Norbert Pohlmann
Helmut Reimer
Wolfgang Schneider

Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe 2007 Conference

Contents

Preface

ENISA is proud to be working with eema, TeleTrusT, NASK (the Polish research and development organization and leading Polish data networks operator) and the German Federal Ministry of the Interior as well as the German Federal Office for Information Security for this year's 9th annual Information Security Solutions Europe Conference.

The aim of the ISSE has always been to support the development of a European information security culture and especially a cross-border framework for trustworthy IT applications for citizens, industry and administration. ENISA is committed to these goals. In our work we assist and advise the European Commission, Member States as well as business community on network and information security as well as on legislative requirements, and we are delighted to support the ISSE again this year.

The security of communication networks and information systems is of increasing concern. In order to face today's complex information security challenges it is clear that working collaboratively with one another is the key to generating new strategies to address these problems. It has been an exciting opportunity to facilitate this collaboration at the ISSE 2007, pulling together the wealth of industry knowledge, information and research that we hold in Europe, as well as across the globe.

The success of this event in generating ideas and frank, lively debate around the complex topic of IT security is due also to the independent, varied nature of the programme, which was selected by world-wide specialists in the field.

Some of the key topics explored at this year's conference have been chosen as the basis for this book, which is an invaluable reference point for anyone involved in the IT security industry.

We hope that you will find it a thought-provoking and informative read.

Andrea Pirotti, Executive Director, ENISA

About this Book

The Information Security Solutions Europe Conference (ISSE) was started in 1999 by eema and TeleTrusT with the support of the European Commission and the German Federal Ministry of Technology and Economics. Today the annual conference is a fixed event in every IT security professional's calendar.

The integration of security in IT applications was initially driven only by the actual security issues considered important by experts in the field; currently, however, the economic aspects of the corresponding solutions are the most important factor in deciding their success. ISSE offers a suitable podium for the discussion of the relationship between these considerations and for the presentation of the practical implementation of concepts with their technical, organisational and economic parameters.

From the beginning ISSE has been carefully prepared. The organisers succeeded in giving the conference a profile that combines a scientifically sophisticated and interdisciplinary discussion of IT security solutions while presenting pragmatic approaches for overcoming current IT security problems.

An enduring documentation of the presentations given at the conference which is available to every interested person thus became important. This year sees the publication of the fifth ISSE book – another mark of the event's success – and with about 50 carefully edited papers it bears witness to the quality of the conference.

An international programme committee is responsible for the selection of the conference contributions and the composition of the programme:

- **Ronny Bjones,** Microsoft (Belgium)
- **Gunter Bitz,** SAP (Germany)
- **Lucas Cardholm,** Ernst&Young (Sweden)
- **Roger Dean,** eema (UK)
- **Ronald De Bruin,** ENISA
- **Jan De Clercq,** HP (Belgium)
- **Marijke De Soete,** NXP Semiconductors (Belgium)
- **Jos Dumortier,** KU Leuven (Belgium)
- **Walter Fumy,** Siemens (Germany)
- **Michael Hange,** BSI (Germany)
- **John Hermans,** KPMG (The Netherlands)
- **Jeremy Hilton,** Cardiff University (United Kingdom)

- **Frank Jorissen,** SafeBoot (Belgium)
- **Matt Landrock,** Cryptomathic (Denmark)
- **Mirosław Maj,** CERT Polska (Poland)
- **Tim Mertens,** ENISA
- **Attila Péterfalvi,** Parliamentary Commissioner for Data Protection and Freedom of Information (Hungary)
- **Norbert Pohlmann,** University of Applied Sciences Gelsenkirchen, Chairman of the Programme Committee (Germany)
- **Bart Preneel,** KU Leuven (Belgium)
- **Helmut Reimer,** TeleTrusT (Germany)
- **Joachim Rieß,** Daimler Chrysler (Germany)
- **Paolo Rossini,** TELSY, Telecom Italia Group (Italy)
- **Wolfgang Schneider,** Fraunhofer Institute SIT (Germany)
- **Jon Shamah,** CoreStreet (UK)
- **Krzysztof Silicki,** NASK (Poland)
- **Robert Temple,** BT (United Kingdom)

The editors have endeavoured to allocate the contributions in these proceedings – which differ from the structure of the conference programme – to topic areas which cover the interests of the readers.

Norbert Pohlmann *Helmut Reimer* *Wolfgang Schneider*

eema (www.eema.org):

Established in 1987, eema is an independent association of IT professionals, businesses and governments providing business and technical networking opportunities at both local and regional levels in the broad areas associated with digital identity and its applications, such as security. Our mission is to stimulate the growth and effectiveness of our members' business in these areas through increased market awareness, cooperation and opportunity creation.

We aim to bring over 1,500 member representatives together in a neutral environment for education and networking puposes. We enable members to share experiences and best practice by holding meetings and conferences, by facilitating working groups who produce reports on topical subjects, and by helping members to connect with the right person to help them solve business issues or develop beneficial business relationships. All work produced by members is available free to other members, and previous papers include: Towards Understanding Identity, Role Based Access Control – a Users Guide, Secure e-mail within a Corporate Environment and Secure e-mail between Organisations.

For more information contact: alison.james@eema.org.

TeleTrusT Deutschland e.V. (www.teletrust.de)

TeleTrusT Deutschland e.V. was founded in 1989 as a non profit making association to promote the trustworthiness of information and communication technology in an open systems environment. In the 17 years of its existence TeleTrusT has evolved into a competence network for applied Cryptography and Biometrics with over 80 institutional members.

The TeleTrusT working groups produce results which create an advantageous framework for trustworthy solutions of daily business processes as well as contributing to their acceptance. Accordant to the demands of the every day practice TeleTrusT supports the area wide implementation of data encryption as well as Identification, Authentification and Signature (I-A-S) in eBusiness applications within industry and administration. In this connection the conformity of standards plays a decisive role as a foundation for interoperable Hard- and Software as well as for services.

The non profit organisation brings together the interests of users and vendors. Thus vendors can satisfy the users' demands more effectively with marketable products and services, in which scalable security mechanisms are implemented.

TeleTrusT seeks and cultivates the cooperation with other organisations with similar objectives – in Germany and internationally. Thus ISSE has been organised in cooperation with eema, ENISA and NASK in Warsaw this year.

For more information contact: sophie.hellmann@teletrust.de

Preface

We are honoured to be hosting and co-organising this year`s ISSE/SECURE 2007 Conference in Warsaw.

As Minister of Interior and Administration, I am responsible for the development and diffusion of Information Technology in Poland, especially for implementing e-Administration and for the development of the Information Society.

Aware of the increasing concern for ICT in all the fields of economic and social activity, the Ministry of Interior and Administration plays a highly active role in legislation, strategy development as well as projects implementation.

A high priority has been given to projects aimed at higher personal data protection and secure electronic systems in public administration. As an example, the Electronic Platform of Public Administration Services project provides for a single platform with e-services of public administration for citizens and businesses. One of its tasks will be to provide public administration with common tools for user's authorization and certification.

The Ministry also took over the competences concerning digital signature implementation in reason of activities strongly related to its policy lines concerning implementation of eID and registers security for the forthcoming public e-services.

The Ministry of Interior and Administration's concern for ISSE/SECURE 2007 conference is an excellent prove of its deep interest for issues concerning the European information security challenges.

We look forward to create a good field for effective transfer of ideas, knowledge and best practices among policy makers, experts in ICT security and industrials.

Władysław Stasiak
Minister of Interior and Administration

Microsoft: A Trustworthy Vision for Computing

The continually evolving computing landscape of today has two primary macro-level developments: more people and businesses rely on computing every day, and the threats that can undermine trust in computing are increasingly sophisticated and malicious.

From the customer's perspective, it is increasingly important that sensitive data are protected, that software businesses adhere to business practices that promote trust with users, and that the technology industry renews its focus on solid engineering and best practices to ensure the delivered product or service is more reliable and secure.

Microsoft's approach to this environment is Trustworthy Computing (TwC), a long-term, collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone. Microsoft formed TwC in January 2002, when Bill Gates committed the company to fundamentally changing its mission and strategy in the key areas of Security, Privacy, Reliability, and Business Practices.

TwC's five-year milestone seems an appropriate time to examine our efforts to date and to affirm the promise of TwC. What follows is an update on some of the things we're doing to ensure that customers can count on every one of our new and exciting innovations.

Pricacy

Microsoft is working with policymakers and industry leaders in the United States to encourage federal laws that establish baseline privacy protections for consumers while still allowing commerce to flourish. And, since privacy threats know no borders, we're also working with governments around the world to make privacy laws as consistent as possible.

Security

Microsoft works closely with other software vendors, the research community and security companies to find better ways to build more secure software, locate vulnerabilities, collaboratively address issues as they arise, and establish best practices across the industry. We partner with law enforcement world-wide to help find and catch individuals who write and distribute malicious software. And, when a new issue threatens customers, our Security Response Center mobilizes teams to investigate, fix and learn from security vulnerabilities. We continue to release security updates on a regular schedule.

Reliability

Over the past few years, we've made great progress in improving the reliability of our products, as well as other software built on our platform, through continuous improvement technologies – software that can diagnose, report, and fix problems as they arise. For example, the error-reporting features in Microsoft Office 2007 perform thorough diagnostics when applications hang or crash, including checking the computer's hard disk and memory and verifying that the customer's software is up-to-date and uncorrupted. It can dynamically keep track of system resources, and help avoid performance and reliability issues when running a large number of applications.

Looking Ahead

Microsoft has spent the past five years working to transform the company around TwC, and it has improved by an order of magnitude in each of the areas noted above. But, there's still plenty of work to do. We've only tapped a fraction of computing's vast potential, and the coming years will continue to bring new innovations that transform how we live and work.

The world of PCs and servers is evolving into a rich web of connected devices and services and computing has become enmeshed into the fabric of our lives. This is why TwC has to do more than address today's challenges – it must ensure that the innovations people will rely on tomorrow are designed from the outset to be reliable and secure, respectful of their privacy, and supported by trustworthy and responsive companies.

Legal, Technical and Social Aspects of Security

Regulating Information Security: A Matter of Principle?

Andreas Mitrakas · Silvia Portesi

European Network and Information Security Agency (ENISA)
{andreas.mitrakas | silvia.portesi}@enisa.europa.eu

Abstract

The widespread use of information technology in daily transactions has exacerbated the role of information security to protect information assets. Regulating network and information security has taken place through instruments and instantiations used for most of the time for different purposes that those strictly needed by information security itself. If information security is the answer to such requirements as confidentiality, integrity and availability of resources, setting up appropriate regulation is the means to set up binding frameworks. Regulation in this respect takes into account the requirements for a soft law approach that encompasses self regulatory frameworks and standards. A set of regulatory principles addressing the content and form of regulation in network and information security is an additional means to further enhance the impact of legislation and serve stakeholders.

1 Introduction

The widespread use of information technology in daily transactions has exacerbated the role of information security to protect information assets. The potential vulnerabilities that have been typically associated with transactions in the Public Administration and private enterprise challenge users and legislators alike. While information security is the answer to such requirements as confidentiality, integrity and availability of resources, establishing appropriate policies is the means to set up binding bilateral frameworks [Pfle00]. Furthermore a regulatory framework underpins certain high level requirements that need to be addressed at legislative level and complements the bilateral arrangements of individual users. Further up stream, there is, however, a latent need of principles of information security in order to guide the regulatory process. This paper addresses such questions as *is there a real need to regulate network and information security*, *under what conditions can it be taken up by the legislator* and *is law is an appropriate means to address regultary principles in information security*? Input to this paper has been drawn from the working group on regulatory aspects of network and information security that ENISA set up in 2006. The remainder of this paper addresses the following areas: an overview or regulatory principles in the light of legal positivism and their influence in the regulatory process of network and information security; specific regulatory considerations for network and information security; a set of regulatory principles that can be leveraged upon to the benefit of more concrete regulation in network and information security.

2 Working with rules

Positivism has vouched that law is a set of rules used to determine which behaviour will be punished and which will be coerced by the public power. If a specific case is not covered under this assertion, then a specialist, like a judge intervenes to determine the case. A legal right or obligation must directly

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2007), 3-17

fall under a legal rule [Dwor77]. Austin described three types of rules, legal, moral and religious ones. A basic set of legal rules is provided by the sovereign who, subsequently, empowers a judge to make new rules or re-assert known ones [Aust1832]. For H.L.A. Hart there is a system of primary and secondary rules whereby primary rules define what is allowed and what is not [Hart61]., Secondary rules affect the operation of primary rules and address three discreet areas namely, the uncertainty about what law is and whether a rule is valid, the rigidity of rules which addresses rules of change and allows laws to be varied, and how to resolve legal disputes from which rules of adjudication emerge. For Hart a legal system is the union of primary and secondary rules.

According to Dworkin, beyond set rules imposed by a designated authority, in a democracy rules also include policies and social standards that are promulgated through various channels associated with social functions. A policy sets out a standard to improve a certain feature of the society [Dwor77]. Standards in this sense should not be interpreted as technical standards that will be discussed separately further down in this paper, but rather as social norms that cut across the society. Principles on the other hand set out a social standard that is a requirement of justice, fairness, or morality. As Dworkin argues, positivism is a model of and for a system of rules that forces us to miss the important role of social standards that are not rules. Principles are rules that conflict and interact with each other so that each principle that is relevant to a particular problem and it provides a reason arguing in favour of but without necessarily stipulating a particular solution thereto [Dwor77]. Empowering a judge requires exercising discretion, which can be asserted when someone is charged of making decision as part of social standards set by an authority.

Long before any explicit manufacturer's liability rules came about, a New Jersey (US) Court, in the case *Henningsen v. Bloomfield Motors Inc*. (32 NJ 358, 1961), was faced with an important question of whether and to what extend a car manufacturer may limit its liability for a defective car. The manufacturer in question has set a contract clause signed to by the buyer which said that the manufacturer's liability for defects was limited to "making good" defective parts while "this warranty was in lieu of all other warranties, obligations and liabilities." Faced with a defective product the plaintiff argued that in his case additional expenses should be covered for by the manufacturer due to the defective product that he made available. At the time there was no statute to point to that would allow the plaintiff to support his argument. The Court in its reasoning took into account limitations in the principle of contractual freedom and it suggested that "in a society like ours where the automobile is a common and necessary adjunct of daily life, and where its use is so fraught with danger to the driver, passenger and the public, the manufacturer is under special obligation in connection with the construction promotion and sale of his car". Subsequently the Court refused to be taken as an instrument of inequity that is there to enforce a "bargain" in which one party takes advantage of the economic necessities of the other.

In *Henningsen,* the guidance of the Court was provided not so much from an established and firm background of rules, but rather from a set of social norms or standards that suggest that a Court cannot be used as an instrument to promote unfairness; except in case of fraud and wilful misconduct contractual freedom can be indeed limited to match social needs of the society. In the absence of a set of rules, exercising discretion provided the appropriate interpretation of a social standard and injected input in case law. Luhmann argues that the essence of positive law is that it is a decision; and to that the concept of positive law can be reduced to. A decision entails that law is not only promulgated through decision, but also is valid by the power of decision which subjects it to change [Luhm95]. In an environment where business needs prevail, adapting law enables it to be a powerful instrument for the wilful promotion and regulation of social and economic goals. Luckily, by virtue of an EU regulatory framework for information society services, we do not have to rely on assumptions such as those posed in *Henningsen* any more.

Setting up meta-rules on how to carry our regulation in those areas related to network and information security that has been deemed necessary, we observe the significant role that technical standardisation, for instance, plays in bringing together legal requirements with specific societal needs. Standardisation has emerged as a key EU policy area that complements the legislative process especially in such areas as products and technology. Standardisation policy in the EU goes back to the *Cassis de Dijon* case in which the European Court of Justice ruled that a product meeting the requirements of one member state should be legally made available in another; allowing the emergence of mutual recognition of technical standards as a matter of significant interest in the EU internal market (ECJ 120/78 of 20/02/79). The EU approach to technical harmonisation has resulted in limiting standards to technical specifications and safety requirements while reserving a prominent place for EU standards organisations such as the European Committee for Standardisation (CEN) and European Telecommunications Standards Institute (ETSI). This role for standards has gradually led to a soft approach that contains covers up for limitations emanating from a strict legislative process that can be seen as too narrow to address business and society needs. Technical standards, thus, provide a layer of "soft law" that deviates from a strict legislative approach [Send05] [Send04]. Often technical standards rely on a framework set out through a directive that is complemented by the appropriate standards. These standards are typically promulgated by the industry. The figure below provides an outlook of frequently used soft law instruments and their association with legislative instruments as they are often encountered in an EU context. A co-regulatory process links the requirements at the legislative level with the outcome of the standardization process that remains in line with the stipulations of the legislative framework.

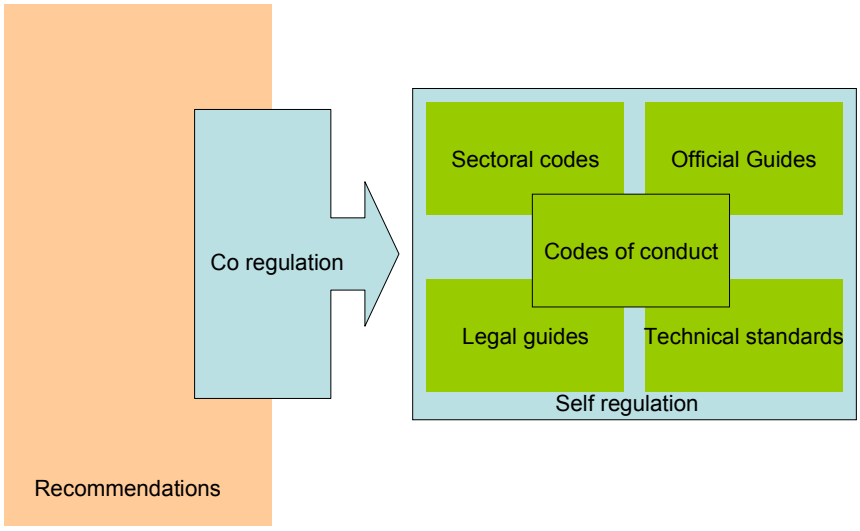

Figure 1: Soft Law instruments in a co-regulation approach

In a concrete situation related to network and information security we observe that Directive 1999/93/EC on a Community framework on electronic signatures, standards establishes a presumption of conformity, meaning that the electronic signature products that meet their requirements also comply with the legal requirements [Mitr06]. This approach has been underlined by the Commission Decision of 14 July 2003 on the publication of reference numbers of generally recognized standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council.

This Decision has endorsed and given legal effect to certain standards promulgated by the industry-led European Electronic Signatures Standardization Initiative (EESSI). Standards assume legal significance in cases where the law mandates them in order to give specific effect to a particular regulation within the EU.

With regard to security standards the ISO 27000 family of standards provides recommendations on information security management to those who are designated to initiate, implement or maintain security in an organization. This standard provides a common basis to pursue security management practices and indirectly to provide confidence in transactions. The ISO 27000 family of standards invokes the general requirement for network and information security and more specifically the requirements for confidentiality, integrity and availability. Integrity in this case encompasses the notions of authentication and non repudiation, which have both been subjected to legislation especially through the electronic signatures directive. The ISO 27000 standard is a self regulatory framework that extends to policies and agreements that all aim at setting up the conditions for network security safeguards within an organisation or in specific transaction frameworks [Mitr07]. The instrument of recommendation can be further used at EU level in order to highlight the significance and role of such standards but also of other instruments such as codes of conduct [Send05].

3 Making rules

Starting from mid-1990s, the technological revolution, characterised by the development and spread of information technologies, has reshaped the material basis of the society. “Economies throughout the world have become globally interdependent, introducing a new form of relationship between economy, state and society, in a system of variable geometry” [Cast04]. Adequate regulatory solutions, at national and supranational level, to face these changes, started to be discussed and adopted. In making rules in network and information society, some regulatory principles are followed. Sometimes, however there could be noted a discrepancy between the desired solution and the one made available by the legislator. Inefficient legislation might have further sipped in and influenced bilateral relationships, leading to regulatory solutions that could be a far cry from what was essentially needed in the first place, when regulation was deemed to be an appropriate solution. Especially at the level of regulatory principles a necessary condition to consider regards the efficiency of the offered solution.

The Coarse theorem gives a notion of what efficiency means when making an agreement. Referring to bilateral relationships, Coarse suggests that a contractual solution must take into account three factors: transaction costs, the efficiency of the outcome and the legal framework to lead to a regulatory solution [Poli89]. The efficiency of a regulatory solution, such as a contract for example also depends upon factors such as the social context, the transaction costs and the legal reality of the environment in which the legal solution is applied [Will05]. A regulatory solution should take such variables into account and include for example the cost of obtaining information, the negotiation cost, the gains of breaching a rule as opposed to possible costs like a reliance remedy or a restitution remedy, etc. If, for example, the cost of obtaining information in order to set up a regulatory framework is quite high such solution might not necessarily be a rational choice [Will05]. Determining the cost of obtaining information on the overall solution is yet another facet of the problem that cannot be easily reached.

There is an additional role, reserved to economic rules, which produces outcomes that are in the interest of everyone [Mitn80]. Economic rules aim at correcting market inefficiencies or failures which is an often appearing feature in a society. In a broad sense, regulation in this regard might include technical and consumer related standards, health and environment standards, competition policies, industry regulations etc [Hix99].

Rules provide incentives and set the limits of human interaction and behaviour with regard to an area of interest. Against this background rules that regard services can be seen as comprising of three general discreet categories being moral, social and economic ones. Economic rules, in specific, focus on these very incentives, in order to establish a system of fines that invokes the approach that recklessness is punished or compliance is rewarded. The flip side of these rules with an economic interest encompasses the concept of using a system of credits that it pays to educate and raise awareness in specific areas of interest. This paper suggests that general rules can be used to enhance the current level of security available to the beneficiaries of the information society as a whole in a way that enhances information society services. There is but limited need for specific formal rules as it is addressed further below. Rules can be based on the three main categories that are mentioned above, being moral, social and economic ones, in order to provide a framework for authorities, users and service providers alike in their efforts to make available or rely upon dependable and robust services that appropriately mitigate network and information security risks.

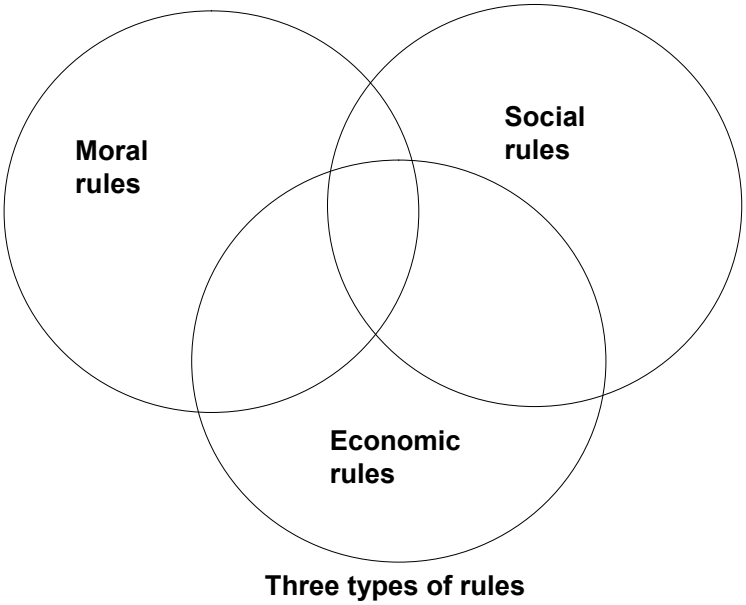

Figure 2: Three types of rules: moral, social and economic

When answering the question "what rules have to do with network and information security?" it is important to highlight the features of the Internet, upon which information society services are largely based in making the most of a secure service and transaction environment. A discreet case that related to information security concerns identity risks in information society that can be epitomised in the motto published along a synonymous cartoon in NY Times on suggesting that "*On the internet nobody knows that you are a dog*", as authored by Peter Steiner who wrote it in his July 1993 cartoon in NY Times. It is questionable whether the age old question regarding social responsibility, which goes: "*could a man resist the temptation of evil if he knew that his acts could not be witnessed*" could be successfully replied in the information age; apparently the reply at least in the real world appears to be 89% of the time [Boas61] [Levitt06]. The shift to avatars made available through the services of Second Life, Second Life is a 3-D virtual world entirely built and owned by its residents demonstrates the significance of this underlying identity drive in information society (http://secondlife.com/). An avatar is an Internet user's

own representation in the form of a three-dimensional model used in computer games. Avatars facilitate the need to take up a role, marking or altogether one's real identity and the Internet is a means that predominantly facilitates this need. Avatars can be deemed as an expression of an underlying social desire to act under an assumed identity that allows the user to authenticate itself in a virtual world. However desirable this approach can barely resemble reality and in a real life context it cannot be morally or socially justified as it would undermine trust. Therefore addressing authentication methods to ensure trust in user access or management for example becomes a priority area for information security.

Readjusting our focus on security, however, the relentless exposure of services, service providers and users to network and information society risks has made it an indispensable feature of information society to rely upon rules in order to ensure the confidentiality, integrity and availability of services. What are these rules that have already become available? Are there any principles that could be leveraged upon in order to ensure that acts and omissions do not necessarily leave services out in the cold?

This paper further examines the role of information security as a component of information society.

4 Information security: to serve and protect?

When examining the role of rules in network and information security it is important to highlight the potential role of rules in addressing the requirements of the information security community. This task becomes more apparent if taking a practical case regarding the protection of personal data and the role of its regulatory framework in Europe. The scope of information security measures in information society can be twofold. On one hand information security aims at protecting the interests of the service provider with regard to access the resources, which are necessary in order to deliver a service [FoBa01]. Security, however, can be used in order to ensure the protection of rights, such as privacy, in a way that the end user benefits. End user in this respect might be a natural person in its capacity as citizen or consumer etc. Additionally legal persons can benefit in terms of legal safety, compliance with regulations in highly regulated environments such as stock markets and the like. Personal data protection is this emblematic area where all stakeholders are better off if they protect data rather that ignore it. To the data controller personal data is an asset that can be leveraged upon in order to deliver meaningful services; as such the data controller has a duty to protect this asset [Ters06]. To the data subjects, on the other hand personal data represents a means to receive personalised services that requires protection due to its vicinity to the personal sphere of the protection of fundamental rights.

This heightened significance of rules in the area of personal data protection emanates from the strong cultural and legislative drive in the early seventies' Western Europe that led to the gradual adoption of data protection legislation. The European Union considered the global reach of certain aspects of data protection law that has led to the currently available European framework on data protection [Buel06].

When examining the needs in terms of rules of network and information society it is important to envisage the potential objectives that these rules might seek to play. Pursuant to the assumption regarding the protection of personal data it is clear that rules of any sort, in network and information security, serve the dual purpose of protecting fundamental rights and ensuring services rendered. Therefore there is a strong societal drive that powers rule making as well as a strong economic drive that sets out a framework of incentives and fines in case of breach as discussed in the previous section. An underlying strong moral element might remain a little out of sight because it might be embedded in the societal requirement that is manifested through legislation at the Member States level. Such moral element associates, however rather with the moral premise of the right "to be left alone", the core element of privacy, rather with the specific mechanics of how such an arrangement might work out in terms of protecting personal

data. As the basic requirement on privacy stated in article 8 of the Council of Europe Convention on Human Rights and Fundamental Freedoms and then in articles 7 and 8 of the Charter of Fundamental Rights of the European Union, has also been enshrined in legislation such as Directive 95/46/EC etc., the associations among the moral and societal elements become apparent.

5 What's law got to do with it?

An emerging legal framework that derives from the role that information plays in modern day transactions is setting up the pace for developments in business and banking. Organizations that implement appropriate security measures mandated by industry regulations or legislation expect to benefit from the mitigation of potential liability of shareholders, employees, customers, trading partners or other third parties involved in a transaction.

The set up of the European Network and Information Security Agency (ENISA) to address selected network and information security matters has emerged as a new element in supporting the approximation of laws in the Member States in the framework of the First Pillar regarding the EU Internal market. To this effect the decision of the European Court of Justice asserted that the principle of article 95 of the Treaty regarding the EU Internal Market is well served just by setting up a measure such as ENISA along with the array of legislative measures undertaken by the European Union over time.

The ENISA case (C-217/04), UK v. EP & Council presents an example of challenging the legal basis of EU Agency based on article 95 of the Treaty on the EU Internal Market. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (hereinafter, ENISA Regulation) has been challenged before the European Court of Justice (hereinafter, ECJ) with regard to the legal basis of ENISA servicing EU Internal Market purposes on the basis of article 95 of the Treaty (ex art. 100a) While art. 95, maintains the system of majority voting it involves co-decision between Council and parliament under art. 251 of the Treaty. It has been noted that this approach results in greater intermediary powers to the Commission at the Council level since gaining a qualified majority suffices for a vote [Weil91]. In its ruling ECJ affirmed that the ENISA Regulation was yet another measure in a broader EU framework regarding network and information security. Being far from the only measure regarding the approximation of laws, as the plaintiff had claimed, the ENISA Regulation has been part of a broader set of regulatory measures composed by the framework Directive and including specific Directives that address various aspects of the EU Internal Market in the area of electronic communications. The ECJ decision highlighted the potential divergence in Member State laws that could emanate from differences in transposing Directives in this area. The ECJ ruling also removed uncertainty by linking article 3 of the ENISA Regulation (EC) 460/2004 with the objectives of the framework Directive as well as of specific Directives in the area of network and information security.

Additional requirements associated with the area of specific activity that regulation is called in to serve also influence the way that regulation is promulgated. For example the need for the end user to become aware of risks and measures to mitigate them or the need for security measures to facilitate or at least to refrain from hindering interoperability can be seen as measures of specific interest that could typically sip in regulation. The table below makes some associations between areas of network and network security and types of rules, such as the above.

Table 1: Ad hoc substance areas and their relation to types of rules

	***Ad hoc* sample substance areas**				
	Data protection	**Privacy**	**Awareness**	**Interoperability**	**Information society Applications**
Social rules	X	X	X	X	X
Moral rules		X	X		
Economic rules	X	X		X	X

The table above is a plain indication of the associations that certain *ad hoc* sample substance areas might have with the rules of choice that can be used as regulatory instrument in a network and information security framework. Essentially this table demonstrates that not all areas of interest or instruments available in network and information security merit or require being associated with a need to have formal rules with an economic impact. As discussed above these rules with an economic impact are essential formal rules promulgated by the legislator. Inevitably on several occasions a regulation can rest at the level of bilateral arrangements in the framework of self regulation as a reflection of a moral requirement or a social constraint imposed in the transaction. While moral or social constraints address the needs of portions of the society they might not have a universal interest or create a grand impact that merits the attention of the legislator. In this regard self regulation may produce results that are sufficiently efficient and therefore more desirable.

6 A Working Group

The ENISA Working Group on Regulatory Aspects of network information security (hereinafter, WG-RANIS) carried out an overview of EU legislation as it has become available in the area of network and information security (http://www.enisa.europa.eu/pages/ENISA_Working_group_RANIS.htm). The target of this Working Group has been to compile a list of activities in an effort to represent state-of-art in an inventory-centric approach that addresses legal actions on issues relevant to network and information security.

In their report this Working Group came up with a significant number of legislative instruments (over 65 in total) that cover the period as of 1990. In total more that 65 instruments were collected that cover a broad range of EU policy and law making [RANIS06]. The areas of legislative attention with an interest for network and information security cover for example: security and financial services, intellectual property rights, corporate and IT governance, data authentication, data protection and retention, electro-

nic communications, networks and services. This very broad approach that has yet to be systematically addressed had been spared no legislative instruments in order to meet the regulatory requirements of network and information security. In this regard regulations, directives, recommendations, resolutions etc., had all been invariably used in to promulgate the legislative framework of network and information security. The instruments of choice to give effect to this framework can be seen in the radar table below that was compiled by the Working Group itself [RANIS06]:

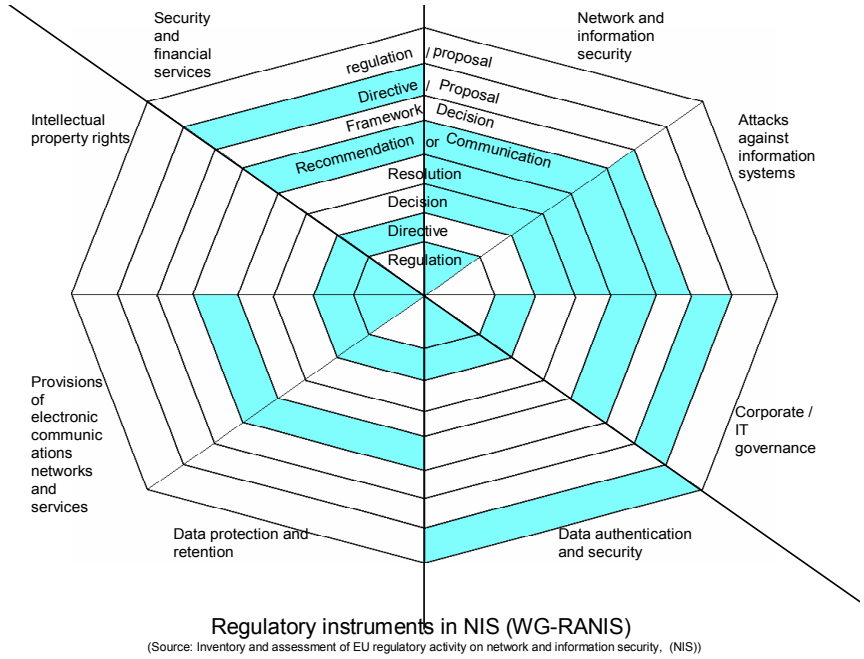

Figure 4: Regulatory instruments in network and information security

7 Regulatory Principles

A set of underlying principles is necessary to guide legislation towards efficient regulation that is commensurate with societal needs. Such legislation should recognise lateral societal needs that are not necessarily represented in legislation itself but which are, nevertheless represented in the form of standards or bilateral arrangements. The principles that WG-RANIS has seen as looming can be found in the report itself. The section below relies on some of these principles, and provides an overview and explanation regarding the regulatory framework at large.

Multi facet legislation

The network and information security regulatory framework is typically multi faceted comprising of several layers, such as privacy, telecommunication, business applications, authentication and identity, intellectual property protection, competition, taxation and electronic communication emerge as interest areas for network and information security. Therefore, as Matsuura points out, there are several substantive categories of law applying to information and network security, such as intellectual property law, privacy law, law of contracts and commercial transactions, consumer protection law, anti-trust law, property law, etc. [Mats02]. Interlacing the underlying legislative principles of various areas can be challenging for the legislator of network and information security who risks voting potentially con-

flicting rules. Hence, sufficient consideration could be given to legislation of lateral areas in a way that adapts new legislation to the existing framework.

Moreover, network and information security addresses a framework that benefits directly or indirectly a multitude of business, government and application areas that merit a legislative approach. In developing new regulations or updating those already existing in the field of network and security, regulators could take into account the impact they might have on all the different stakeholders and to consider the different possibilities the various areas of law might offer.

Political background
In the EU, the "Bangemann Report" was one of the first reports on the then new subject area of information and communication technology and its implications for the society; this report was prepared by the High Level Expert Group containing recommendations presented to the Council to ensure competitiveness for European enterprises the international service market [COM94] and [KLP+06]. In March 2000, at the Lisbon Summit meeting "Towards a Europe of Innovation and Knowledge", EU Heads of State and Government agreed to make the EU the most innovative knowledge-based society by 2010. The eEurope 2005 Action Plan was launched at the Seville European Council in June 2002 and aimed to "stimulate secure services, applications and content based on a widely available broadband infrastructure". The eEurope 2005 initiative ended in 2005 and was followed by the i2010 initiative, which is strategic policy framework laying out guidelines for the information society and the media until 2010. The political drive behind eEurope has shaped the legislative framework in several of the areas adjacent to network and information security. The inevitable embracing between politics, policy and law underline that legal initiatives often need to have political support in order to become effective and enforceable, while they maintain the interest of the stakeholders.

A global role for Europe
In a networked world, EU legislation on information security should not be drafted in isolation from the rest of the world. While being a legislative pioneer, as it has been the se for the EU in the area of personal data protection, makes it a hard case to prove to the rest of the world, in the long run the results can span across several countries that adopt the EU promulgated model. Appropriate communication at an international level is necessary along with coordination that advances EU premises in network and information security and asserts that network and information security risks cannot be isolated and dealt with in one region or sector of industry only. It is important that the EU maintains a continuous dialogue, for instance, with the Organization for Economic Co-operation and Development (OECD), the G8, the World Intellectual Property Organization (WIPO), the World Trade Organization (WTO), and International Telecommunication Union (ITU). The immediate effect thereof is to avoid duplications in legislation and regulation and use synergies to reach world-wide an enhanced level of network and information security.

Soft law approach
Since traditional regulatory instruments, such as legislation, in some cases turn out not to be easily applicable or effective (in particular in the on-line environment), other modalities of regulations can be considered as possible alternatives [Send05]. Approaches such as co-regulation and self regulation might service well the set up of requirements for network and information security. Providing a legal mantel under a framework directive or a recommendation is an essential extension to give legal validity to some of those standards, especially the ones having the most far-reached consequences for the stakeholders. It is also important to maintain a view on building the regulatory requirements in the architecture of the security standard at hand, an approach that has the obvious benefit of cutting down on compliance tests and reaffirming trust [Lessi06].

Identity, Information Security and Rights Management

Design Rationale behind the Identity Metasystem Architecture

Kim Cameron · Michael B. Jones

Microsoft
{kcameron | mbj}@microsoft.com
http://www.identityblog.com/, http://research.microsoft.com/~mbj/

Abstract

Many of the problems facing the Internet today stem from the lack of a widely deployed, easily

understood, secure identity solution. Microsoft's "InfoCard" project and the Identity Metasystem vision underlying it are aimed at filling this gap using technology all can adopt and solutions

all can endorse, putting users in control of their identity interactions on the Internet. The design decisions presented in this paper are intended to result in a widely accepted, broadly applicable, inclusive, comprehensible, privacy-enhancing, security-enhancing identity solution for the Internet. We present them and the rationale behind them to facilitate review of these design decisions by the security, privacy, and policy communities, so that people will better understand Microsoft's implementations, and to help guide others when building interoperating implementations.

1 Introduction

1.1 The Challenge: A Ubiquitous Digital Identity Solution for the Internet

By definition, for a digital identity solution to be successful, it needs to be understood in all the contexts where you might want to use it to identify yourself. Identity systems are about identifying you self (and your things) in environments that are not yours. For this to be possible, both your systems and the systems that are not yours – those where you need to digitally identity yourself – must be able to speak the same digital identity protocols, even if they are running different software on different platforms. In the case of an identity solution for the entire Internet, this is a tall order. It means that, to succeed, the solution will need to be adopted by the wide variety of operating systems, browsers, and web servers that collectively implement the phenomenon we know of as "the Internet". ".

1.2 Practical Considerations

To have any hope of such widespread adoption, we believe that any Internet-scale identity solution will need to satisfy these practical considerations:

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2007), 115-127

- **Improved Security and Privacy:**
  To be widely adopted, platform and software vendors will need to be convinced that the solution results in improvements in the overall Internet security landscape. Likewise, consumers (and their advocates) will need to be convinced that the solution improves the consumer privacy landscape.
- **Inclusive of Technologies:**
  There are a number of identity technologies in widespread use today (Kerberos, X.509, SAML, etc.) with more being invented all the time. To gain wide acceptance, the solution should be able to leverage existing identity technologies and deployments, incorporating them as part of the solution and building upon their strengths, rather than calling for their wholesale replacement.
- **Inclusive of Scenarios:**
  The solution must be broadly applicable across a wide range of use cases, even accommodating those with conflicting requirements. For instance, in many cases users will want guarantees that their identity providers can't accumulate a record of the sites they visit. However, in some governmental and financial settings, an audit record of sites visited using an identity may be required. Both kinds of identities should be able to be accommodated. At an even more basic level, the solution must be applicable not just on workstations but also on different devices such as wireless mobile devices and cell phones.
- **Incrementally Deployable:**
  The solution must coexist with and complement existing authentication systems, rather than calling for a "forklift upgrade" or "flag day" where existing solutions must be replaced by the new one all at once.

1.3 Architecture of a Proposed Solution

Such a solution, the Identity Metasystem [Microsoft 05a], has been proposed and some implementations are under way. The Identity Metasystem is based upon a set of principles called the "Laws of Identity" [Cameron 05b]. The Laws are summarized in Appendix A. The

Laws are intended to codify a set of fundamental principles to which a universally adopted, sustainable identity architecture must conform. The Laws were proposed, debated, and refined through a long-running, open, and continuing dialogue on the Internet [Cameron 05a]. Taken together, the Laws were key to defining the overall architecture of the Identity Metasystem.

While the Laws of Identity have undergone broad review and been met with significant acceptance, that's certainly not the end of the story. While the Identity Metasystem is designed in accordance with the Laws, there are also numerous practical design decisions that had to be made to translate the vision into working, interoperable systems. The purpose of this paper is to publish the design decisions underlying the Identity Metasystem architecture and the rationale behind them. This is intended both to enable a deeper understanding of the problems that this solution addresses and to enable discussion of these design decisions by the security, privacy, and policy communities.

2 Identity Problems on the Internet and an Overview of the Proposed Solution

The section briefly describes the problems motivating the need for a new identity solution for the Internet and gives an overview of the mechanisms that the Identity Metasystem employs to do so.

2.1 The Internet's Problems are often Identity Problems.

Many of the problems facing the Internet today stem from the lack of a widely deployed, easily understood, secure identity solution. Microsoft's "InfoCard" project and the Identity Metasystem vision underlying it are aimed at filling this gap using technology all can adopt and solutions all can endorse, putting users in control of their identity interactions on the Internet. A comparison between the brick-and-mortar world and the online world is illustrative: In the brick-and-mortar world you can tell when you are at a branch of your bank. It would be very difficult to set up a fake bank branch and convince people to do transactions there. But in today's online world it's trivial to set up a fake banking site (or e-commerce site …) and convince a significant portion of the population that it's the real thing. This is an identity problem. Web sites currently don't have reliable ways of identifying themselves to people, enabling imposters to flourish. One goal of InfoCard is reliable site-touser authentication, which aims to make it as difficult to produce counterfeit services on the online world as it is to produce them in the physical world. Conversely, problems identifying users to sites also abound. Username/password authentication is the prevailing paradigm, but its weaknesses are all too evident on today's Internet. Password reuse, insecure passwords, and poor password management practices open a world of attacks by themselves. Combine that with the password theft attacks enabled by counterfeit web sites and man-in-the-middle attacks and today's Internet is an attacker's paradise. The consequences of these problems are severe and growing. Last year the number of "phishing" sites was growing at over 1000% per year [Anti-Phishing 05]. Online banking activity is declining [Gartner 05]. The recent FFIEC guidance on authentication in online banking reports that "Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation" [FFIEC 05]. Consumer trust of the Internet is low and dropping. The status quo is no longer a viable option.

2.2 "InfoCard" and the Identity Metasystem

The code-named "InfoCard" project at Microsoft is a joint effort with a diverse coalition of contributors across the computer industry to produce an authentication solution for the Internet that can:

- be widely accepted,
- work in a broad range of identity contexts,
- utilize existing authentication technologies, including multiple factors,
- incorporate new authentication technologies as they are invented, and possibly most importantly,
- enable users to simply and consistently make informed and positive authentication decisions on their own behalf.

The result of this effort is known as the Identity Metasystem [Microsoft 05a], an overview of which is contained in this section. As previously mentioned, the Identity Metasystem is based upon a set of principles developed through an open industry dialog [Cameron 05a] called the Laws of Identity [Cameron 05b]. What do we mean by an "Identity Metasystem"?

This concept is probably most easily introduced through an analogy.

Before 1982, the networking world was fragmented. If you wanted to write a networkenabled application you had to choose what network to write it for: Ethernet, Token Ring, ArcNet, X.25, etc. The invention of a Network Metasystem, the Internet Protocol (IP), changed all that. It made it possible to write networking applications that worked across networks without knowing the particulars of each

network. It even enabled those applications to work with new networks that hadn‘t been invented yet, such as 802.11 wireless networks.

Digital identity is similarly fragmented today. If you want to write an identity-enabled application, you have to choose which identity system to write it for, such as Kerberos, SAML, X.509, Liberty, custom username/password systems, etc. The Identity Metasystem is intended change all that, just as IP did for networking. It will make it possible to write identity-enabled applications that can work across multiple identity systems and can even use new identity systems as they are invented and connected to the Identity Metasystem. This analogy holds true in another way. IP didn't compete with or replace the individual networks such as Ethernet — it used them. Similarly, the Identity Metasystem doesn't compete with or replace individual identity technologies such as Kerberos, Liberty, X.509, SAML, etc. — it uses them. That's why it's called an identity metasystem —it's a system of systems, tying individual identity systems into a larger interoperable metasystem (see Law 5). By allowing different identity systems to work in concert, with a single user experience, and a unified programming paradigm, the metasystem shields users and developers from concern about the evolution and market dominance of specific underlying systems, reducing everyone's risk and increasing the speed with which technology can evolve.

2.3 Roles within the Identity Metasystem

Different parties participate in the metasystem in different ways. The three roles within the metasystem are:

- **Identity Providers,** which issue digital identities. For example, credit card providers might issue identities enabling payment, businesses might issue identities to their customers, governments might issue identities to citizens, and individuals might use self-issued identities in contexts like signing on to web sites.
- **Relying Parties,** which require identities. For example, a web site or online service that utilizes identities offered by other parties.
- **Subjects,** which are the individuals and other entities about whom claims are made. Examples of subjects include people, companies, and organizations.

2.4 Claims-Based Identities and InfoCards

In the Metasystem, digital identities consist of sets of claims made about the subject of the identity, where "claims" are pieces of information about the subject that the issuer asserts are valid. This parallels identities used in the real world. For example, the claims on a driver's license might include the issuing state, the driver's license number, name, address, sex, birth date, organ donor status, signature, and photograph, the types of vehicles the subject is eligible to drive, and restrictions on driving rights. The issuing state asserts that these claims are valid. The claims on a credit card might include the issuer's identity, the subject's name, the account number, the expiration date, the validation code, and a signature. The card issuer asserts that these claims are valid. The claims on a self-issued identity, where the identity provider and subject are one and the same entity, might include the subject's name, address, telephone number, and e-mail address, or perhaps just the knowledge of a secret. For self-issued identities, the subject asserts that these claims are valid.

In the client user interface, each of the user's digital identities used within the metasystem is represented by a visual "Information Card" (a.k.a. "InfoCard", the source of this technology's codename). The user selects identities represented by InfoCards to authenticate to participating services. The cards themselves represent references to identity providers that are contacted to produce the needed claim data for

an identity when requested, rather than claims data stored on the local machine. Only the claim values actually requested by the relying party are released, rather than all claims that the identity possesses (see Law 2).

2.5 Putting the User in Control

One of the fundamental tenets of the Info- Card work is that users must be in control of their identity interactions (see Laws 1 & 2). Among other things, this means that users must be given the choice of which identities to use at which services, they must know what information (which claims) will be disclosed to those services if they use them, and they must be informed how those services will use the information disclosed. In the offline world, people carry multiple forms of identification in their wallets, such as driver's licenses or other government-issued identity cards, credit cards, and affinity cards such as frequent flyer cards. People control which card to use and how much information to reveal in any given situation.

Similarly, the Identity Metasystem makes it easier for users to stay safe and in control when accessing resources on the Internet. It lets users select from among a portfolio of their digital identities and use them at Internet services of their choice where they are accepted. The met system enables identities provided by one identity system technology to be used within systems based on different technologies, provided an intermediary exists that understands both technologies and is willing and trusted to do the needed translations. Part of being in control that's all too often overlooked is that to be in control, you must be able to understand the choices you're presented with (see Laws 6 & 7). Unless we can bring users into the identity solution as informed, functioning components of the solution, able to consistently make good choices on their own behalf, we won't have solved the problem. Many identity attacks succeed because the user was fooled by something presented on the screen, not because of ins cure communication technologies. For example, phishing attacks occur not in the secured channel between web servers and browsers — a channel that might extend thousands of miles — but in the two or three feet between the browser and the human who uses it.

The Identity Metasystem, therefore, seeks to empower users to make informed and reasonable identity decisions by enabling the use of a consistent, comprehensible, and self-explanatory user interface for making those choices. One key to securing the whole system is presenting an easy-to-learn, predictable user interface that looks and works the same no matter which underlying identity technologies are employed. Another key is making important information obvious — for instance, displaying the identity of the site you're authenticating to in a way that makes spoofing attempts apparent. Likewise, the user must be clearly informed which items of personal information relying parties are requesting, and for what purposes. This allows users to make informed choices about whether or not to disclose this information.

2.6 Authenticating Sites to Users

To prevent users from being fooled by counterfeit sites, there must be a reliable mechanism enabling them to distinguish between genuine sites and imposters. Our solution utilizes a new class of higher-value X.509 site certificates being developed jointly with VeriSign and other leading certificate authorities. These higher-value certificates differ from existing SSL certificates in several respects. First, these certificates contain a digitally signed bitmap of the company logo. This bitmap is displayed when the user is asked whether or not they want to enter into a relationship with the site, the first time that the site requests an InfoCard from the user.

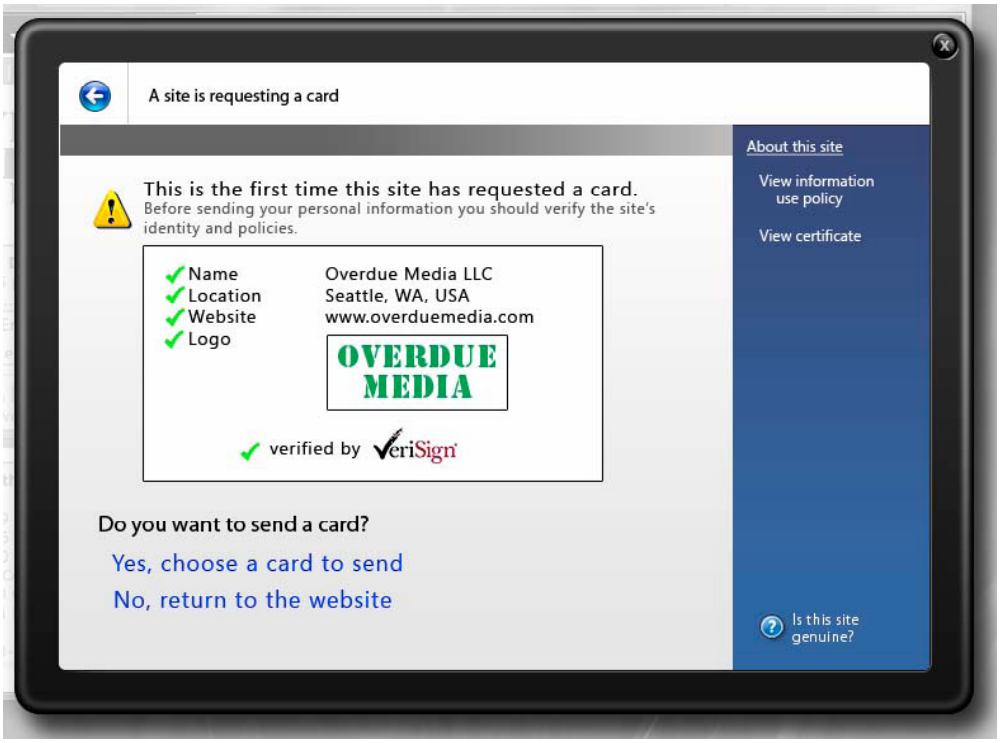

Figure 1: Site Verification Screen

Second, these certificates represent higher legal and fiduciary guarantees than standard certificates. In many cases, all that having a standard site certificate guarantees is that someone was once able to respond to e-mail sent to that site. In contrast, a higher-value certificate is the certificate authority saying, in effect, "We stake our reputation on the fact that this is a reputable merchant and they are who they claim to be". Users can visit sites displaying these certificates with confidence and will be clearly warned when a site does not present a certificate of this caliber. Only after a site successfully authenticates itself to a user is the user asked to authenticate himself or herself to the site. To make this all more concrete, Figure 1 shows an example of what a screen displayed upon a user's first access to a relying party accepting "InfoCards" might look like. As this example shows, the screen can include the name, location, web site URL, and logo of the organization whose identity is being approved (such as Overdue Media). It can also include the name and logo of the organization that has verified this information (such as VeriSign). To help the user make good decisions, what's shown on the screen varies depending on what kind of certificate is provided by the identity provider or relying party. If a higher-assurance certificate is provided, the screen can indicate that the organization's name, location, website, and logo have been verified, as shown in Figure 1. This indicates to a user that this organization deserves more trust. If only an SSL certificate is provided, the screen would indicate that a lower level of trust is warranted. And if an even weaker certificate or no certificate at all is provided, the screen would indicate that there's no evidence whatsoever that this site actually is who it claims to be. The goal is to help users make good decisions about which identity providers they'll let provide them with digital identities and which relying parties are allowed to receive those digital identities.

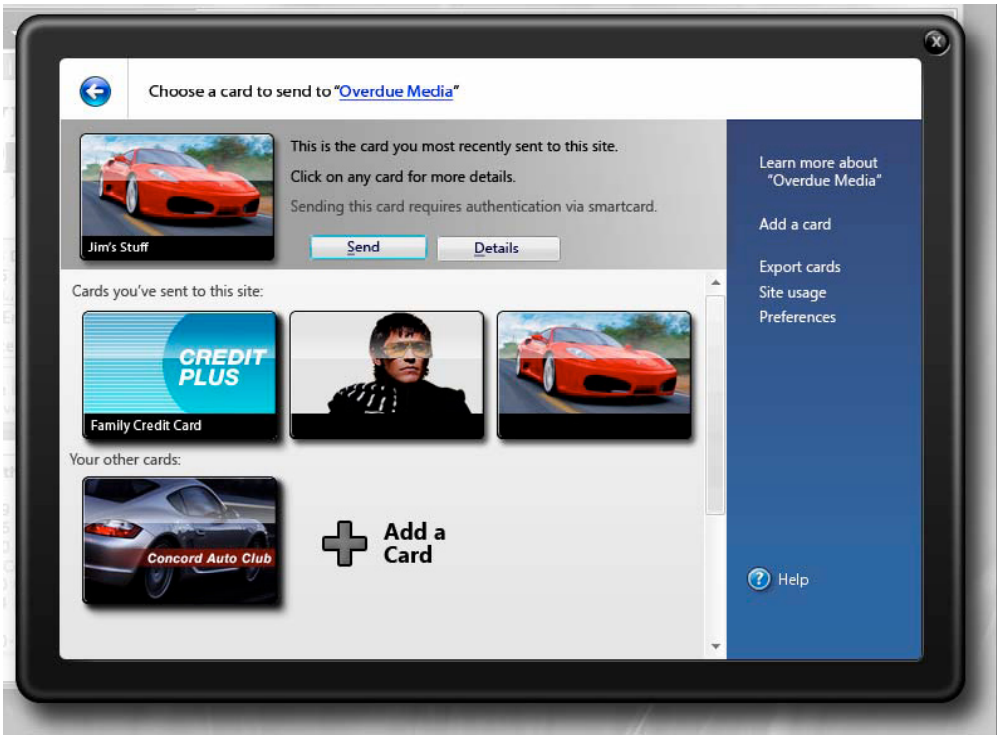

Figure 2: Identity Selector Screen

2.7 Authenticating Users to Sites

InfoCards have several key advantages over username/password credentials:

- Because no password is typed or sent, by definition, your password can not be stolen or forgotten.
- Because authentication is based on unique keys generated for every InfoCard/site pair (unless using a card explicitly designed to enable cross-site collaboration), the keys known by one site are useless for authentication at another, even for the same InfoCard.
- Because InfoCards will resupply claim values (for example, name, address, and e-mail address) to relying parties that the user had previously furnished them to, relying parties do not need to store this data between sessions. Retaining less data means that sites have fewer vulnerabilities. (See Law 2.)

InfoCard implements a standard user interface for working with digital identities. Perhaps the most important part of this interface, the screen used to select an identity to present to a site, is shown in Figure 2. As this screen shot illustrates, each digital identity is displayed as an InfoCard. Each card represents a digital identity that the user can potentially present to a relying party. Along with the visual representation shown above, each card also contains information about a particular digital identity. This information includes what identity provider to contact to acquire a security token for this identity, what kind of tokens this identity provider can issue, and exactly what claims these tokens can contain. By choosing to use a particular card, the user is actually choosing to request a specific security token with

a specific set of claims created by a specific identity provider. But from the user's perspective, they're simply selecting an InfoCard to use at a site.

2.8 Protocols Behind the Identity Metasystem

The Identity Metasystem is built on a small number of interoperable Web Services (WS-*) protocols. Specifically, the encapsulating protocol used for claims transformation within the Metasystem is WS-Trust [WS-Trust 05]. Format and claims negotiations between participants are conducted using WS-MetadataExchange [WSMetadataExchange 04] and WS-SecurityPolicy [WS-SecurityPolicy 05]. Finally, messages are secured using WS-Security [WS-Security 04]. These protocols enable building a platform independent Identity Metasystem and form its "backplane". Like other Web services protocols, they also allow new kinds of identities and technologies to be incorporated and utilized as they are developed and adopted by the industry. To foster the interoperability necessary for broad adoption, the spec fications for these (and other) WS-* protocols are published and are freely available, have been or will be submitted to open standards bodies, and allow implementations to be developed royalty-free. Deployments of existing identity technologies can be leveraged in the metasystem by implementing support for the small number of WS-* protocols above. Examples of technologies that could be utilized via the metasystem include LDAP claims schemas; X.509, which is used in Smartcards; Kerberos, which is used in Active Directory and some UNIX environments; and SAML, a standard used in inter-corporate federation scenarios.

3 Design Decisions behind the Identity Metasystem

This section lists many of the key design decisions behind the Identity Metasystem architecture and gives the rationale for them.

3.1 Protocol ≠ Payload

There are a number of forms of digital identity in use today such as Kerberos, X.509, SAML, and username/password systems, with more being invented all the time. Each typically represents identities in a different manner, and yet it is highly desirable to be able to utilize all these kinds of identities within the same identity solution. While some identity systems have developed custom communication protocols tied to particular identity formats, doing so results in little or no interoperability between the different systems using those incompatible protocols. Instead, we decided to employ a single encapsulating protocol set capable of utilizing all identity payload formats in a common manner. Specifically, the protocol set was chosen to enable specification of requirements, negotiation of capabilities, transmission of payloads, and transformation of payloads, all in a format independent manner. This means that the encapsulating protocol remains stable even as the types of payloads used evolve.

3.2 Identity Selector ≠ Identity Provider

The Identity Metasystem employs software on each platform that lets users choose an identity from among their portfolio of identities to use for each authentication. This software is called the Identity Selector, and is invoked each time the user needs to make a choice of identities.

(Figure 2 shows a screen shot of an Identity Selector.) A key decision was to implement an Identity Selector that is independent of any specific identity provider, technology, or operator.

Smart Tokens, eID Cards, Infrastructure Solutions and Interoperability

Infrastructure for Trusted Environment: In Search of a Solution

Claire Vishik · Simon Johnson · David Hoffman

Intel Corporation
{claire.vishik | simon.johnson | david.hoffman}@intel.com

Abstract

Millions of PCs are currently sold equipped with a Trusted Platform Module, TPM, serving as a root of trust on the platform. Trusted Computing as an area of security has acquired significant visibility, and many new products and a growing number of research projects in areas ranging from virtualization to network security are based on Trusted Computing technologies and vision. In order to fully realize the vision of the Trusted Computing community, dedicated or compatible trust infrastructure for verification and attestation is required. Similar to other trust-enabling technologies, Trusted Computing needs an infrastructure that can verify the claim that a device is genuine and can be trusted to take part in a transaction, in which it is involved. Such an infrastructure will enable an environment where individuals can use the technology for protected transactions and potentially employ less risky authentication methods. This paper explores the role of infrastructure in Trusted Computing, starting with the discussion of the infrastructure's importance and issues in trust establishment, followed by the description of the basics of Trusted Computing functionality requiring infrastructure support. We use examples of other trust enabling infrastructures, such as general-purpose PKI and infrastructure for Identity Federation to highlight common approaches. Finally, we touch upon economics of trust and intermediation, in order to define potential models for building enabling infrastructure for Trusted Computing.. While the paper doesn't propose concrete solutions for the infrastructure problem in Trusted Computing, some possible avenues of building the necessary framework are outlined.

1 The Problem of Trust Establishment

Establishing and verifying identity of an individual or a device in a networked environment has always presented a serious problem [CHHD06, FRKH00]. Although access control is instrumental in permitting the use of networks or access to data only to the accounts that have proper authorization and have been authenticated, there are numerous open issues. One of the premises of Trusted Computing is to provide a foundation of a trusted platform and trusted environment, thus enabling the users to trust their own devices and other devices on the network In order for a user or device to be trusted, it is not sufficient to be successfully authenticated or to possess a valid key or credential. An authorized user can access restricted resources from a compromised device or network. Or an unauthorized user may be using legitimate credentials belonging to a different individual as well as a compromised platform. While some protocols make it possible to identify a device accessing the network, outside of Trusted Computing, there is no standard procedure to ascertain that the device is running an expected configuration or that the platform has not been compromised. Increased protection of the network helps protect the users of the network and information stored and processed by the users of the network.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2007), 217-225

Trusted Computing Group defines technical trust as the assurance that the "entity behaves in an expected manner for the intended purpose.[1]" In a more narrow sense, we can say that a platform can be trusted if it is running an expected configuration

In order for advanced platforms to deliver real business value and leverage usage models benefiting from a trusted environment and interaction with other trusted devices and users, we need to devise supporting protocols helping platforms and services to identify themselves, trust identification provided by the other parties, and engage in activities within the framework where security risks are well understood [KALP05]. To achieve this level of trust, users, platforms, and services have to use more detailed profiles and ensure information in those profiles can be validated by the infrastructure that is trusted by the participants.

Software can be hacked by software, and parameters and messages within software systems can be misrepresented with greater ease. Therefore, hardware-based trust is typically considered as providing greater assurance due to its greater resistance to tampering. Hardware-based trust has always been a strong advantage of Trusted Computing. But because hardware platforms use software systems for user-focused functionality, in a truly trusted environment it is important to be able to share information about the state of various components, both hardware and software, and create a mechanism to trust the information contained in these reports.

TCG (Trusted Computing Group) defined platform credentials (Endorsement Credentials) to establish that the platform has a genuine TPM. By signing this credential, TPM manufacturer, platform OEM, or organizational IT can make an assertion that a TPM with certain properties has been installed on a platform. This assertion allows those interacting with the platform to evaluate the level of trust the platform in question should be accorded. For example, if the TPM manufacturer signed the credential, it will be necessary to determine if the manufacturer can be trusted. If an attestation protocol is used, it will be important to establish if the Certificate Authority (Privacy CA) involved in the process is trustworthy. The credential can contain additional information about functionality that can help establish if the capabilities are adequate to support the necessary level of trust.

In many cases, more information may be necessary to provide greater assurance and elicit greater trust. In a simplified case, if we know that a platform from Company X network is accessing an application at Company Y with a user account that is properly authorized and authenticated, trust developed in the course of the transaction may be limited. But if we know that platform from Company X is running an expected configuration, has a hardware root of trust, and the user is biometrically authenticated, a higher level of trust is possible.

Yet greater disclosure of facts is likely to have an impact on users' privacy, and therefore an additional set of requirements for privacy protection is necessary for trust infrastructure that supports more advanced usage models. In this environment, platforms and services need to apply the principle of the least privilege, meaning that every module, user, or program must be able to access only information and resources that are necessary for their legitimate purpose. A related requirement for platforms and infrastructure in the environment requiring greater disclosure is to be able to apply policies in order to carry out minimal levels of disclosure necessary to establish the necessary level of trust [FLLU05]. If, in addition to the principle of the least privilege applied consistently, platforms and infrastructure can exchange messages including varying levels of detail, the resulting variable disclosure will provide greater privacy protection and support higher levels of trust in cases when it is mutually necessary for the participants in the attestation process. More flexible policies associated with disclosure can support

1 Definition of technical trust used by the Trusted Computing Group (TCG).

multiple levels of trust, ranging from a confirmation of the membership in a large group to details of the state of the components on a platform.

Finally, in a complex environment characterized by varying levels of trust and multiple types of trusted devices, the use of standard protocols to establish trust will have to be adopted, in order to enable the participants to understand and interpret policies and reports provided in a trusted network.

It is evident that trust establishment for advanced platforms requires intelligent infrastructure that can evaluate evidence of trust from a variety of sources and in accordance with flexible context-driven policies.

2 Background: Trusted Computing and TPM

Among recognized attributes of a trusted device, some are internal to the device (e.g. isolation or user and supervisor processes, isolation of programs, protected long term storage and identification of the current configurations), but other attributes require supporting infrastructure (e.g. ability to obtain verifiable reports of the platform identity using an attestation mechanism for the external observer to confirm the validity of these reports) [GRAW06]

Some important capabilities of TPMs defined in TCG specifications rely on trust infrastructure – a Certificate Authority (Privacy CA) or a CA serving as a verifier for DAA (Direct Anonymous Attestation) protocol. Although TPMs have become ubiquitous on branded PCs, with many models including a TPM as a standard component and some organizations, e.g. in the financial sector, standardizing on platforms with TPMs, two factors precluded the vision of Trusted Computing from being realized completely. One is the lack of consistent support in standard business operating systems, although XEN, Microsoft Vista, and improved TPM drivers are ushering in a more favourable environment. The other is the lack of dedicated or compatible trust infrastructure of CAs supporting attestation, authentication, and, in some cases, verification. The sections below describe TPM components and functions, highlighting the role of the trust infrastructure.

2.1 TPM Functions: Attestation

TPMs are self-contained computing environments that have perimeter protection and can perform certain computations without relying on external resources. A TPM consists of a Program Code Segment (PCS), a small CPU that executes the PCS, non-volatile memory where persistent keys and secrets are stored, and active memory used to store non-persistent secrets that are lost on power-off.

Attestation refers to a set of functions and protocols that enable a TPM to prove to a remote entity that the platform is using a particular configuration. This assertion can constitute a foundation for trust establishment. The attestation claim must be supported by a trustworthy source. To perform attestation, a TPM uses an Attestation Identity Key (AIK) to quote, or sign, platform measurements sent as a part of the attestation process. A TPM has a unique Endorsement Key (EK) pair and an Endorsement Credential signed by its manufacturer, platform OEM, or the IT department, asserting the validity of the EK and the TPM. The public portion of the EK and the Endorsement Credential are used to convince the trusted third party (Privacy CA) of the genuine nature of a TPM.[TCGS07]

The TCG has defined protocols to extend the trust from the EK to an AIK after a Privacy CA evaluates the evidence provided by a TPM on a platform. The EK is not used as a proof of the platform configuration directly, but AIKs, which can be created and destroyed by TPM owners, are instead used for

platform attestation. The Privacy CA creates Identity Credentials for AIKs associated with a TPM.. After an Identity Credential is acquired, any AIK operation accompanied by that credential is an assertion of trust validated by the Privacy CA .If the Privacy CA trusts the manufacturer of the TPM (or OEM or the IT department) and the root of trust for measurement (RTM) on the platform, and a remote entity trusts the Privacy CA, a quote signed by a valid AIK accompanied by an Identity Credential constitutes a cryptographic proof of the current state of the platform. Thus, we can see that in order to establish trust and perform attestation for multi-organizational use of TPM-enabled platforms, external trust infrastructure is necessary.

With the growing importance of virtualization, the need for infrastructure that supports trustworthiness of a TPM enabled platform continues since the same level of assurance is needed for virtual TPMs, and the need for trusted third parties is only enhanced by virtualization [GORS06]. TPM virtualization takes place when several domains need access to the same set of resources in a "physical" TPM, as opposed to several partitions sharing resources in one TPM allocated to each. . Each virtual TPM manages its own set of TPM resources, including its own Endorsement Key (EK), Storage Root Key (SRK), PCRs (Platform Configuration Registers), monotonic counter, and general purpose NVRAM. TPM virtualization offers a range of implementation options that can support either greater assurance or greater flexibility and performance, thereby permitting to design systems for a wider variety of use models [BECG+05].

In order for a virtual TPM to function identically to hardware TPMs, a certain level of assurance based on the validation by a trusted third party (Privacy CA) is necessary. Similarly to the hardware TPM, a virtual TPM needs evidence of its identity and genuine nature obtained from the Privacy CA or through a less stringent procedure, still rooted in the reliance on a CA [BECG+05]. Even in less strict environments, the challengers have to know the criteria for the issuance of credentials by the signer in order to trust that signer. The details and capabilities of the virtual TPMs may be either explicitly or implicitly stated in the credential, potentially enabling sophisticated policies based on the functionality described.

Although virtual TPMs may offer greater flexibility in defining the appropriate level of assurance and performance needed in a trusted environment, their reliance on infrastructure is not diminished by virtualization. CAs or equivalent third parties necessary for trust establishment continue to be indispensable.

3 Other Environments

Trusted Computing is not the only technology requiring infrastructure to enable some of the core capabilities. In today's age of ubiquitous connectivity, external infrastructure is required to carry out essential functions in most protocols. The necessary infrastructure is built by various stakeholders to support functionality that brings definite benefits. The stakeholders vary from governments and international organizations to private companies.

Infrastructure for trust establishment has additional restrictions and requirements: it needs to provide a certain level of assurance while assuming the risks for breaches and deficiencies. Below we present brief illustrations of infrastructure efforts associated with some technologies.

3.1 General Purpose PKI

Public Key Infrastructure or PKI is an arrangement that connects users' public keys with their digital identities through a Certificate Authority or a CA, also called "Trusted Third Party". Trusted Computing

as well as other technologies based on asymmetric cryptography requires a CA as part of the verification and validation processes. The user identity is unique for each CA. CA issues certificates that bind various attributes together, asserting to the validity of a public key and to the truth of other properties referenced. A PKI enables the users to establish trust through the CA without having to exchange confidential information directly. Early in the Internet age, PKI was considered as a foundation for creating a trusted environment on public networks [WAWU99]. Although many security conscious enterprises and most governments have built PKI, the vision of a global PKI used for reliable authentication on the Internet has not been realized. In practice, over time the reach of most PKI projects has been reduced, and a large proportion has not been successful [LOOP05]. There are numerous reasons for the failure. Technical reasons include general complexity of the certificates, associated policies, and related protocols; difficulties in carrying out lifecycle management of credentials, lack of automation for certificate and key exchange among users of different PKIs; lack of pragmatic procedures for PKI cross certification. Semi-proprietary implementations of CAs make integration with applications, already challenging because of the underlying complexity, practically impossible. But more than technical reasons, it is the business environment that is responsible for the failure of PKI to become as wide-spread as the early technologists had hoped. After all, if there was a valid market reason for the technology to thrive, technical problems would probably have been resolved due to strong economic incentives to achieve success. In reality, it is very expensive to establish and run a PKI, and it proved impossible to charge the users for the certificates, since the benefits of using certificates are unclear to a lay person. Only models that rely on charging enterprises in need of state-of-the-art e-commerce environments have been successful, with Verisign emerging as a leader in this area.

3.2 Federated Identity

It is also useful to mention briefly the Liberty Alliance, a standards consortium formed in 2001 to promote open standards for federated identity management. The Liberty Alliance specifications are designed to ensure that a user does not need to re-authenticate when accessing linked accounts. Because of the linkage of accounts and use of standard protocols, privacy and other policies can be enforced in a more consistent manner. In the six years of its existence, Liberty Alliance scored numerous successes as the organization grew and its specifications enjoyed a good level of adoption.

However, the full vision of the Federated Identity Framework requires significant infrastructure investment by establishing Identity Providers, organizations that maintain and ensure the validity of "registries of identities" as part of the federated system and are trusted by the users and owners of these identities. Although there are numerous successful implementations of systems with federated identity features on a smaller scale, global identity services have not emerged, due to reasons similar to those outlined in the section on PKI: underlying complexity of specifications and lack of economic incentives that would compensate the organizations for assuming the risks acting as Identity Providers.

3.3 DNS

The creation of the DNS (Domain Name Service) was a successful effort to establish a global infrastructure for an indispensable service. Unlike the two previous examples, though, trust establishment is not its main function. DNS serves as a phone book for the Internet by associating domain names with other information necessary to carry out services on the Internet. Its most basic service is to translate host name to IP addresses. In this brief section, we attempt to summarize the reasons for the success of DNS as opposed to many other infrastructure efforts that could create significant benefits for the users, but nonetheless failed.

Economics of Security and PKI Applications

Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach

Anas Tawileh · Jeremy Hilton · Stephen McIntosh

School of Computer Science, Cardiff University
5 The Parade, Cardiff CF24 3AA, UK
{m.a.tawileh | jeremy.hilton | s.b.mcintosh}@cs.cardiff.ac.uk

Abstract

Small to medium sized enterprises (SMEs) constitute a major part of the global economic activity. Due to the distinct characteristics of these enterprises, approaches to information security management that were mainly developed for larger organisations can not be feasibly applied in the context of SMEs. In this paper, we present some of the challenges impeding the implementation of information security management in SMEs. We propose a holistic approach based on Soft Systems Methodology to facilitate the development of security management systems within SMEs. The new approach acknowledges the limitations faced by SMEs and accounts for the systemic nature of the information security problem. We demonstrate the usefulness of our approach through a practical case study. The paper concludes with a brief summary of the findings and presents directions for future work.

1 Introduction

The Internet has been growing at a significant pace over the past few years. Both large and small-to-medium sized businesses invested substantial resources to create their presence on the global network. Increasingly, more information is created or converted into digital format, saved in different storage devices and transmitted over a plethora of interconnected networks. While the rapid growth of the Internet has changed the way we communicate, conduct business and achieve our goals, crime and security threats such as badware, spam, phishing and viruses have also increased, undermining users' trust and confidence in the Internet [HoHD02].

These threats can also result in major losses for companies around the world and impair the continued growth and utilization of the beneficial aspects of the Internet and the global Information Society. Such costs are incurred through loss of productivity, loss of business and damage to the organisation's "brand", and through the investments required for the protection of connected systems from attacks and misuse [CaMR04] [AsCH03].

The information security problem is characterized by complexity and interdependence. It contains a significant number of factors and elements that interrelate with each other. The presence of the human factor complicates the situation even further, as humans have free will, and will always act upon their own best interest [Jame96]. Moreover, the increasing reliance on the Internet in almost every business activity makes security a major concern on the agendas of many different stakeholders (individuals, businesses, governments, etc) [PaPo00] [TI3P03].

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2007), 331-339

As security is a common concern among all stakeholders, combating information threats requires collaboration to ensure that the Internet is a secure medium which is needed for building a thriving information society. However, one of the challenges in reaching collaboration is that each group has a different position and approach to how to address security issues and deal with the potential trade-offs related to security and usability. Furthermore, different stakeholders possess different resources that they can invest in countering security threats. The gap between large and small-to-medium sized enterprises in the information security arena has been increasing substantially as a direct result of the scarcity of resources available to SMEs.

A significant element of any information security system are the costs associated with its design, development, implementation and decommissioning. Major investments need to be expended to build and maintain highly reliable, responsive and trustworthy information security systems [Ande01]. While very few would argue that information stored, processed and communicated in computer systems do not incur significant risks, the case for investing in appropriate security measures may still be difficult to justify [Lamp00]. It can be argued that the major reason behind the prioritisation of information security on corporate agendas in the past decade has been the increased and stringent regulatory compliance requirements imposed on commercial organisations. In addition, large businesses have developed a reasonable understanding of the consequences of poorly protected information systems. Consequently, larger proportions of business budgets have been allocated to improving the protection of the corporate digital assets.

While these investments and initiatives will certainly reduce the threats posed by the modern electronic marketplace, other aspects of the problem remain largely unaddressed. The complexity and interdependence of the security problems on the Internet seriously limit the effectiveness of any initiative undertaken within specific organisational or geographical contexts. Threats and attacks can originate from anywhere, without being bound to specific geographies or organisational borders [YeBU03].

Because of a serious lack of awareness of the negative consequences of information security issues and threats among small to medium sized enterprises (SMEs) [eCom00], added to the perception of less strict regulatory compliance requirements and the very high relative costs of securing digital information, the information and communications infrastructures within these firms remain highly unsecured and vulnerable [ABS03]. Increasingly, interconnectedness is becoming a major requirement for business communications. Large organisations rely on the services provided by many smaller partners and contractors spread across geographical borders. These smaller firms should be granted certain levels of access to the large organisations' information systems in order to deliver on their business contracts. By gaining access to the organisational information systems, partners and contractors are effectively becoming parts of the corporate network. Given the possibility for security threats and attacks to originate from any machine connected to the global network, SMEs act as the "weakest link" in the network. The weakest link in any network is an attractive point of entry for intruders to hack into the system and any network is as secure as its weakest link. This implies that for the global Internet to be properly secured, a more holistic approach should be taken, with special attention paid to the weakest link: SMEs.

In this paper, we present a new holistic approach to the management of information security in SMEs based on Soft Systems Methodology. Firstly, we will discuss the importance of the security problem within SMEs and why there is a need for a simple, holistic and low cost approach to security management. Afterwards, we introduce our approach to managing security in SMEs and explain the system development process. The application of the model in real world situations is then described through a practical case study and the paper concludes with a summary of the discussion and the areas that require further research.

1 Background

The problem of information security in SMEs cannot be solved only by raising awareness about the seriousness of its consequences. Within the UK, Government, in the form of the DTI, and industry organizations such as the Institute of Directors and the Confederation of British Industry, regularly publish general guidance for industry about the risks. However, many other factors are at play to complicate the situation even more; and the call for immediate action is vital. Even with appropriate awareness and complete understanding of the security issues, SMEs do not possess the required resources (human, monetary or technical) that should be invested to solve the problem. SMEs typically operate under very tight budgets; have seriously limited manpower and many needs competing for a very limited supply of resources, leading to information security being pushed down the priorities list. There is a negative feedback cycle at play here: less awareness of the information security problem pushes it down the priorities list, which in turn reduces the resources allocated to it, leading to even lower awareness (Fig. 1).

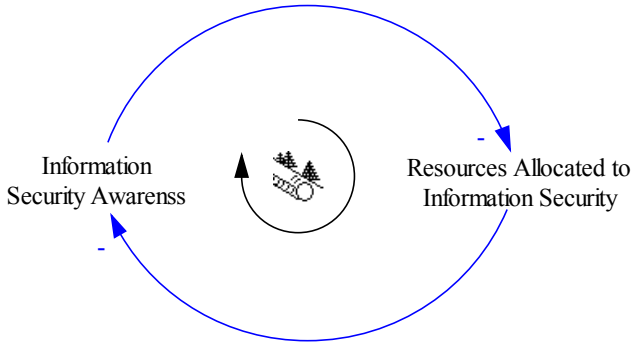

Fig. 1: Negative Feedback Loop of Information Security Awareness in SMEs

While the above mentioned problems do not usually occur in the context of large organisations, they certainly have a significant effect on the security problem within these firms. The interconnectedness of the Internet implies that even though these problems may be contained within smaller businesses, they have a substantial impact on other organisations as well. Most of the initiatives started in order to improve information security in large organisations had a local focus, assuming that the development of company-wide information and communications security infrastructure will enhance the security status across the organisation. This assumption ignores the essential fact that electronic attacks and security threats can originate from any place on the globe. An increased protection of the perimeter of the corporate network is not an effective option anymore due to the cross-border communication and collaboration requirements. Security should be approached with a holistic perspective that considers the interdependent and interconnected nature of modern global communications [ChCZ04].

Furthermore, because of the serious shortage of qualified technology professionals and expertise, information security is generally perceived as a high cost that should be justified well enough to be pursued [LaEl00]. Large and multinational organisations and conglomerates are struggling to get their own security budgets approved and allocated, even though the case they are making is quite appealing. With this perceived high cost of security, it will be over-optimistic to assume that large corporations will allocate sufficient resources to develop security outside their organisational borders.

To understand the scope of the information security problems within SMEs and how they might affect the information assurance status of the whole economy, the relative volume of business conducted by SMEs was compared against the overall economic activity in Europe and the United States. The Department of Trade and Industry (DTI) in the UK reported a total number of business enterprises of 4.3

million at the start of 2005. Small enterprises (defined as having 0–49 employees) constitute 99.3 % of this figure, while medium businesses (50–249 employees) represent 0.1 %. Only 0.1 % of all businesses in the UK fall into the large enterprises category (more than 250 employees) [Dti05].

Europe has, according to the Observatory of European SMEs, more than 19 million small or medium sized enterprises (using the same classification scheme mentioned above), comprising 99.8 % of all business enterprises in the continent. On the other hand, only 6,000 enterprises in Europe are large businesses [EuCo03]. In the United States, small and medium sized enterprises (those with fewer than 500 employees), constitute 99.7 % of all businesses [SBAo03].

Chris Anderson [Ande06] identified several reasons behind the proliferation of extreme market segmentation and niche creation witnessed in the last two decades. He claims that the Internet has radically changed the market dynamics of many major industries. The democratisation of production and distribution tools has placed significant power in the hands of small businesses and, to a certain degree, levelled the playing field for competition with larger corporations. This has led to the creation of a virtually unlimited number of micro market niches in almost every single industry. Small businesses are better fitted to satisfy the requirements of these micro niches, which in turn resulted in the significant growth of these businesses. The development of aggregators (websites that mediate transactions between consumers and producers in the world of unlimited choice [Ande06]) has lowered barriers to entry and supported the growth of new market entrants. Anderson argues that these trends will continue for many years to come. This would lead to further expansion of SMEs both in number and market share.

In addition to describing the forces behind the increasing proliferation of SMEs, Anderson's ideas draw attention to the projected growth in the information security problems in these organisations. Micro businesses established to satisfy the demands of the emerging tiny market niches do not possess adequate time, nor resources to actively tackle the issues of information security. Traditional approaches to information security cannot provide satisfactory solutions to the needs of these businesses. Most of the current approaches require considerable investments of time and resources, and demand high levels of technical expertise. Therefore, the "Long Tail" of the business information security market remains unaddressed. The next section presents a suggested holistic approach to tackle information security management in SMEs.

2 A Holistic Approach to Information Security

Several methodologies and standards were developed to address the increasingly important issues of information security (examples include CRAMM [Cram06] and ISO17799 [Iso05]). Some of these standards became mandatory requirements imposed by different regulatory compliance legislation. However, we argue that these approaches were not designed specifically with SMEs in mind. As a result, they require substantial technical expertise and significant investments. We propose a simple approach to information security management in SMEs that avoids the limitations of previous methods while acknowledging the systemic nature of the situation. The approach is based on the four main stages illustrated in Fig. 2.

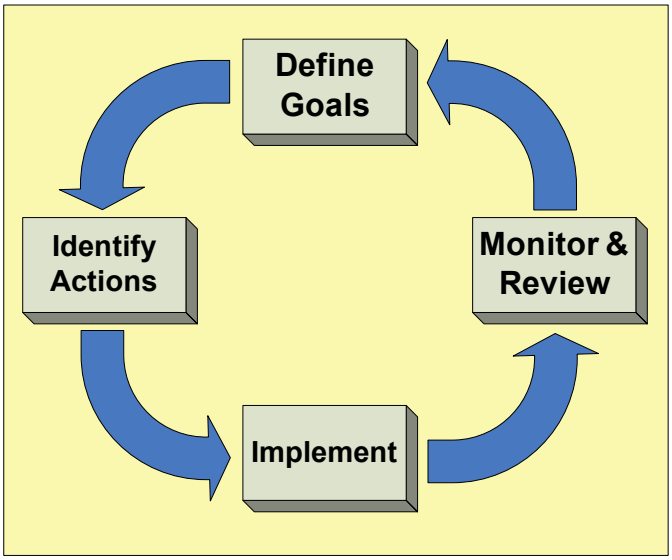

Fig. 2: Four Stages of the SME Security Management Process

Before any information security management system can be developed, the intended objectives of the system must be clearly defined and formulated. It is important to acknowledge at this stage the changing business environment in which SMEs usually operate. This will require the security objectives to adapt to match the new business requirements. Therefore, flexibility in defining and redefining goals with minimum resource requirements is critical to the success of the proposed approach. To define the requirements in a clear and unambiguous way, we propose the use of the Soft Systems Methodology (SSM). SSM was proposed by Peter Checkland as "a general problem solving approach appropriate to human activity systems" [Chec99].

SSM suggests an intellectual construct called a "Root Definition" (RD), which aims to provide a clear and unambiguous textual definition of the system to be modelled (in this case the information security management system). It provides a way to capture the essence (root) of the purpose to be served by this system [Chec99]. The Root Definition has 6 components, which can be memorised using the mnemonic (CATWOE). We have mapped these elements to match the purposes of information security management in SMEs and to facilitate the development process. The mapping is provided in Table 1.

Table 1: Elements of a Root Definition

Element	Original Description	SME Security
C	Customer of the system	In which organisation will the information security management system (ISMS) be implemented?
A	Actors in the system	Who will implement and maintain the ISMS?
T	The Transformation process that the system should undertake	What is the single most important objective to be achieved by the ISMS?
W	(Weltanschuuang) or Worldview upon which the system is based	How the company's security objectives will be achieved?
O	Owner of the system	Who is the owner of the organisation?
E	Environmental constraints	What are the constraints affecting the ISMS within the organisation?

3 Case Study

The following case study illustrates the process of capturing the goals of the information security management system in a small organisation. Firstly, the elements of the root definition should be defined by answering the questions posed in Table 1. While this may be a reversed order of deriving root definitions compared to the suggestions of SSM, (in the "pure" form of which it is argued that the CATWOE mnemonic should be used as a "quality" test of the Root Definition) it would significantly reduce the difficulty of developing these definitions[1]. This case study described the implementation of our holistic information security management approach at a small consultancy firm (3 employees) based in Germany. Table 2 provides Logiteca's answers to the CATWOE questions.

Table 2: Analysis of Logiteca's Requirements

Element	SME Security Question	Logiteca's Answer
C	In which organisation will the information security management system (ISMS) be implemented?	Logiteca.
A	Who will implement and maintain the ISMS?	Logiteca's staff members.
T	What is the single most important objective that should be supported by the ISMS?	Operate the business with reliable information appropriate to current business needs.
W	How this objective will be achieved?	Ensuring staff members understand and act on relevant security issues and that the company's information systems are established and operated in a manner appropriate to the importance of the information processed.
O	Who is the owner of the organisation?	Logiteca's general manager.
E	What are the constraints affecting the ISMS within the organisation?	Limited time, funds and staff.

Based on these answers, the root definition of the ISMS at Logiteca can be easily formulated as follows:

> *A general manager owned system, operated by Logiteca's staff members, to operate the business with reliable information appropriate to current business needs by ensuring staff members understand and act on relevant security issues and that Logiteca's information systems are established and operated in a manner appropriate to the importance of the information processed, while considering the limited time, funds and resources available.*

Once the security objectives are defined and captured appropriately in a root definition, the second step entails identifying actions that should be taken to achieve these goals. SSM proves to be an invaluable tool to perform such a task, as it provides a logical approach to the process of translating root definitions into a list of activities through a well defined modelling process. Based on the root definition presented above, a model of the intended ISMS was developed (Fig. 3) and the list of activities to be performed by Logiteca was derived. This list is reproduced in Table 3. After the required activities are identified, responsibilities can be assigned to determine who will be doing each activity and be accountable for that. The time frame for conducting each activity can also be determined and the performance measures defined.

1 We have for some years been using this approach with postgraduate students unfamiliar with SSM, to coach them in the development of Root Definitions.

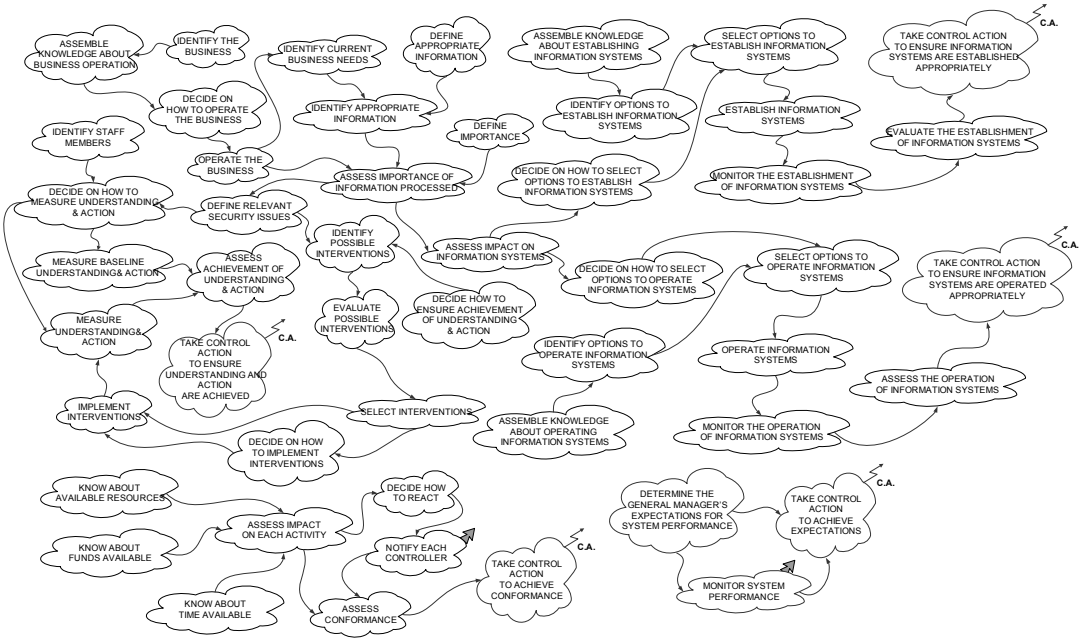

Fig. 3: Soft Systems Methodology Model for the ISMS at Logiteca

Table 3: List of Actions for Logiteca's ISMS

No	Action	Who	When	Measure
1	Define business information	Logiteca Staff		
2	Identify business information	Logiteca Staff		
3	Assess importance of business information	Logiteca Staff		
4	Define relevant security issues	Logiteca Staff		
5	Decide on how to measure security understanding and action	Outsourced		
6	Identify staff members	Logiteca Staff		
7	Measure baseline security understanding and action	Outsourced		
8	Identify possible interventions "awareness programs"	Logiteca Staff		
9	Decide on how to evaluate interventions	Logiteca Staff		
10	Evaluate possible interventions "awareness programs"	Logiteca Staff		
11	Select awareness program	Logiteca Staff		
12	Implement awareness program	Outsourced		
13	Measure security understanding and action	Outsourced		
14	Assess enhancement of security understanding and action	Logiteca Staff		
15	Take control action to ensure awareness and action are enhanced	Logiteca Staff		
16	Assess impact on information systems (IS)	Logiteca Staff		
17	Decide on how to select options to establish and operate IS	Logiteca Staff		
18	Assemble knowledge about available security technologies	Logiteca Staff		
19	Decide on how to evaluate security technologies	Logiteca Staff		
20	Evaluate security technologies	Logiteca Staff		
21	Select appropriate security technologies	Logiteca Staff		
22	Implement appropriate security technologies	Outsourced		
23	Monitor the establishment and operation of IS	Logiteca Staff		
24	Assess the establishment and operation of IS	Logiteca Staff		
25	Take control action to ensure IS are established and operated in a manner appropriate to the importance of information	Logiteca Staff		