ENISA Quarterly

enisa European Network and information Security Agency

IN THIS EDITION

Trusted Computing

Vol. 3, No. 3, Jul-Sep 2007

As our expert, Giles Hogben, stated: "Social Networking is like a 'digital cocktail party'. You may enjoy meeting many people, but you also want to avoid a digital hangover."

In introducing this issue of ENISA Quarterly I would like to focus on a trend which is attracting considerable media attention.

Social Networking (SN) has emerged as one of the most successful social and technological phenomena of the 21st century. User numbers have increased rapidly since the first social networks emerged in 2004. MySpace and Facebook, for example, are widely visited websites with hit rates that are increasing rapidly.

As with many fast-growing technologies, security has not been the first concern. SN websites create a feeling of being amongst friends. Millions of young people disclose intimate details of their personal lives but very few realise, for example, that a potential employer might one day discover these details. The risks of identity theft, extortion and spear-phishing are greatly increased due to the level of personal information that users readily provide with little or no protection. New technologies like on-line face recognition and Internet archives also make it very difficult to hide or remove private information once it has been posted on-line.

So how do you protect your on-line social identity? Many SN providers already take action, e.g., by filtering out zip codes, by applying abuse-reporting buttons, or through moderation tools. But, in dealing with this, we need to be aware that, even with strong privacy protection features in place, the pressures on businesses and users often pull in the opposite direction. Even though users do not pay directly, there is clearly a strong business case for having access to user profiles. Socially as well as economically, the pressure is on against privacy. Policy-makers need to find ways to reduce the incentives that destroy privacy, for example by creating portable social networks, where data is controlled by the users themselves and by allowing them to inflate the numbers of friends attributed to them, thereby removing the incentive to accept random 'friend' requests. Awareness and education are also key to the solution. According to a recent study, users of Facebook were more careful after answering a survey about privacy than they were beforehand.

ENISA gathered SN experts at a recent workshop to discuss relevant security issues

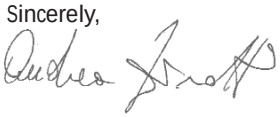
ISSN1830-3609

and to make recommendations for addressing security in SNs. The Agency also plans to publish a position paper on this later this autumn. The aim is to benefit both users and providers of social media, by encouraging a safer environment on SN websites and making both professional and social networks safer platforms for interaction.

Now onto another topic – ENISA recently organised the first meeting with the new members of the Permanent Stakeholders' Group (PSG) in Athens. The new PSG met with many ENISA technical experts and began by reviewing the contributions to the 2008 Work Programme. The input of all stakeholders is extremely valuable and very much appreciated.

Finally, it was a pleasure to meet some of you at the 2007 ISSE Conference, which this year took place in Poland. This was another highlight in ENISA's growing list of successful joint events. We are convinced that this conference is an important meeting venue for non-commercial, strategic discussion on the future of Network and Information Security.

Sincerely,



Andrea Pirotti
Executive Director, ENISA

A Word from the Editor

Do you trust your computer? Or, more generally, do you have trust in computing? The usual answer to these questions would probably be no. This is a deficiency that the concept of Trusted Computing (TC) seeks to rectify.

TC is a set of open standards that define a technology which aims to enhance security by using the transitive properties of trust. That means that if one trusts X and X trusts Y, then one must also trust Y. In this way, TC proposes to have a closed hardware component which is the root of trust based on which one can then trust all other components and systems, even remote ones. There are several different interpretations of trust. The concept of TC is based on the interpretation that having trust in a specific component or a system means that "it will behave in a particular manner for a specific purpose".

Many vendors nowadays base all their efforts to provide security on building trusted systems and infrastructures. This shows that TC has gained the trust of the vendors as a tool for ensuring trusted and secure infrastructures in the future.

But TC is a new technology and as such brings new risks and concerns. There are major issues, especially related to privacy. One big worry is the potential loss of anonymity and the threat of unwanted surveillance and even control, since the hardware root of trust is unique and can be identified, even from a remote location, and therefore an attacker could use this key to track the history of the activities of a system that is based on that root. Another important question is whether actual implementations are compliant with the defined standards, since at present there is no formal test to prove compliance. So implementations and deployments could be prone to errors, making them vulnerable to attackers.

Is global deployment of TC a panacea for all security problems? The answer is not yet clear – probably we will never know. But what we can definitely say about TC is that it is an important initiative with a valid basis and strong support from industry which, with appropriate attention from industry and most importantly from policy-makers to counter the various risks and concerns, especially relating to privacy, could lead to more secure computing.

In this issue, we welcome a number of articles on TC. Markus Linnemann and Norbert Pohlmann, a member of our Permanent Stakeholders' Group (PSG), provide an easy to follow introduction to TC, comparing it with the airbags of a car. Claire Vishik, also a member of the PSG, and David Hoffman provide a more in depth description of TC, explaining also the motivation behind its introduction. Peter Lipp et al, members of the Trusted Computing Group of the Institute for Applied Information Processing (IAIK) at the Graz University of Technology, introduce OpenTC, a research project co-funded by the European Commission that is addressing a number of open issues of TC. Finally, Marion Weber and Jörn-Uwe Heyder provide a report on a recent Workshop on TC that was organised by the German authorities, which highlights the important role that public authorities and policy-makers have in ensuring the smooth introduction of TC.

Our own experts report on recent activities and events: the ENISA and CERT/CC Workshop on Mitigation of Massive Cyber Attacks and the third ENISA Awareness Raising Workshop that was hosted by Portugal.

We have also received some interesting articles from the open call for contributions. Christian Wernberg-Tougaard and Bjørn Bedsted present a report from the Danish expert group on future IT security threats; Andreas Wedner describes the objectives of the Meridian Conference on Co-operating to Protect Critical Information Infrastructures; while Erika Hersaeus and Helena Bäckström describe their experience supervising the Swedish National Top-Level Domain, .se.

I am very happy that in this issue we also introduce a new regular column which we hope will stimulate food for thought in an informal, perhaps even cynical way. In the first of these joint contributions by a member of our Management Board, Pernilla Skantze, and a member of the PSG, Nick Coleman, they look at the phenomenon of Social Networking, to complement our Executive Director's foreword.

We constantly seek means to improve the level of quality of our magazine. To that end, we have decided to implement a new procedure for the submission of articles. In the future we will require submission of a full article rather than simply an abstract, prior to the evaluation and selection process. In this way we will be able to more accurately judge the proposals we receive, which are constantly increasing in numbers. Please continue to send us your articles. Forthcoming special issues are planned in the areas of

- Secure Software
- Resilience of Networked Infrastructures.

Last but not least, the ENISA Quarterly distribution list is now fully automated with a web interface. In order to subscribe you need first to register with the ENISA Community at: www.enisa.europa.eu/eq/.

Enjoy reading this issue of ENISA Quarterly!

Sincerely,

Panos Trimintzios
Editor-in-Chief, ENISA Quarterly

Dr. Panagiotis Trimintzios is an Expert at ENISA responsible for Relations with Industry, Academia and International Organisations.

From the World of Security – A Word from the Experts

An Airbag for the Operating System – A Pipedream?

Markus Linnemann and Norbert Pohlmann

We have all become accustomed to fastening our seatbelts in the car, moving the seat to the right position and adjusting the mirrors correctly, but the most important safety features are the small technical refinements installed in the vehicle: the anti-lock braking system (ABS), electronic stability programme (ESP) and the airbags. As soon as a situation becomes dangerous, these safety systems are activated and protect us and our car against serious damage or injury. Why are there not any similar safety mechanisms for computer operating systems which we could also use on a daily basis as we do with cars?

Safety in IT versus safety in cars

There are many security tools which help us to detect and protect ourselves against harmful software. However, virus scanners and firewalls have to be properly configured and maintained. They do not therefore offer fully automated security. While it is rare for motorists to be attacked directly or intentionally put into dangerous situations, repeated and targeted attacks on all computer systems that are connected to the Internet occur increasingly often in the IT world. Currently it takes an average of approximately six minutes until an unprotected computer system is infected with malware.

New developments in the IT world also occur several times faster than in the automobile industry. The complexity of established operating systems is increasing continually in order to meet the rising demands of the information and knowledge society. However, their proneness to errors also increases disproportionately with this complexity. This fact is underlined by the large number of patches and security updates which are issued daily.

It is always easy to recognise one's own car by its colour, make, shape and number plate, with the key being the ultimate means of authentication of a vehicle's driver. In the IT world we use passwords or security tokens for our authentication with respect to a computer system, but a computer system does not provide any authentication of itself with respect to us. By extending the analogy, this is like saying that we are not able to determine whether we are sitting in the right car or whether the car will brake when we press the brake pedal.

The concept of Trusted Computing

Trusted Computing is a security technology being developed by an industrial consortium with more than 160 international members. The output of this consortium is a number of open specifications whose fundamental aim is to make IT products and services more trustworthy. The intention is to improve the security of distributed applications in a manner that is economically viable, i.e., there should be no massive changes to existing hardware or software. The main idea is the use of a hardware component, the Trusted Platform Module (TPM), that cannot be manipulated. TPM could then be used as the core of trust for systems and software, and therefore software-based attacks could be counteracted.

The open specification of the Trusted Platform Module has been implemented in the products of many manufacturers and is currently integrated into over 60 million computer systems. By the end of 2008 it is hoped that more than 200 million of these hardware components will have been supplied.

How it works

This security module acts as a trusted anchor in a computer system, the so called 'root of trust'. Starting with the booting process of a computer system, all hardware elements and software programmes (BIOS, operating system, application programmes etc.) are measured with the help of hash functions and their signatures are stored in the Platform Configuration Register of the TPM. Consequently the system configuration of the computer system can be measured in full and is therefore also verifiable.

In the car analogy, this is comparable with an inspector who records the entire assembly process of a car and subsequently is able to show the 'integrity' of the vehicle on the basis of a certified list of control numbers, e.g., a chassis number, for all the parts. If a car part is replaced, the car is no longer in its original condition and is no longer trustworthy according to the list. This only monitors the state of a system in relation to a reference. It does not mean in general that the new state of the system is insecure, but it is possible. By analogy this is precisely the method of system configuration verification offered by the TPM. Using these security functions it is possible for computer systems to verify the status of their system configuration to a user or other computer systems. This procedure is known as 'attestation'.

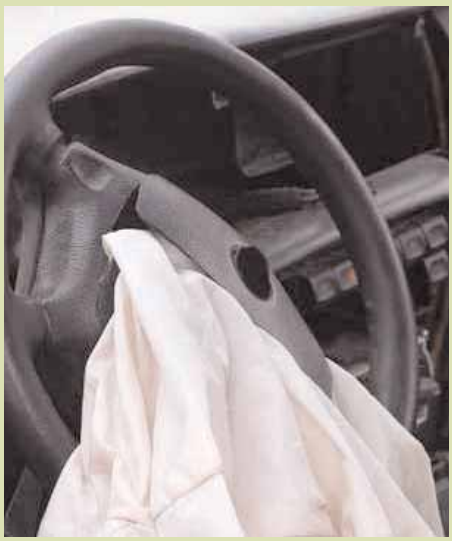
Moreover, the TPM offers the opportunity of encrypting data and storing them confidentially. In this process the data are tied cryptographically to the system configuration during encryption. This procedure is known as 'sealing', and guarantees that sealed data can only be accessed if the computer system is in a known state (system configuration). In the figurative sense it is therefore possible to determine precisely whether, for example, the braking system has been tampered with or not and therefore whether it is fully functional.

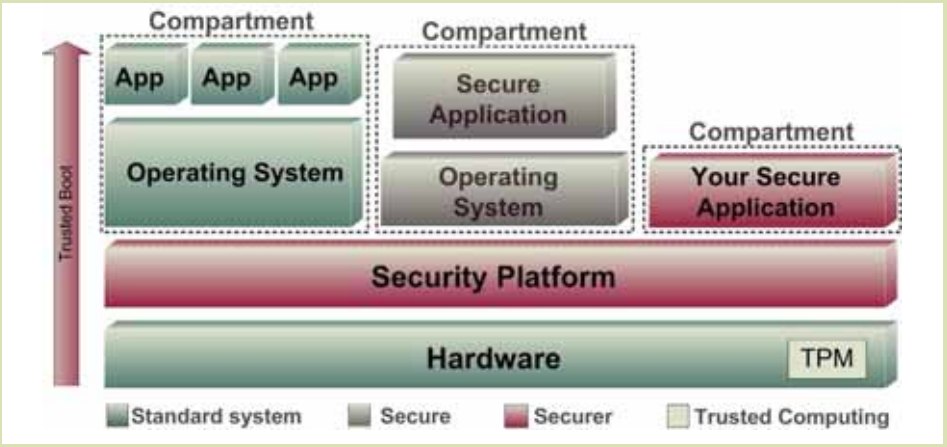
Security platform as part of the Trusted Computing concept

Up to now Trusted Computing applications have only been tools which can be used to generate more trustworthiness in computer systems. However, the term Trusted Computing stands not only for security chips, such as the TPM. It is an umbrella term for all functions which can generate security using new methods. A TPM module alone does not bring greater security. This is a passive security module that offers security services. In order to be able to use this in a confidential manner, a security platform is required which guarantees this property. In the analogy of the car it is the employee who monitors the construction of the car, together with the test engineers who check the authenticity and functional efficiency. In technology it is an operating system-type security platform.

Current operating systems cannot be used as a security platform, as they are easily compromised and could harbour viruses and Trojan horses which would simulate a trustworthy status which does not correspond to the actual status. A security platform therefore positions itself above the hardware and below the conventional operating system. Its task is to be as immune as possible to attacks and to check security-critical processes from this situation.

In order to be able to fulfil these specifications, a security platform should consist of a very small code base and therefore be far less complex than established operating systems. As a result of minimalisation, the error probability is considerably smaller and the trustworthiness higher. By means of virtualisation techniques, a security platform is in the position to execute several applications and/or operating systems in parallel. It is therefore possible to execute individual secure applications in parallel in so-called compartments completely isolated from the established operating system.





System architecture with the Turaya security platform

The trustworthiness of the secure applications can be verified by the measurement opportunities offered by the TPM. There is therefore no problem if the established operating system has been compromised by malware, as all security-critical processes can be executed outside the operating system by secure applications. The compartments can contain either exclusively secure applications that have been adapted for the security platform, or a clean operating system with standard applications. In the latter case the operating system is then measured together with the application in order to be able to demonstrate the intactness, i.e., the integrity, at all times (see diagram above).

A security platform in combination with Trusted Computing technology offers a broad spectrum of design possibilities for trusted applications. This makes possible end-user systems which can safely administer and store data. Harmful software such as Trojan horses and viruses are simply isolated from security-relevant data. Server and client systems can be reliably authenticated – for example, during on-line banking the bank's computer can be identified at all times and the bank data processed confidentially.

The airbag for operating systems for more trustworthiness

The EMSCB (European Multilateral Secure Computing Base) is a project in which several universities and IT security firms are involved that aims at developing a trustworthy computing platform with open standards to solve many of the security problems of conventional platforms. Turaya is the main system that provides a trustworthy, fair and open security platform based on Trusted Computing technology. It also offers the opportunity to enforce rules and regulations (policy enforcement), thus providing new and trustworthy possibilities for enterprise rights management. The processing of classified documents on different computer systems with different policies becomes possible. For example, documents can be viewed and printed on certain computer systems, while on others they can only be viewed.

The main objective of the project is to create a security platform with an open architecture and interfaces that serve as a basis for trustworthy IT systems. New and innovative business models are made possible by the provision of the security platform for PCs, PDAs, cell phones and embedded systems.

Further partnerships are welcomed with those who wish to build on the Turaya security platform in order to provide new inspiration from Europe in the field of IT security. Further information on the project is available at www.emscb.org.

The 'airbag' for the operating system is therefore no pipedream. The developments in Trusted Computing are enabling a large leap to more security in IT, in the same way that the airbag did for the car. The car airbag is being permanently refined and today offers side protection, head protection and protection for motorcyclists. We believe that Trusted Computing technology, in combination with a security platform based on an open architecture and open interfaces, has the potential to solve a number of today's security problems as simply as an airbag.

Markus Linnemann (markus.linnemann@internet-sicherheit.de) is the Project Manager of the Trusted Computing project at the Institute for Internet Security in the University of Applied Sciences Gelsenkirchen in Germany.

Norbert Pohlmann (norbert.pohlmann@informatik.fh-gelsenkirchen.de) is a Professor at the Institute for Internet Security at the University of Applied Sciences Gelsenkirchen and a member of the Permanent Stakeholders' Group (PSG) established by ENISA.

Devices that can be Trusted

Building a more secure environment for the enterprise without sacrificing privacy

Claire Vishik and David Hoffman

Sophisticated attacks and security breaches can have a devastating impact on organisations and affect millions of computer users around the world. With information crucial to individuals or enterprises almost always available in digital formats in interconnected systems, even less serious attacks can paralyse essential areas of an enterprise's daily operations. Currently available means of protection for networks, computers and data are insufficient. The predominant use of exclusionary models of protection – exemplified by firewalls, intrusion detection tools, access control and similar methods – is becoming less effective with the proliferation of highly mobile networked devices. The diversity of operations spanning multiple networks and thousands of systems, accessed by millions of users, makes it impossible to analyse all of the elements in need of protection, while the high mobility of devices containing confidential information makes them an attractive focus for serious security attacks.

In the fight to protect systems and networks, technologists are at a disadvantage in relation to hackers. The attacker needs to know just one vulnerability to be successful, while technologists have to eliminate *all* weaknesses in order to guarantee security. This is an impossible task. In order to improve security, we need to use a combination of techniques that can help software security tools and secure networks operate with greater efficiency.

In this article we look at recent security trends in enterprise protection, focusing on client protection, that offer one way forward. Trusted Computing can enhance some aspects of personal computer (PC) security, and offers a new approach to privacy-friendly technology development.

Vanishing perimeter and new protection models

In theory, only authorised users and applications can access protected systems and networks, and they are allowed to perform only those functions permitted for the types of accounts that they hold. But, in reality, the picture is not so clear cut.

The notion of a perimeter that separates protected (trusted) organisational networks from public networks has become less strictly defined. In every organisation, most laptops, PDAs or removable storage tools can operate both inside and outside the 'trusted zone'. Enterprise users of these diverse mobile devices freely perform activities inside and outside organisational networks, using internal and external accounts, while customers, contractors and visitors from outside the organisation are often allowed to perform various functions internally. The trusted network bounded by its perimeter needs additional technologies to maintain its trusted status. Building trusted platforms is a step towards the continued integrity of organisational networks.

In addition to a less strict definition of the perimeter, other trends have contributed to the changes in approaches to security in an organisation, such as:

- **Externalisation of security components.** Many organisations have built extensive security infrastructures including Public Key Infrastructures (PKIs), firewalls, intrusion detection systems and identity management systems. Using this infrastructure to enable security in software and sometimes hardware applications has become more widespread. The **centralisation of security functions** is a consequence of the emergence of organisational security infrastructures.

Examples of Centralisation and Standardisation of Security

Area	Approach	Standards	Business Goal
Access Control	Directory, meta directory, Single Sign-On (SSO)	Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML), Liberty Alliance framework	Ensure that user accounts and credentials are up-to-date, protected, regularly audited and available in a uniform format
Credentials management	LDAP, PKI, SSO systems	LDAP, PKI-related standards	Ensure that credentials are protected and managed throughout their lifecycle
Authorisation	Policy management, definition and enforcement systems	Attribute certificates, eXtensible Access Control Markup Language (XACML), Platform for Privacy Preferences Project (P3P)	Ensure that activities of authorised users, applications and devices are well defined in a machine-readable form

- **Use of open standards and increasing reliance on certification.** Open standards are commonly used in security systems to ensure higher levels of interoperability, but the diversity of implementations makes the value of a recognised standard review of a system (i.e., certification or self-certification based on a shared framework) much greater.

The trends listed above apply to a greater degree for networks and server environments. For PC clients or other highly mobile computing devices such as PDAs or smart phones, the means of protection are still limited, although available technologies are commonly used.

PCs can rival servers for the amount of sensitive information they store, and consequently many attacks are directed at networked clients. With greater computing power and practically unlimited storage, a PC today has become a repository of highly confidential information, aggregating data from multiple sources. A breach into a PC may be substantively equivalent to a breach affecting multiple business-critical servers. Yet PCs are lightly protected compared with servers and networks...

Client PCs need higher levels of protection

The annual SCI/FBI Security Survey (http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf) highlights an interesting paradox regarding the state of security in the enterprise: while security tools are commonly deployed, security breaches remain relatively common. 97% of organisations use anti-virus software, 79% have implemented anti-spyware tools, 63% encrypt data in transit and 43% encrypt data at rest, and 80% conduct security audits, yet 52% have experienced security breaches.

Most PCs in an organisation are patched on a regular basis, use relatively up-to-date anti-virus and anti-spyware tools and have a standard more secure operating system (OS) image. However, they do not undergo a rigorous configuration analysis during normal operations. A non-generic Trojan, a customised malicious software package, or an unauthorised user may remain undetected on a PC as long as there is general compliance with the security policies. Even protection against generic threats is not as effective as we would like to believe. Up-to-date virus definitions and patches can be pushed to PC clients without delay, but an end-user can switch off updates if they are inconvenient, or miss them when disconnected from the enterprise network.

Trusted Computing

As the sophistication of software attacks increases ahead of detection techniques, how can we continue to trust our own computer and other devices? How can we ensure that an entity "will behave in a particular manner for a specific purpose"? And what does it mean, in non-technical terms, that a platform is trusted?

Users would trust the platform more if it possessed the following features:

- Hardware-based protection, with the existing software taking advantage of it.
- The ability to recognise when something is wrong and provide some protection when a problem is detected.
- Mechanisms that verify configuration information reported by the platform.

Trusted Computing is a series of open standards developed by the Trusted Computing Group (TCG – www.trustedcomputinggroup.org) with the goal of creating an environment that a user or provider of a service can trust. This trust would be due to additional security features, such as greater scrutiny of unauthorised changes on a device and support for platform authentication. The TCG is an international standards body with more than 150 member companies working together to develop new specifications. The core specification describes the Trusted Platform Module (TPM), a secure chip, typically attached to the motherboard of a PC and consisting of several components including secure storage for encryption keys and integrity measurements, random number and key generators and enablement for secure execution. Additionally, the TPM can help to seal data and secrets at a predefined platform status, closing access if platform measurements detect that it has been compromised.

A TPM also supports attestation that provides information about the security status of a platform. The TCG has defined platform credentials (Endorsement Credentials) to establish that the device has a genuine TPM. By signing this credential, the TPM manufacturer, the original manufacturer of the platform, or an IT organisation make an assertion that a valid TPM with certain properties is installed on a platform. The credential is used to obtain Identity Credentials for domain-based Attestation Identity Keys (AIKs). AIKs are used to sign the 'quote' – a set of confirmed measurements providing proof that a platform is trustworthy. Those interacting with the platform can evaluate the level of trust the platform should be accorded, after making a determination if they trust the entity that signed the Platform Credential and the Privacy Certification Authority (CA) that issued the Identity Credential.

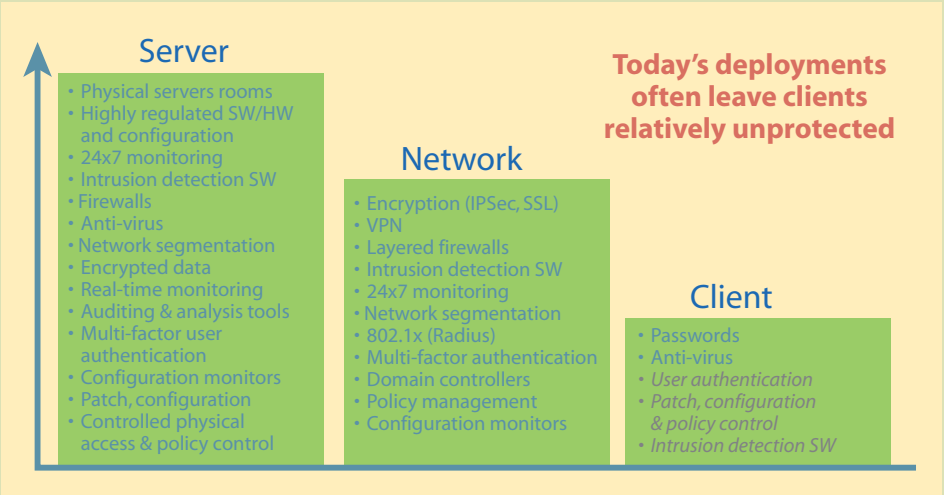
Upholding security while protecting privacy

Different levels of trust are possible in diverse computing environments, with more extensive disclosure of features on a platform that can be proved trustworthy supporting higher levels of trust. However, the more we know about hardware and software elements and accounts on a device, the greater the potential impact on privacy can become.

During the last decade, approaches have been developed allowing technologists to incorporate security and privacy in the design process. While formal methodologies have been created to take security risks into account early in the design process, similar techniques to account for privacy risks have yet to mature. The 'design' of privacy-friendly identifiers, while covering a small subset of privacy-friendly features, is a good illustration of possible approaches to privacy-friendly design because identifiers are pervasive in all systems and protocols.

A better identifier

Privacy-friendly identifiers are designed in a way that makes their links to objects and the individuals they denote more difficult to capture. The table on page 7 illustrates some of these features: a 'better' identifier is dynamic, not linked to identifiable information, can be transferred to a different object and is controlled by the user.



Client Protection versus Server and Network

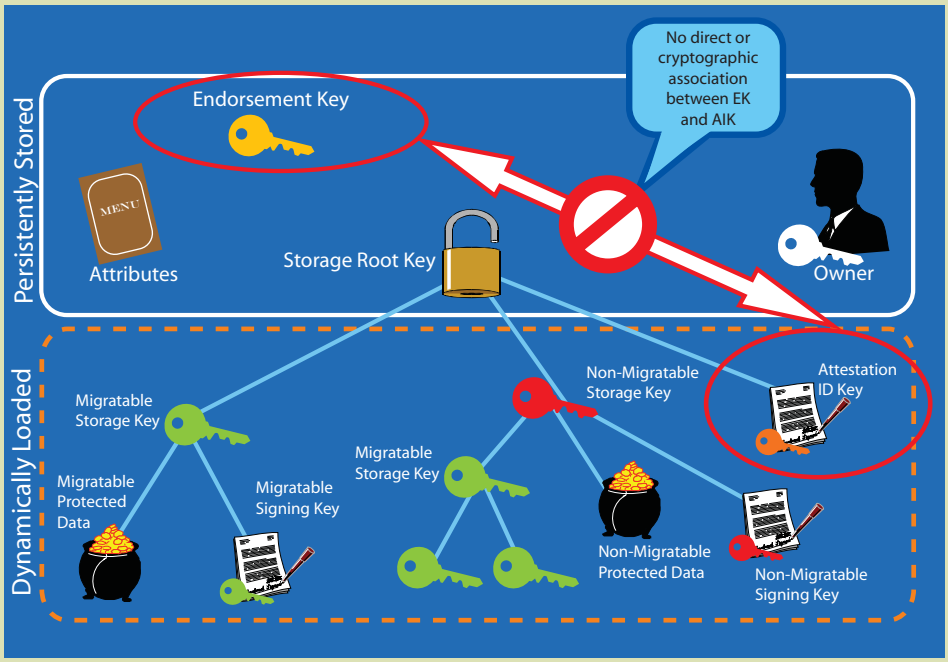
Some features of unique identifiers

Feature	Description	Better Identifier
Ability to identify	Ability of the ID, or its easily obtainable combinations with other information, to reliably identify an individual or an object with sole ownership by an individual	Has no connection with the individual or easily attributable object
Mutability	Frequency of change	Changes very frequently, sometimes used only once
Transferability	Extent to which the identifier can be transferred to a different object or can be applied to a large group of objects	Can be transferred from object to object with ease
Assignability	Ease of passing the object with identifier to other individuals	Can be easily transferred to other individuals or attributable objects
Accessibility	Ease with which the identifier can be accessed	User exercises control over who / what can access the identifier

While incorporating all of these features into all new protocols and systems cannot be expected due to the intrinsic limitations of technology, some of these characteristics have become common, for example, incorporating dynamic identifiers as proxies for static IDs, e.g., TMSI (temporary subscriber ID) represents IMSI (permanent subscriber ID) in some transactions in GSM networks. User or owner control over the security components is becoming a requirement too. TPM-equipped PCs require the owner's authorisation to switch on the TPM. A standard browser asks for permission to display secure and non-secure components on one page. Privacy-friendly identifiers are used in conjunction with other technologies to improve privacy...

In a more complex example, the TPM specification defines the (cryptographic) key hierarchy so that a static identifier (Endorsement Key (EK)) is substituted with domain-oriented keys (Attestation Identity Keys) in user protocols, and there is no cryptographic association between the EK and the AIKs...

To achieve greater privacy, it is possible, even for very secure environments, to substitute identification with verification that an ID belongs to a trusted group and therefore can be authorised. In the TCG framework, the Direct Anonymous Attestation (DAA) protocol can ensure complete anonymity of transactions while convincing a verifier that a trusted hardware module is used. Today's technology can support enhanced privacy by improving identifiers and verification / authentication protocols.



TPM Key Hierarchy

Conclusion

Security technologies are commonly used in organisations, and security vulnerabilities are better analysed and understood now than ever before, but a relatively high incidence of security breaches remains.

Centralisation and standardisation of security systems play a positive role in improving overall security. Yet these methods are not always sufficient for protecting increasingly mobile devices that now store valuable and confidential information. Better protection of client PCs and the information they hold from increasingly sophisticated software attacks can be achieved only through a combination of multiple technologies, in both hardware and software. Trusted Computing promotes a higher standard of security, in which a user knows with more certainty which device can be trusted and whether his / her own device is trustworthy. An environment composed of trusted platforms will be a safer computing environment.

Privacy and security go hand-in-hand: secure systems that do not support privacy are no longer acceptable. Privacy-friendly design may add complexity to the lifecycle of technology development but, with careful planning and long-term vision, it can be successfully implemented.

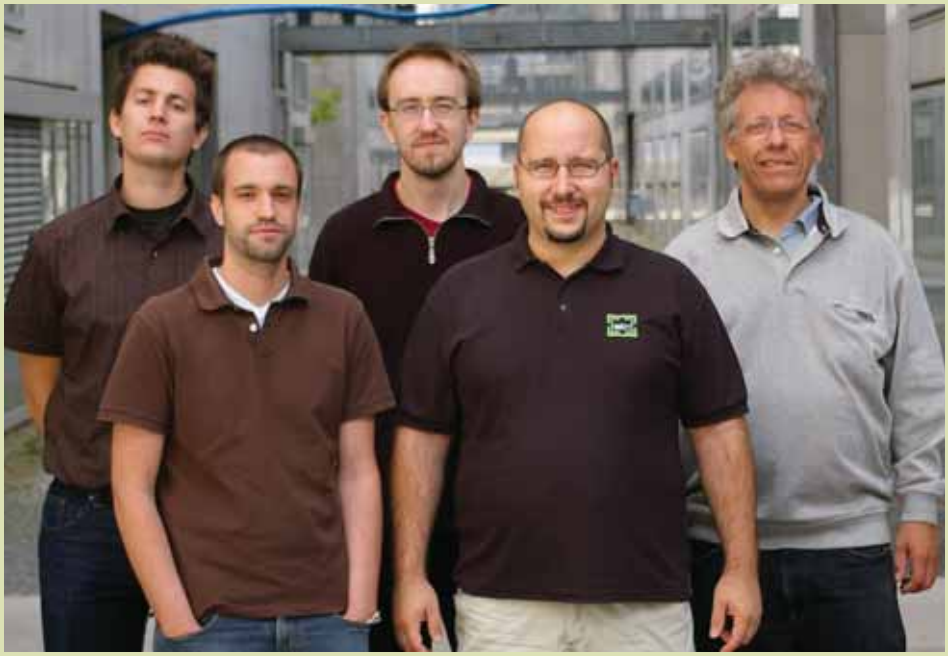
David Hoffman (david.hoffman@intel.com) is Group Counsel and Director of Security and Privacy Policy for Business Processes and Product Development at Intel Corporation.

Claire Vishik (claire.vishik@intel.com) is Trust, Security Standards & Regulations Manager at Intel Corporation and a member of the Permanent Stakeholders' Group established by ENISA.

Can you Really Trust your Computer Today?

Emerging architectures for Trusted Computing

Kurt Dietrich, Tobias Vejda, Ronald Toegl, Martin Pirker, Peter Lipp



From left to right, back row: Ronald Tögl, Martin Pirker, Peter Lipp; front row: Tobias Vejda, Kurt Dietrich

The lack of platform security in today's computers has given rise to waves of successful attacks, resulting in severe damage to enterprises and the potential failure of critical infrastructures. While viruses and worms usually reproduce and spread automatically, more recent Trojan horses aim to take over a computer system without the user being aware. Thus, concealment is one of their most important characteristics. Trojan horses manipulate the host operating system using so-called root-kits such that malicious processes are hidden from the user. They often also install a hidden back-door, allowing a hacker to take over control of the machine under attack. They will also try to manipulate any security software, especially virus scanners, that may be installed.

Such modern and highly sophisticated attacks are often 'profit'-driven. For instance, an attacker with full access to a system could install a key logger to collect private and confidential information such as passwords, personal identification, transaction or credit card numbers from the user. The captured system could also be used to store and distribute illegal content or to take part in other distributed attacks. However, behind such attacks other malicious intentions may be lurking too: in summer 2007 the press reported that numerous computers in German government institutions (including the Chancellery) had been infected by Trojan horses originating from China, raising fears of espionage.

The open and flexible design of today's computer systems and networks results from the primary goal of 'getting things done' in the simplest way possible. Applications of computing technologies aim to offer an immediate and clear benefit without introducing additional issues to worry about. However, security lessons learned from today's Internet clearly suggest that open communication with unknown and possibly treacherous systems is the root cause of the lack of security today. The fundamental problem of deciding which computer or communication system can be trusted can no longer be avoided. While in the real world 'trusted' may have all sorts of different and subjective meanings, here the term is used as defined by the Trusted Computing Group (TCG) and refers to an entity that "behaves in the expected manner for the intended purpose". Trusted Computing does not therefore depend on the idea of perfect security under all conditions, because the demands on system security will vary according to a specific task. Instead, it focuses on enhancing existing systems with mechanisms to report their current operational state to assist communicating partners in making an informed decision as to whether or not to trust their peer at a given moment in time.

Trusted Computing architecture

In legacy personal computers it is not possible to break out of the vicious circle of trying to protect software from manipulation using unprotected security software. Thus the TCG based their architecture on an additional hardware component referred to as a Trusted Platform Module (TPM). While the functionality of this hardware device resembles that of a smart card, it is soldered to the PC, and therefore physically bound to it. A tamper-resistant casing contains low-level blocks for asymmetric key cryptography, key generation, cryptographic hashing (SHA-1) and random number generation. With these components it is able to keep secret keys protected from any remote attacker. Additional high-level functionality consists of protected non-volatile storage, integrity collection, integrity reporting (attestation) and identity management. Of special interest is that the TPM is a passive device, a receiver of external commands. It does not measure system activity by itself but rather represents a trust anchor that cannot be forged or manipulated.

The underlying principle for establishing trust on a platform is the so-called 'transitive trust' model. A system is broken down into smaller entities, each of which is not trusted by default. Starting with the power-on-cycle, all software is measured before it is loaded. Measurement means calculating the hash of the binary representation of the software and other dependent data like configuration files etc. The measurement value is stored inside the TPM before control is passed on and this process is repeated throughout the whole software stack. By using this model, trust in a heterogeneous system consisting of a potentially large number of entities can be based on a single root-of-trust, the TPM.

During a work cycle, system activity is continuously reported to the TPM by running software and the TPM keeps a log of the system event measurements it receives. Through the use of cryptography, a TPM can provide compelling proof that the system is currently in a specific state and also that this proof originates from a unique, trustworthy piece of hardware – the TPM. A verifier may then decide if the state of the system is acceptable, depending on the security requirements.

Privacy concerns

A major concern of the opponents of trusted computing is the potential loss of anonymity and the threat of unwanted surveillance and even control, since a TPM may be identified by its Endorsement Key (EK). As this key is unique to the TPM, an attacker could use this key to track the history of the activities of a certain platform.

In order to address this issue, the TCG introduced the use of a Privacy CA (Certification Authority) or Direct Anonymous Attestation (DAA). Both concepts rely on the deployment of short-term keys and unlinkable certificates and signatures, thereby concealing the platform's identity.

Current European research activities

The European Community funded project, 'Open Trusted Computing' (OpenTC), is an international research and development project. The consortium behind it includes many well-known companies, research institutes and universities, including the Institute for Applied Information Processing at the Graz University of Technology in Austria.

The major goal of OpenTC is the development of a trusted and secure computing system based on open source software for traditional computing platforms and embedded systems like mobile phones. The OpenTC consortium is working on the design and implementation of an 'open Trusted Computing framework' including an architecture that is based on security mechanisms provided by low level operating system layers with isolation properties and interfaces to Trusted Computing hardware.

The framework and technology developed by OpenTC will empower European citizens to realise and exercise their right of informational self-determination in the context of using trusted, secure and reliable IT equipment. This fundamental capability allows a broader public use of IT – which is increasingly central to all future growth and economic development – without the dangers and limitations resulting from malware, possible misuse and attacks to systems.

Due to its higher visibility, Trusted Computing and its applications are the main focus of a growing number of scientific conferences and workshops. Research focuses include GRID security, document security, Trusted Computing for embedded systems and alternative attestation mechanisms.

The TPM specification is not rigidly defined when it comes to implementation, leaving many open issues for research and development efforts. For instance, the current state-of-the art – requiring a separate chip to provide the necessary functionality – may prove not to be the best for all platforms. Alternatives aim at providing remote software verification without using additional hardware or, at least, reducing additional hardware to a minimum. The security of these implementations is an area of active research.

Trusted Computing also affects areas other than purely technical ones. The all-embracing capabilities of Trusted Computing technology have legal as well as economic consequences. The main legal concerns are copyright, anti-trust law, data privacy law and digital rights management, the impact on which are not yet clear. Trusted Computing is also attracting attention in the field of information security economics.

Conclusion and outlook for the future

Today, Trusted Computing is a target of investigation by many international research programmes and institutions. However, companies are still hesitating about integrating this new technology into their IT systems; with growing confidence in this new technology and additional areas of application, they are likely to change their position.

The Institute for Applied Information Processing and Communications (IAIK) is working in different areas of IT security. These areas include e-Government, Very Large Scale Integration (VLSI) design, side channel analysis, cryptography and Trusted Computing. IAIK is also observing other rapidly-evolving technologies like networking or system-on-chip design, and is undertaking consultancy for a number of national and international institutions. At the same time, IAIK puts considerable effort into providing high class education to its students. Within OpenTC, IAIK has developed a set of tools and Application Programming Interfaces (APIs) for the Java™ language. These results are freely available at: http://trustedjava.sourceforge.net/.

Ongoing research in trusted systems also affects new versions of Trusted Computing technology and its core components. Recent advances in cryptanalysis, for instance, have shown that SHA-1 is not sufficiently secure. As progress in cryptanalysis will probably affect other cryptographic algorithms as well, algorithm agility will be one focus of new specifications. Furthermore, promising technologies such as the trusted execution environment from Intel are already available on consumer platforms.

Although several approaches have been proposed to improve and extend the current functionality, existing Trusted Computing technology focuses primarily on common desktop computer systems. However, ambitious efforts are being made to bring Trusted Computing technology to the embedded and mobile world, aiming not only at mobile phones but also at storage systems such as hard disks. As a consequence, the availability of Trusted Computing enabled hardware is constantly increasing. TPMs, that were only available on certain platforms in the past, will be available in many different devices.

Kurt Dietrich (Kurt.Dietrich@iaik.tugraz.at), Tobias Vejda (Tobias.Vejda@iaik.tugraz.at), Ronald Toegl (Ronald.Toegl@iaik.tugraz.at), Martin Pirker (Martin.Pirker@iaik.tugraz.at) and Peter Lipp (Peter.Lipp@iaik.tugraz.at) are all members of the Trusted Computing Group of the Institute for Applied Information Processing (IAIK) at the Graz University of Technology.

From our own Experts

Mitigation of Massive Cyber Attacks

ENISA and CERT/CC Workshop, 19 September, Porto, Portugal

Mehis Hakkaja

For the third year in a row ENISA has organised a workshop to help develop the Computer Emergency and Response Team (CERT) community in Europe. While previous workshops have been primarily aimed at increasing CERT presence in Europe, this year offered a timely opportunity to address some of the clear reasons why we need a strong and well prepared CERT community these days – for example, to mitigate the growing spread of wide-scale cyber attacks.

Often we do not even notice how increasingly dependant we are becoming on computers and networks in our everyday lives. The cyber attacks that troubled Estonia over a four-week period in April and May this year served as a reminder that was brought by the media to the attention of ordinary people and hopefully to many of the policy-makers of Europe as well.

With a population of close to 1.3 million, Estonia is one of the smallest EU Member States, yet it is also one of the most active in the use of IT. As an Estonian citizen, I often ask myself why such attacks should even matter to the ordinary person in Estonia. Most Estonians use on-line banking; 85% of last year's tax declarations in Estonia were completed on-line and 94% of tax payers received their tax refund directly into their bank accounts only five working days later. One starts to wonder how many public and private sector system interdependencies make all this accessible to the man or woman in the street via the Internet. More government e-services are listed at: www.ria.ee/xroad/presentation/ but, to sum up, going back to paper is no longer an option for Estonia.

Needless to say, the recent four weeks of attacks against numerous Estonian government and media sites, Internet service providers and almost all on-line banks were taken seriously not only by Estonians, but by many other countries too. Estonia was lucky to have established a CERT team at the national level a year ago, which was already in position to co-ordinate the mitigation of these attacks. Hillar Aarelaid from CERT Estonia summarised these events at the workshop.

To discuss what should be done in response to such incidents, ENISA teamed up with some of the best experts in CERT matters, the CERT® Coordination Center (CERT/CC) from Carnegie Mellon University in the US, to deliver the workshop. In a similar situation, it was the outbreak almost two decades ago of the 'Morris Worm', which brought down most of the Internet and served as the eye-opener that quickly led to the establishment of CERT/CC in 1988. The CERT model has since spread and today there are over 110 CERTs in Europe (www.enisa.europa.eu/cert_inventory/) and even more worldwide, but still not every country in Europe has a national level CERT initiative and some have no CERTs at all.

The workshop gathered together representatives of 25 European countries, including 22 EU Member States, with a wide mix of established and new CERTs and CERTs that are yet-to-be established. The day was divided into four sessions: 'Overview of the threat environment'; 'Key players in building a framework for managing cyber activities before, during and after the event'; 'Legal issues that prevent or facilitate co-operation'; and 'Short scenario in responding'. The workshop agenda and presentations are available on-line at: www.enisa.europa.eu/pages/04_01_3nd_cert_ws_2007.htm

ENISA and CERT/CC experts teamed up for the CERT workshop

It was a fruitful day in Porto and we hope that European countries will benefit from this workshop. Without question, co-operation and co-ordination are essential when dealing with a multitude of attacks, targets and sources, and CERTs are playing a central role.

Whether you are concerned about your own country or your neighbours in Europe, please take a look at our map of CERTs in Europe (www.enisa.europa.eu/cert_inventory/downloads/CERT_Euromap.pdf), and check whether there is sufficient coverage to make networks safer in your area.

Mehis Hakkaja (mehis.hakkaja@enisa.europa.eu) is an Expert in ENISA's section for CERT Co-operation.

Portugal Hosts the Third ENISA Awareness Raising Workshop

Kjell Kalmelid

On 18 September, the Awareness Raising Section of ENISA and the Portuguese members of the Agency's Management Board co-organised ENISA's third Awareness Raising workshop during Portugal's 2007 Presidency of the European Union. The Workshop was one of the activities planned within ENISA's Work Programme 2007 and was aimed at sharing the Agency's findings with Member States and industry representatives.

Pedro Veiga, the Portuguese representative on ENISA's Management Board, gave the first welcome address. He was followed by the Executive Director of ENISA, Andrea Pirotti, who referred to the Portuguese European Presidency slogan, "A Stronger Union for a better world", when saying that "in a united effort we shall raise awareness across Europe and beyond".

Cristina Bueti, Policy Analyst with the International Telecommunication Union (ITU), opened the workshop by presenting the recently launched initiative, Global Cybersecurity Agenda (GCA). The GCA is an ITU framework for international co-operation aimed at proposing global strategies to address well-defined challenges and threats. Prof. Luís Magalhães, President of The Knowledge Society Agency (UMIC) in Portugal, briefed the audience on the mission of UMIC which includes awareness raising activities targeting the citizens of Portugal.

Isabella Santa, Senior Expert in Awareness Raising at ENISA, together with Chris Potter of PricewaterhouseCoopers LLP, presented the recently finalised ENISA study, *'Information Security Awareness Initiatives: Current Practice and the Measurement of Success'* (www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf). The ENISA expert explained that the study has been produced in the light of the fact that "money is being spent on awareness raising without actually measuring the effectiveness of the campaigns". Mr. Potter briefed the audience on how the study was carried out and presented its main findings.

On the topic 'Awareness challenge: roll out global security awareness across the business', different companies' approaches to raising the awareness of their customers were outlined by Nuno Cruz, IT Special Projects Supervisor with TV Cabo, a major Internet service provider in Portugal, and Marjolein Kruithof, Awareness Adviser with Vodafone Group Security, a worldwide organisation with millions of customers. Nick Truman, Head of Internet Security at British Telecom (BT) in the UK, told the audience about the BT approach, giving as examples two ongoing initiatives: *Internet Green Cross Code*, produced by BT and targeting parents and teachers, and *Get Safe Online*, a government and private sector initiative supported by BT which helps consumers and micro-businesses use the Internet safely.

After the lunch break, François Thill, Assistant Director for Communications in the Ministry of the Economy and Foreign Trade in Luxembourg, described the Cyberworld Awareness and Security Enhancement Structure (CASES) which is part of the Luxembourg national strategy on information security. Under the title, "Is trust in ICT eroding in Europe and what to do to fight it?", Christian Wernberg-Tougaard of the Unisys Corporation stressed the importance of awareness raising as a means of keeping trust in the 'digital world'.

João Paulo Azevedo, Team Leader of the Security Incident Response Team (SIRT) of Caixa Geral de Depósitos, a major bank in Portugal, presented "a vision of security challenges in the banking sector". Alan Stockey, former Head of IT Risk Management (EMEA) with JP Morgan in the UK, delivered the final presentation, sharing his experiences in carrying out awareness raising programmes targeting an audience of technological graduates, and the strategies behind such programmes. Johannes Wiele of LANline in Germany moderated the closing discussion.

Details of the full programme, together with abstracts and the presentations, are available at: www.enisa.europa.eu/pages/04_01_3nd_ar_dissemination_ws_2007_program.htm

Kjell Kalmelid (kjell.kalmelid@enisa.europa.eu) is an Expert in the Awareness Raising section of ENISA.

RSA CONFERENCE EUROPE 2007

Dialogue with ENISA at RSA Europe 2007

Tuesday 23 October, 12.45-13.45 hrs

ENISA is organising a roundtable lunchtime discussion session with the theme 'A Dialogue with ENISA' at the forthcoming RSA Europe 2007 Conference in London, UK.

The session, on the Tuesday afternoon of the conference, will provide an excellent opportunity to meet face to face with ENISA representatives and to learn about both current and future projects but, most importantly, it will be an opportunity to comment and to propose new areas for co-operation and potential projects which the industry would like ENISA to take up.

The moderators of the session will be Mathea Fammels and Panagiotis Trimintzios, both of ENISA's section on Relations with Industry, Academia and International Institutions.

In addition, on the afternoon of Wednesday 24 October, Ronald De Bruin, head of ENISA's Co-operation and Support Department, will deliver a presentation during the session on 'Regulatory Frameworks – How to Ensure an Innovative but Safe Communications Environment'.

More details about the conference can be found at: www.rsaconference.com/2007/europe

From the Member States

Trusted Computing from a European Perspective –

The impact on the public sector

Marion Weber and Jörn-Uwe Heyder

At a time when more and more companies, public authorities and private individuals are relying on widely networked information and communication technologies, it is important to ensure the integrity and confidentiality of the data exchanged to create trust in the IT systems being used. The technology that is available today does not fully meet these expectations. It may be difficult to use, or open to tampering, because it is implemented by software which runs in an untrusted environment, or it is not available on mass market systems by default.

To solve these problems, a number of IT companies have founded the Trusted Computing Group (TCG), an organisation which aims to specify open standards for hardware-enabled trusted computing. Under the name Trusted Computing, the group plans to promote and support trust by technical means in contemporary IT platforms (personal computers, notebooks, mobile phones and PDAs).

For this purpose a standardised security chip – the Trusted Platform Module (TPM) – is to be integrated into the different IT platforms and supplemented by trustworthy operating systems and trustworthy infrastructures. The TPM contains functions to test the integrity of the platform. It will also provide functions for hardware-supported encryption, the signing of data or the authentication of the platform against third parties.

On the one hand this new approach seems to be able to equip mass market systems with functionality that could guarantee the integrity and confidentiality of the data being exchanged. On the other hand, one has to weigh up these opportunities against possible risks. For example, the question arises as to whether the technology can be easily handled by everybody or if only experts will be able to use this functionality. Additionally, one has to consider if the European privacy and data protection laws and directives are respected by a consortium which consists mainly of US-based companies. Moreover, some critics fear that the combination of the largest IT companies in a consortium like the TCG will disadvantage smaller companies or Free / Open Source solutions.

The implementation of this technology therefore seems to have consequences for many people. To discuss the impact on public authorities in Europe and their possible influence on Trusted Computing, the German Federal Ministry of the Interior and the Federal Office for Information Security (BSI) held a workshop on **"Trusted Computing from a European Perspective – The Impact on the Public Sector"** within the framework of the German EU Council Presidency. The event took place at the Science Centre in Bonn on 26 and 27 February 2007. Approximately seventy IT and administration experts accepted the invitation to discuss the opportunities and risks involved in the use of trustworthy information technology in a public authority environment. The group of European participants from 19 EU Member States and the EU Commission was extended by special experts from New Zealand, Japan and the US.

Open questions

The discussion opened with questions from the public authorities about Trusted Computing. The EU Commission and the German Government presented basic views from an authority's perspective. Andrea Servida, an EU Commission representative, pointed out the social, economic, legal and technical challenge of new security technologies like Trusted Computing. The German Federal Ministry of the Interior, the Federal Ministry of Economics and Technologies and the Federal Office for Information Security presented the fields of application for TC but also noted the related risks.

From their point of view, Trusted Computing incorporates functions which can enhance the security of contemporary IT systems for mass markets. The use of these systems in public authorities – for example in e-government applications, where it is important to check the integrity of the communication partners and to guarantee the confidentiality of the data exchanged – requires the constant development of both the latest TCG specifications and the implementations that are currently available.

Dr. Markus Dürig of the German Federal Ministry of the Interior, during his presentation

On the other hand, it was emphasised that Trusted Computing technology alone is not sufficient to protect classified data, so that specialised solutions will still be required for the sectors requiring high levels of security. But Trusted Computing technologies could improve the possibility of exchanging sensitive data within the public authorities' networks while at the same time exploiting the advantages of untrustable networks like the Internet. The Internet offers not only many benefits but also significant risks to society, which could be reduced by the techniques of Trusted Computing. Further more, people are increasingly conducting their business on the move and want to be able to access both their sensitive data and all the information of the Internet from everywhere, with any type of device. This convenience is accompanied by new threats to all kinds of sensitive data. The presenters recognised that Trusted Computing offers standardised solutions to interact with different devices in insecure environments in a trusted way.

Nevertheless, the delegates did ask many questions about the potential misuse and risks, which have to be answered before the technology can be used in such a way. Firstly the TCG standards are being developed by a large group of IT companies. These companies have different interests which sometimes compete with each other. As a result, the standards have to be checked to ensure that the promised and expected level of security is actually reached and that they are not the result of too many compromises. Another important point is to confirm whether the actual implementations are compliant with the standards. At the moment there is no real proof of this and Ahmad Sadeghi, Professor at the Ruhr-University in Bochum, Germany, addressed the workshop with a proposal for a compliance test which has been developed by his research group. The group recognised that no TPM currently on the market is 100% compliant. Additionally the implementations of trusted operating systems, the necessary infrastructure and the applications that use the technology are not completely finished.

More questions were introduced by Peter Schaar, the German Federal Commissioner for Data Protection and Freedom of Information who is also the chairman of the Art. 29 Working Party, a European Data Protection Group. With any implementation it is important to be able to fulfil the different data protection and privacy rights that exist by legislation. Especially in the European Union, the legal preconditions differ from those of the United States or Asia. In his speech, Schaar complimented the TCG for having sought a dialogue about this and that they have installed specialised working groups to consider all these aspects in the Trusted Computing technology. In addition, he pointed out the most important data protection issues which any implementation should offer.

A very useful contribution to the discussion was made by Hugh McPhail, a representative of the New Zealand government. He presented a paper about principles and policies for the use of Trusted Computing and Digital Rights Management. This paper was published in 2006 by his group (www.e.govt.nz/policy/tc-and-drm) and is especially designed to meet the needs of public authorities. The paper is general; it does not focus only on the specific concerns of New Zealand so it can be used by public authorities in any country. Among other aspects, McPhail pointed out that public authorities cannot enforce which IT systems citizens should use. Every e-government service must also allow users to use the service without Trusted Computing technology, if they prefer.

Solutions

It was not only questions about open issues which were discussed during the workshop. The second day dealt with solutions. Several members of the TCG's Board of Directors used the opportunity to hold discussions with the representatives of European public authorities. Mark Schiller, President of the TCG and Director of the Security Strategy Office at Hewlett Packard (HP), described the current efforts within TCG and explained the Group's structure. He offered the delegates the possibility of taking part in the TCG's standardisation work and to use this as a means of helping to improve the technology in a way which meets their needs. To this end he introduced a special membership degree which has been designed for universities and public authorities – the so called Liaison Program (https://www.trustedcomputinggroup.org/join/).

Boris Balacheff, also of HP, introduced OpenTC, a European Commission co-funded project in which a consortium of different research groups and companies from European Union countries are developing a trusted operating system based on Open Source software and Trusted Computing hardware technology. This project is a good example of how Trusted Computing technology does not necessarily discriminate against Open Source.

The two days were completed with a talk by Seigo Kotani, a Japanese participant from Fujitsu, who was invited to present the Japanese IPEC (Internet Protocol Equipment Certification Study Group), a special group that he is heading which aims to co-ordinate the Japanese activities around Trusted Computing and to deal with specific Japanese needs.

Conclusion

The lectures and discussions at the workshop clearly showed that Trusted Computing can contribute to enhancing the security of IT applications and solutions in the context of a public authority. It remains for the industry now to develop secure, trustworthy and interoperable implementations in order to provide a trustworthy basis for e-government and e-commerce applications.

The participants in the workshop all agreed that the discussions and ideas presented were very useful for their work. The constructive dialogue between implementers and public authorities was particularly appreciated by a number of those present. By popular consent the dialogue is to be continued and intensified to enrich the Trusted Computing process with European ideas and demands and to strengthen the European influence.

Workshop on Trusted Computing

A significant contribution to this work will be an event on Trusted Computing that includes a scientific conference, workshops and spring school, which is planned by the OpenTC consortium and the Technikon Forschungsgesellschaft mbH for 10–13 March 2008 in Villach, Austria. More information about the event is available at: www.trust-conference.eu

Marion Weber (marion.weber@bsi.bund.de) is a senior expert in operating systems security having specialised in Trusted Computing technologies at the German Federal Office for Information Security (BSI).

Jörn-Uwe Heyder (joern-uwe.heyder@bsi.bund.de) is a senior expert in international relations and Internet security at the BSI, and the German National Liaison Officer for ENISA.

IT Security Beyond Borders

A report from the Danish expert group on future IT security threats

Christian Wernberg-Tougaard and Bjørn Bedsted

The security of Information and Communication Technologies (ICT) is something that most citizens of the European Union today are fighting for – either by battling viruses, spam, phishing or other malware, or by fending off schemes to compromise privacy and extract personal (usable) information. But the current outlook paints a much darker picture – at least if no action is taken at the international level.

The challenge was taken up recently by an expert working group examining 'IT-Security Beyond Borders', under the auspices of the Danish Board of Technology (DBT) (for the composition of the group, see below). The mandate of the group was to look at what could threaten the IT security of Denmark that could only be adequately addressed through international action, and to suggest a strategy for enhancing IT security in Denmark that would go significantly further than any other similar previous effort. It became apparent that now is the right time to take concrete steps in the form of, among other things, lawmaking, certification and labelling programmes.

Our working processes included brainstorming among more than forty leading Danish IT security experts who drew up a prioritised list of themes. This list included six distinct problems with solutions, which were discussed with global IT security leaders in different fields of knowledge (see below). Finally the meta-problems and their solutions were validated with industry and public sector interest groups.

Citizens are becoming more and more distrustful of the digitised service society – they fear for loss of privacy, loss of societal services and services tied to digitalisation. Research into the trust level of citizens around the globe (Unisys Trusted Enterprise Index), that is shortly to be published, shows that more than 50% of European citizens are "Extremely concerned" or "Very concerned" about others having unauthorised access to their personal information. The erosion of trust can lead to an escalating distrust of digital solutions – and hence fuel further erosion. In order to utilise the power of the digitised service society, trust among citizens (and companies) in digital services must be restored. This calls for a combination of awareness raising and collaboration between research-public-private bodies to outwit the next generation of IT security threats. While growth in e-trade, home banking etc. is escalating throughout Europe, the benefits of IT currently surpass the problems, but the danger lies in the erosion of trust.

If we take Denmark as an example, in order to meet its official goal of being an innovative knowledge-based and entrepreneurial society, able to punch its weight at the global level, Danish citizens and companies must be able to communicate securely; both within and beyond Denmark's borders. This is an important prerequisite for taking full advantage of the potential offered by globalisation and hence a prerequisite for Denmark's welfare in the future. It is therefore necessary that Denmark, the EU and the world at large seriously increase their efforts to prevent and fight national and international cyber-crime. Many of the security problems which Denmark faces cannot be solved nationally – they require international collaboration.

Technological development has meant that an increasing number of societal functions are integrated with the Internet, including, for instance, e-government, e-banking and e-commerce. This trend increases society's vulnerability to cyber-crime and means that poor IT security, as often seen in the form of software flaws or lack of protection against viruses and hackers, still has serious consequences. Connecting to the Internet increases the risk of threats emanating from anywhere in the world.

Among the analysis institutes and law enforcement agencies around the world, there is a clear consensus that problems associated with cyber-crime are widespread and growing. One explanation is that the global Internet is particularly well suited for criminal activity. Perpetrators typically hide behind networks of computers, located in numerous different countries, making Internet-borne criminal action incredibly difficult to investigate and solve. The fact that cyber-crime is becoming more complex

The members of the working group on IT-security Beyond Borders:

- Preben Andersen, Director of DK-CERT
- Christian Wernberg-Tougaard, Member of ENISA's advisory panel on 'Awareness Raising', Director of Unisys
- Brian Birkvald, leader of IBM's security group in Denmark
- Morten Storm Petersen, Director of Signaturgruppen A/S
- Carsten Stenstrøm, Director of Technology Security, DR (Danish Broadcasting Corporation)
- Lars Neupart, Director of Neupart A/S

Project Manager: Bjørn Bedsted, The Danish Board of Technology

International Advisors to the Working Group:

- Howard Schmidt - former White House IT security advisor and member of ENISA's Permanent Stakeholders' Group
- Prof. Reinhard Posch – Chief Information Officer for the Government of Austria and Chairman of ENISA's Management Board
- Tyler Moore – IT security economist
- David Marsh – chairman of ENISA's Ad Hoc Working Group on Regulatory Aspects of Network and Information Security and member of the United Nations CEFACT Steering Group

underlines the fact that cyber-criminals are becoming increasingly skilled in their trade.

Though the problems grow ever greater, cyber-crime is poorly addressed within Denmark and also internationally, compared with other forms of crime. The amount of scientific investigation and publicly available statistics regarding cyber-crime is very limited and concrete initiatives to prevent and confront cyber-crime are characterised by a lack of resources and focus.

Problems and solutions identified by the working group

The working group of experts has sought to develop and present internationally-focused recommendations for cross-border IT security problem areas that have been identified as among the most significant now and in the near future. The goal is that all of the recommendations should be realisable in practical terms. The group advises that the recommended solutions should be applied simultaneously as soon as possible. The following is an overview of the problem areas that have been identified and a brief description of the working group's recommendations:

1. Vulnerabilities in software and hardware

Problem: Measured in the number of instances and their consequences, vulnerabilities in hardware and software are the most serious of all IT security problems. The consequences of these vulnerabilities are more significant for small and medium-sized enterprises (SMEs), public institutions and private citizens than for large firms.

Solution 1: Develop a model that ensures that the security updates in software are installed on users' computers as soon as a security flaw is identified. The process should be imperceptible to the general user while advanced users should be given the option to steer their own update process. Large software updates, often called 'service-packs' by some providers, would, however, remain installable only after the user's approval.

Solution 2: There should be EU regulation to require that vendors of electronic, network-based (IP-based) hardware such as computers, telephones, MP3-players, alarm-systems and, in the future, even refrigerators, must deliver their products with the latest firmware and software updates pre-installed.

Solution 3: Denmark/the EU should create a 'white-list' for software and hardware products. The public sector could then set the example and drive the market by only using white-listed IT products.

Solution 4: A certification programme for Internet Service Providers (ISPs) should be established. All ISPs in the EU should be obliged to follow a code that at least meets the standard set by the Danish ISP Security Forum's code of conduct. Within 3-5 years, it should be made law that all ISPs are ISO 27001-certified (or meet an equivalent standard).

2. Inadequate awareness of IT security problems

Problem: Inadequate knowledge is a significant cause of the lack of security. The human factor is, inter alia, important in relation to social engineering, 'phishing', identity theft and the spread of harmful software. The consequence for individuals is the loss of data including documents, photos, films, music, etc.; and for companies, the loss of client records and intellectual capital. The lack of IT security knowledge is rarely limited to the firms and citizens who are ill-secured themselves. The consequences of poor security can spread to a firm's customers, partners etc., and to the people listed in a private user's address list – in total, causing exponential damage and economic loss. In the light of this, network administrators, employees and managers should prioritise security much higher than they do today. And general awareness and knowledge among the population at large should be significantly raised.

Solution 1: The focus on IT security in school should be increased. The aspects of IT security should be linked with students' use of personal computers throughout the course of their education.

Solution 2: 'The Board for Greater IT Security' focusing on citizen awareness should be established.

Solution 3: There should be regulation against 'Cyber-pollution'.

3. The inability to differentiate between secure and insecure products and services

Problem: An ever greater number of products and services contain an element of connectivity and thus it is ever more relevant to offer secure products and services to users with the aim of improving the general level of security. These products include computers, mobile phones, hard disk recorders in TVs, media centres, refrigerators and similar items in a private home. In the near future, nearly all machines, including cars, boats and planes, will be connected to the Internet.

Solution: Denmark should take the initiative to develop a concept for labelling Internet-connected products, so that individuals and companies are given the ability to see the security level of a given product. For example, a star-rating, as in the auto-industry's 'crash-test' scheme, could be implemented. The labelling programme should include the entire EU, and thereafter spread to the global market.

4. The lack of concerted, international efforts to fight cyber-crime

Problem: Cyber-crime is a difficult arena for law enforcement agencies in Denmark as well as in the EU and the world at large. Interpol is largely absent from the fight against IT-related crimes and Europol's role is relatively small due to limited resources. The growing amount of cyber-crime on a global plane is tackled with inadequate police efforts. Fighting cyber-crime is generally prioritised low in comparison with other police investigations so the sector receives few resources and therefore has an acute lack of competent personnel.

Solution 1: Structuring the efforts: cyber-crime should be acknowledged as a new law enforcement specialisation. At least one unit responsible for cyber-crime should be appointed in each police district, and a central authority should also be established that can address complex cases concerning cyber-crime professionally – nationally and internationally. Prioritising cyber-crime at a high level should not come at the cost of other police activities. Rather budget increases are needed to supplement the efforts.

Solution 2: Increasing the knowledge level: Law enforcement authorities must be equipped with greater competency across the board – from the education of specialists in the various sectors of cyber-crime to increasing the knowledge of prosecutors and judges.

Solution 3: International co-operation agreements should be further developed to ensure more efficient and effective processing of international cyber-crime cases.

➲

5. Lack of secure identification

Problem: Communication security is a prerequisite for the free flow of information, efficient e-government and thus better public service in the future. Citizens' usage of the increasingly integrated economic service infrastructure in the EU and around the world could be halted by the lack of a clear identification mechanism, nationally and across the EU. A secure identification mechanism would, inter alia, minimise the risk of the abuse of personal data. One could imagine a mechanism that would eliminate the difficulties connected with the exchange of patient records between Danish and foreign hospitals. It is a national responsibility to create a digital identification that can protect citizens' personal data against identity theft. The working group concludes that all citizens in Denmark and the EU at large should be equipped with an identification mechanism with strong security features.

Solution: Denmark should establish a long-term strategy for the further development of the existing 'Digital signature' into a 'citizen service passport', as a 'digital identity, which would then help to minimise the risks involved in e-government, e-trade, and other forms of electronic communication. The goal is that, in the long run, all EU citizens should have an *interoperable* digital ID. The working group points to a project under development in Austria, as a source of inspiration. The Danish development work should be co-ordinated in relation to the entire EU, with the goal of building a secure, EU-interoperable 'citizen service infrastructure', using common and open communication standards.

6. The lack of focus on IT security in public procurement

Problem: Under 5% of the criteria found in contracts for public procurement of IT account for security. The working group finds that IT security is not taken seriously when the EU and its member countries take bids on infrastructure and systems contracts. It is problematic that technical specifications for IT security and privacy in the public procurement of IT products are either inadequate or non-existent, and that these contracts seldom contain an assessment of the consequences of a security breach on all of the interconnected public units, many of which are not themselves part of the procurement agreement.

Solution: Regulation should establish IT security as a key parameter in all public procurement contracts where IT is a component. Specification sheets and bids should contain both a security analysis that assesses the consequences of a security breach for interconnected sectors.

Additional information about 'IT-security Beyond Borders' can be found at www.tekno.dk/it-security_beyond_borders

Christian Wernberg-Tougaard (Christian@wernberg.org) is an ICT-security and awareness raising expert currently appointed as advisor for the Danish Minister of Science, Technology and Innovation on ICT-security, and a member of the expert group on 'IT-Security Beyond Borders'.

Bjørn Bedsted (bb@tekno.dk) is a Project Manager in the Danish Board of Technology.

Co-operating to Protect Critical Information Infrastructures

The Meridian Conference, 24-26 October

Andreas Wedner

The Swedish Emergency Management Agency (SEMA), together with the Meridian Program Committee, invites government representatives to this year's Meridian Conference in Stockholm, Sweden, from 24-26 October 2007.

SEMA is continuing the work of previous annual conferences in establishing a confidential environment for fruitful discussions and networking between senior government officials who are responsible for policy on critical information infrastructure protection (CIIP). The Conference is part of the Meridian Process for governments worldwide to discuss among themselves how best to co-operate to protect critical information infrastructures in the light of new challenges of connectivity and dependency which cross national borders. The aim of the Conference is to foster an open dialogue that delegates will continue to develop when they return to their respective countries.

This year's Conference will feature the application of the G8 CIIP principles to the development of CIIP policies, the emerging relationship between CIIP and general Critical Infrastructure Protection (CIP), and the new challenges of securing process control systems in critical national infrastructures. It will also include a wide spectrum of security workshops on Process Control Systems to explain these cross-sector systems in a straightforward and understandable manner. Conference delegates will also have an opportunity to discuss the diverse ways that globalisation affects the development of new national policies for the protection of critical services and the underlying information infrastructure. Such policies include managing international dependencies and co-operating with the private sector that owns or controls many of a nation's infrastructure assets.

The Conference will be held at the Hilton Hotel on the island of Södermalm in Stockholm. The registration fee includes hotel accommodation and all meals, as well as the gala event dinner on 25 October.

To register on-line and for further information, visit: www.meridian2007.org

Andreas Wedner (Andreas.Wedner@kbm-sema.se) is an Analyst at the Information Assurance Department of the Swedish Emergency Management Agency (SEMA).

Supervision of the Swedish National Top-Level Domain, .se

Erika Hersaeus and Helena Bäckström

The Swedish National Post and Telecom Agency (PTS) is the public authority that supervises the electronic communications and postal sectors in Sweden. Since 1 July 2006, PTS has been assigned to exercise supervision under the National Top-Level Domains for Sweden on the Internet Act (2006:24) – the 'Top-Level Domains Act'.

The Act deals with the technical operation of national top-level domains (TLDs) for Sweden on the Internet in addition to the allocation and registration of domain names under these domains.

In the autumn of 2006, PTS carried out supervisory work by compiling information based on questions that had been put to the administrator of the national TLD.SE. The aim was to assess whether or not .SE was operating securely and effectively in the public interest and whether the domain names, the IP addresses and the other information registered into the system were correct and reliable.

PTS limited its supervision to the requirements laid down in the Top-Level Domains Act, which stipulates that the name server operation for the .se zone must be managed securely and effectively from a technical perspective, that registering an entry should take place in a secure manner while protecting integrity, and that name resolving in the .se zone must be carried out efficiently.

Specifically, PTS's supervision encompassed the following areas:

- the technical solution, the reserve capacity and protection of the name servers
- the generation, distribution and correctness (authenticity) of the zone file
- the operational organisation and monitoring systems of .SE
- the registration of an entry
- the updates of software and hardware
- the creation and maintenance of a business continuity plan
- the assurance of information security, and
- the preparedness for possible threats and attacks in the future.

Findings

From an analysis of responses to a questionnaire and the provisions of the Act, it was shown that, on the whole, .SE runs its operation in a secure and effective manner with the public interest in mind. The physical and logical protection provided ensures that traffic functions properly, and offers effective protection of data in the TLD. .SE employs well known IETF (Internet Engineering Task Force) standards for logical protection and performs regular software and hardware updates. Registering an entry takes place in a manner that is secure and protects integrity, and name resolving in the .se zone is carried out efficiently. .SE has secured a redundant name server architecture and imposes requirements on both its name server operators and its registrars (domain name resellers). .SE has also shown its preparedness for emergencies and has demonstrated a satisfactory level of information security.

Future supervisory activities

During 2007, PTS is following up .SE's security work and training in respect of its crisis management plan on a regular basis. The assessments from the 2006 supervisory work are based on the prevailing traffic loads, look-up capacity, number of domain names, threat profiles etc. during the period in relation to .SE's security work. Any significant increase in the number of domain names registered in the .se zone in the future may lead to a different assessment if .SE does not expand its systems and reserve capacity to keep pace with this growth.

It is likely that, during the autumn of 2007, PTS will extend its supervision of the provisions of the Top-Level Domains Act by looking at the allocation of domain names, dispute resolution and the transfer of data to the supervisory authority, with the aim of maintaining a secure and effective domain name operation in the interest of both the general public and the nation.

Details of the supervisory work can be found (in Swedish) at: www.pts.se/Archive/Documents/SE/PM_tillsyn_av_se_doman_feb_2007.pdf.

The Top-Level Domains Act and the PTS

The Swedish Government has appointed PTS as the authority responsible for ensuring compliance with the new National Top-Level Domains for Sweden on the Internet Act. This Act encompasses the party administering national Top Level Domains (TLDs) for Sweden. The Internet Infrastructure Foundation, .SE, is the stakeholder currently responsible for the '.se' TLD and is in charge of managing the day-to-day operation and administration of this TLD.

The aim of the Act is to give central government the opportunity to control and supervise the administration of the domain and to prevent any inadequacies in the DNS service, the technical system which recognises which IP address corresponds to a certain domain name. The Act will also ensure that the party responsible for the operation of the .se zone can provide satisfactory accessibility, quality and security, and give the authority appointed by the Swedish Government, i.e., PTS, statutory support for its supervisory work. In other words, the power to order a party in charge of the operation of the '.se' zone to take any measures that are necessary. The Act stipulates requirements concerning the technical operation and maintenance of registers as well as principles for the allocation and registration of domain names.

Erika Hersaeus (Erika.Hersaeus@pts.se) is a technical analyst of Internet Infrastructure issues in the Network Security Department of the Swedish National Post and Telecom Agency, and a technical expert in the supervisory work of the administration of the Swedish Top Level Domain, '.se'.

Helena Bäckström (Helena.Backstrom@pts.se) was the legal adviser in the Network and Security Department and is now head of the Services Accessibility Section of the Consumer Department in the Swedish National Post and Telecom Agency.

ENISA Short News – Third Quarter 2007

Panagiotis Trimintzios

Information Risk Management – Why Business Needs it?
ENISA and INTECO are co-organising an event on Information Security Risk Management on 8-9 November 2007 at Hotel 1898 in Barcelona, Spain.
http://enisa.inteco.es/

ENISA co-organised the ISSE/SECURE in Warsaw, 25-27 September
The leading, non-commercial ISSE conference gathered 400 Network and Information Security (NIS) experts from business, industry governments and scholars.
(www.enisa.europa.eu/pages/02_03_news_2007_09_24_enisa_isse.html)

ENISA host for all EU-Agencies' Accountants
ENISA hosted the second meeting of the Accounting Officers of the European Agencies and Advisory Bodies in Heraklion on 6-7 September. About 30 accountants participated in this biannual conference which is an open forum for discussion among the Accounting Officers of the European Community.
(www.enisa.europa.eu/pages/02_03_news_2007_09_13_account_meet.html)

How to measure the success of information security awareness?
How do you know if end-users really take action to make their computers secure? ENISA presented the first European report on current practices for measuring successful awareness raising initiatives in information security across the European Union (EU), which contained the responses from 67 European organisations headquartered in nine different countries. The report provides an outline analysis of recommended security awareness practices, measurements of effectiveness and metrics, including case studies, mainly of governments and private companies within the EU.
(www.enisa.europa.eu/pages/02_01_press_2007_08_22_meas_succ.html)

ENISA aims for European Interoperability of Identities
A recent ENISA workshop brought together European eID card projects, Electronic Passport authorities, banks, industry and standards bodies to discuss the key issues.
(www.enisa.europa.eu/pages/02_03_news_2007_08_22_enisa_eur_eid.html)

Can we trust reputation? ENISA studies on on-line reputation
With eBay's seller reputation, Amazon's product ratings and Skype's recent launch of a business rating system, on-line reputation systems are increasingly important. ENISA is looking at threats to reputation and how reputation can be used as a weapon in the security arsenal.
(www.enisa.europa.eu/pages/02_03_news_2007_08_21_online_rep.html)

New composition of the Permanent Stakeholders' Group
The new ENISA Permanent Stakeholders' Group has been appointed to advise and assist ENISA. The group is composed of 30 experts representing stakeholders from industry, academia, users and consumer organisations.
(www.enisa.europa.eu/doc/pdf/stakeholders/perm_stake_info_appoint_1_0.pdf)

How safe is on-line 'Social Networking'?
Myspace, Twitter, Facebook – Social Networking is the web success story of the new century. The statistics are mind-bending – Myspace claimed its 100 millionth user in August 2006. But a recent ENISA workshop put the question – "how safe are on-line social networks?"
(www.enisa.europa.eu/pages/02_01_press_2007_08_16_social_net.html)

Open vacancies at ENISA
There are open vacancies at ENISA for Senior Experts and Seconded National Experts.
www.enisa.europa.eu/pages/07_05.htm

The ENISA General Report 2006 has gone on-line
(www.enisa.europa.eu/doc/pdf/general_report_2006.pdf)

New distribution list for ENISA Quarterly
The ENISA Quarterly (EQ) magazine announcements list has been created in the ENISA Community membership area. Please join the list in order to be updated with all news related to EQ: new editions, call for articles etc.
(http://lists.enisa.europa.eu/list/subscribe.html?mContainer=10&mOwner=G2t322x372p)

ENISA wishes to thank all the contributors to the publication. Please remember that all contributions reflect the views of their authors only, and are not in any way endorsed by the European Network and Information Security Agency. ENISA assumes no responsibility for any damages that may result from use of the publication contents or from errors therein.

The ENISA Quarterly is published once each quarter. You can find information about ENISA Quarterly, including back issues and subscription information, on the EQ pages on the ENISA website: www.enisa.europa.eu/enisa-quarterly/

Editor-in-Chief, Panagiotis Trimintzios: eq-editor@enisa.europa.eu