outlining why information security is important, how long a password should be and why you need antivirus software? Or is it the way you configure your firewall, which is actually more often directly implemented in the system rather than documented in a written policy?

At the end of the day, it's a bit of all of this. "Policy" comes from "poli", the old Greek word for town, and policies are the rules that a town - or any other group - gives itself to make living together more reliable, secure, transparent and fair for everybody. In information security, it starts with the



"big picture", when a government paves the way for future development - or reacts to a recent crisis -, giving its opinion on how various entities in a country and across borders should deal with network and information security. Then, a company, an organization, or a public entity adjusts this general thinking to its own needs and capabilities. It takes into account economic and technological trends, balancing a number of risks against the values that information process-

ing has for this entity. Finally, organizational, procedural and technical controls are used to turn this more strategic way of thinking into reality.

One of the problems with this approach is that in today's technology world, everything is connected. The small Lithuanian company with only 50 people has to follow the rules of a number of EU Directives transposed into national law, using advanced security technology from a tiny start-up company in Silicon Valley, thousands of miles away. It is very likely that somewhere on the way between Brussels, Vilnius, and Palo Alto, communication will suffer. What the first one wants, is not what the second one implements with the third one's technology. Here lies the core of today's information security conundrum. Whether the question is how to best fight spam, how to evaluate the impact of a security breach, or why an intrusion detection system is adequate to "protect against unauthorized access" - exchanging such information is full of misunderstandings. Not speaking the same language is a source of mistrust.

Of course it is impossible that everybody uses the same language. Requirements are different, so people have developed different jargons for communicating. Within each group of people, a specific vocabulary helps communicate more efficiently. A group of executive directors is only interested in strategic issues of information security, while Windows and UNIX administrators need to discuss technical details. Most users have only a limited knowledge of computer security, so they have to be addressed in a language they understand. When designing a security policy that outlines rules for a specific group, ideally each group gets its own customized policy. Yet all of these policies work together. Output of one policy is input for another. What we need most are ways of bridging the gap between them, of translating the jargon of one group into the language of the other.

In addition, the question still is: what is a good policy and how do I recognize a bad one? Which policy was already successful? How do I know that it was successful? Consequently, people start asking about best practices. They know that they are not the first ones facing Internet risks and they do not want to reinvent the wheel. So why not simply copy what others have done? Well, what works best for one group or organization, might not work at all for another one. So there are best practices for specific industries, systems, user populations, age groups etc. Still, there are also some commonalities. A laptop requires very similar controls, whether it is part of a government, company, university or home network. Of course it depends on the level of security that an organization requires, but even within the area of government, university, company etc. there are different levels - while a low level in government and a low level in a company might actually be treated equally. So the ideal way of defining organizational and technical guidance is to compile a (arguably quite long) list of detailed information security controls, combine relevant ones as information security policies for specific purposes, and package a number of such policies into information security best practice guides for specific target groups. |

From the Member States

Creating A Secure Information Society: The Lithuanian Way

In pursuit of IT security coordination in governmental institutions and understanding the difficulties that governmental institutions confront in striving to implement IT security requirements and solutions, the Lithuanian Ministry of Interior prepared a PHARE financed project "Technical assistance for strengthening capacities of authorities dealing with IT and electronic data security". The main objective of this project is to ensure that IT security in Lithuania corresponds to EU requirements and operates effectively.

One of the main tasks of the project is to raise IT security awareness among government officials. To that end, a unique IT security training program, consisting not only of training material and training courses but also an IT security distant learning system, was created. Security officers of the main governmental institutions have been trained using this program, and this year more than 200 government officials will be taught IT security. And this is only the starting stage of using the distant learning system; indeed all governmental officials will be taught IT security in the near future.

Creation and implementation of such a unique IT security training program makes Lithuania a leading country in IT security awareness raising among governmental institutions in Eastern Europe.

There are other important tasks for this project. These include the evaluation of the existing situation in the field of IT security and the revision of existing legal documents regulating the sphere of IT security so that they are in line with EU requirements and international standards. As well, the project will see the preparation of IT security requirements that will be applied to different information systems classification levels and the creation of a risk analysis manual which will help governmental institutions to effectively identify and manage security threats and vulnerabilities.

Undoubtedly IT security is a continuous process and cannot be finished with just one project. To that end, the Lithuanian Ministry of Interior is preparing a new IT security strategy. This will ensure the continuity of the project and also a more precise coordination of IT security, close cooperation between private and governmental sectors and map out the creation of a secure Information Society in Lithuania.

For more information and specifications please contact:

Torvaldas Česnulevičius

Head of Security Supervision Division
Information Policy Department
Ministry of Interior
+370 5 2717374

torvaldas.cesnulevicius@vrm.lt |

Don't forget about the upcoming "Readiness for Handling Network and Information Security Incidents" Conference in Vilnius on Nov 23rd-24th! www.securityconference.rrt.lt

Developments in Germany

IT Security Certification for German Health Card

Bernd Kowalski

The Federal Ministry for Health and Social Security (BMGS) has started one of Germany's largest and most innovative IT projects with the introduction of the electronic health card, which is planned for 2006. 80 million insured people will be given the new health card; 21,000 chemists, 123,000 practicing doctors, 65,000 dentists, 2200 hospitals and just under 270 health insurance companies will be connected to each other via the new telematic infrastructure.

The electronic health card must be technically suitable to provide authentication, encryption and electronic signature functionality in order to ensure that the sensitive data is subject to maximum security. It will be possible for the insured person to save specific medical information and to make this available to a doctor or chemist as required. However the insured person remains in control of the data that has been saved and the way it is processed. Smart cards are considered to be a key technology for simple, easy access to personalised application services.

Questions relating to data protection and IT security play a key role in the introduction of the electronic health card. Consequently, the most important components of the system must be subject to security evaluation and certification. This creates trust in the information technology because the complexity of the IT systems only permits an assessment of its security through systematic evaluation.

For this, the Federal Office for Information Security (BSI) has developed protection profiles using common criteria for the electronic health card, the medical career IDs, the secure module card and the connector that controls the information flow between the telematic infrastructure and the primary systems. Only such products that have been subject to IT security certification on the basis of these protection profiles will be authorised for use. Thus, the most important components of the system are subject to an IT security check.

As a result, Germany is assuming a pioneering role in Europe. The aim is to encourage certification in other countries on the basis of these protection profiles. Manufacturer-certified products, e.g. smart card manufacturers, can then offer their certified products for cross-border, international recognition on the basis of the CCRA Treaty http://www.commoncriteriaportal.org/public/expert. Thus, these protection profiles form an excellent basis for implementing IT security aspects in health services across Europe and at the same time will support the further opening of the European health market.

BSI enjoys a high international reputation regarding its certification activity. This is expressed both in the constantly growing number of certification customers and its active role in various common criteria committees. In this context, the BSI contributes its 17 years of experience toward developing criteria and evaluating the most varied product classes in the further development of the common criteria.

Bernd Kowalski is head of Department at the Federal Office for Information Security (BSI). |

BSI publishes 2004 annual report

The BSI has published its 2004 report, which covers all the key events in the reporting period. The report handles such classic issues as malware and certification as well as security protection, e-government and future technologies such as RFID and biometrics. The English version of the annual report can be downloaded free of charge from http://www.bsi.bund.de/literat/jahresbericht/jahresbericht_2004/index.htm. |

BSI's BOSS program provides free software for network-wide security testing

BSI provides free software to check network systems. The BSI Open Source Security Suite (BOSS) is an easy-to-use Nessus-based security scanner with German language GUI. BOSS can not only check the security of any computer in a network, it can also control and carry out local checks on GNU/Linux computers with various security tools centrally. The software can be downloaded free of charge from the BSI website at http://www.bsi.bund.de/produkte/boss/index.htm. |

BSI Report on IT Security in Germany

Europe, and with it also Germany, is already far advanced on the way to the information society. Today, information technology is part of the national infrastructure without which private households and public life would come to a standstill.

Recently the Federal Office for Information Security (BSI) published the first report on IT security in Germany.

The report clarifies the seriousness of the situation: in the second half of 2004 over 1,400 new IT vulnerabilities were uncovered – an increase of 13% over the first half of the year. The situation is even more dramatic for malicious software (malware). Over 7,300 new worm and virus variants were registered in the same period. This corresponds to an increase of around two thirds over the previous six months. Trojan horses were responsible for one third of the 50 most frequent malware in the second half of 2004. The share of spam messages is now between 60 and 90% of all e-mail traffic. And the increasing number of phishing attacks also endanger Internet security.

It is very clear that threats due to malware in the form of computer viruses, worms and spam will continue to increase in the future. New transmission technologies such as voice over IP (VOIP), wireless LAN and mobile phone communication have already been targeted for attack and will be more heavily threatened in future.

And the attacks are becoming faster. The period between a weakness becoming evident and its exploitation is currently 6.4 days and will continue to shrink – until we see zero-day exploits. There is also a trend towards Internet criminality becoming more professional and commercialised. Instead of isolated computer hackers, those behind the selective attacks are increasingly members of organised crime.

The protective measures that already exist are barely adequate today. Only around half of those responsible for IT in companies have a written strategy to protect their information technology. For example, in spite of the large volume of spam emails, anti-spam measures are not implemented across the board in companies and public administrations in Germany. At least 9% of organisations are subject to the flood of spam without any protection at all. Existing protective measures therefore have to be improved further for adequate protection. The BSI, as the central German IT security agency, is well prepared for the challenges. But it goes without saying that not only the BSI needs to be active – everybody does. Everybody has to co-operate — regardless of whether they are system administrators or private users. Optimum protection for information technology is only possible if all social groups tackle the issue.

Acknowledging these new challenges, Germany regards IT security as an integral part of national security policy. This is why the Federal Government adopted the National Plan for Information Infrastructure Protection (NPSI) in July 2005.

This plan sets out aims and measures to enhance co-operation between the state and the business sector as an overall strategy to ensure security in the field of information technology in our country. The National Plan is addressed to all societal groups, because comprehensive protection of our IT systems is possible only with joint co-ordinated efforts.

The three strategic objectives of the National Plan for Information Infrastructure Protection are

- prevention: protecting information infrastructures adequately;
- preparedness: responding effectively to IT security incidents;
- sustainability: enhancing German competence in IT security/ setting international standards.

Many risks associated with the use of information technology can be reduced or even controlled by preventive measures. The prevention objectives of the NPSI include:

- greater public awareness of risks associated with IT use,
- greater use of trustworthy information technology and reliable encryption products,
- clear definition of responsibilities for IT security in companies and public authorities.

However, it is impossible to completely rule out IT security incidents, no matter how good the defences are. The response objectives of the NPSI include:

- establishing a National IT Crisis Response Centre at the Federal Office for Information Security (BSI),
- initiating the creation of an international watch and warning network,
- analysing and evaluating IT security incidents in the IT Crisis Response Centre.

To ensure long-term protection of information infrastructures in Germany, the National Plan for Information Infrastructure Protection provides for the following action:

- encouraging the development of trustworthy and reliable information technology,
- teaching IT security skills nationwide in schools and professional training centres,
- supporting national basic research and participating in international research projects.

The Federal Government has already begun drafting an Implementation Plan for the Federal Administration (Umsetzungsplan Bund) and a CIP Implementation Plan (Umsetzungsplan KRITIS). The Umsetzungsplan Bund will set out IT security standards for the federal administration and thus supplement the Federal Government's IT strategy.

The BSI report on IT security in Germany can be downloaded from http://www.bsi.ivbb.bund.de/literat/lagebericht/index.htm. (German version)

The National Plan for Information Infrastructure Protection (NPSI) can be downloaded from the BMI website at http://www.bmi.bund.de

Edited by: Boaz Gelbord.
boaz.gelbord@enisa.eu.int

More about ENISA

For the latest information about ENISA, check out our website at www.enisa.eu.int.

Publications Office
Publications.eu.int