Norbert Pohlmann | Helmut Reimer |
Wolfgang Schneider (Eds.)

ISSE 2011 Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe 2011 Conference

VIEWEG+ TEUBNER

ISSE
INFORMATION SECURITY SOLUTIONS EUROPE

Norbert Pohlmann | Helmut Reimer | Wolfgang Schneider (Eds.)

ISSE 2011 Securing Electronic Business Processes

IT

By the author:

Future of Trust in Computing
by D. Grawrock, H. Reimer, A.-R. Sadeghi and C. Vishik

Autonomous Land Vehicles
by K. Berns and E. v. Puttkamer

Microsoft Dynamics NAV
by P. M. Diffenderfer and S. El-Assal

Using Microsoft Dynamics AX 2009
by A. Luszczak

From Enterprise Architecture to IT Governance
by K. D. Nieman

www.viewegteubner.de

Norbert Pohlmann | Helmut Reimer |
Wolfgang Schneider (Eds.)

ISSE 2011 Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe 2011 Conference

With 103 Figures

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

1st Edition 2012

Editorial Office: Dr. Christel Roß | Andrea Broßler

Vieweg+Teubner Verlag is a brand of Springer Fachmedien.
Springer Fachmedien is part of Springer Science+Business Media.
www.viewegteubner.de

Cover design: KünkelLopka Medienentwicklung, Heidelberg
Typesetting: Oliver Reimer, Jena
Printing company: AZ Druck und Datentechnik, Berlin
Printed on acid-free paper
Printed in Germany

ISBN 978-3-8348-1911-6

Contents

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 nineth ISSE book – another mark of the event's success – and with about 30 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:

- **Ammar Alkassar**, Sirrix AG (Germany)
- **Ronny Bjones**, Microsoft (Belgium)
- **Pavel Čeleda**, Masaryk University (Czech Republic)
- **Roger Dean**, eema (United Kingdom)
- **Jan De Clercq**, HP (Belgium)
- **Marijke De Soete**, Security4Biz (Belgium)
- **Jos Dumortier**, K.U. Leuven (Belgium)
- **Walter Fumy**, Bundesdruckerei (Germany)
- **Riccardo Genghini**, S.N.G. (Italy)
- **Michael Hartmann**, SAP (Germany)
- **John Hermans**, KPMG (The Netherlands)

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2010), vii-x

- **Jeremy Hilton**, Cardiff University (United Kingdom)
- **Francisco Jordan**, Safelayer (Spain)
- **Frank Jorissen**, tygris (Belgium)
- **Marc Kleff**, Siemens Enterprise Communications (Germany)
- **Hasse Kristiansen**, Ernst & Young (Norway)
- **Jaap Kuipers**, DigiNotar (The Netherlands)
- **Matt Landrock**, Cryptomathic (Denmark)
- **Norbert Pohlmann (chairman)**, University of Applied Sciences Gelsenkirchen (Germany)
- **Bart Preneel**, K.U. Leuven (Belgium)
- **Steve Purser**, ENISA
- **Helmut Reimer**, TeleTrusT (Germany)
- **Wolfgang Schneider**, Fraunhofer Institute SIT (Germany)
- **Jon Shamah**, EJ Consultants (United Kingdom)
- **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*

TeleTrusT Deutschland e.V. (TeleTrusT Germany)

The IT security association TeleTrusT Germany was founded in 1989 to provide a reliable framework for deployment of trustworthy information and communication technology.

Today, TeleTrusT is a widespread competence network for IT security currently representing more than 110 members from industry, science and public institutions, with associated member organizations in Germany and other countries.

In various TeleTrusT working groups IT security experts, users and interested parties meet each other in frequent workshops, round-tables and expert talks. The activities focus on reliable and trustworthy solutions complying with international standards, laws and statutory requirements.

TeleTrusT is keen to promote the acceptance of solutions supporting identification, authentification and signature schemes in electronic business and its processes. TeleTrusT facilitates information and knowledge exchange between vendors, users and authorities. TeleTrusT aims on standard compliant solutions in interoperable schemes.

TeleTrusT comments on political and legal issues related to IT security, organizes events and participates in conferences. TeleTrusT is carrier of the "European Bridge CA" (provision of public key certificates for secure e-mail communication) and runs the expert certification programme "TeleTrusT Information Security Professional (T.I.S.P.).

Keeping in mind the raising importance of the European security market, TeleTrusT seeks co-operation with European and international organisations and authorities with similar objectives. Thus, this year's European Security Conference ISSE is being organized in collaboration with eema, ENISA and the Czech Chamber of Commerce.

Contact: TeleTrusT
Dr. Holger Muehlbauer, Managing Director
Chausseestrasse 17, 10115 Berlin, GERMANY
Tel.: + 49 30 / 4005 4310
holger.muehlbauer@teletrust.de
www.teletrust.de

eema

For 24 years, EEMA has been Europe's leading independent, not-for-profit e-Identity & Security association, working with its European members, governmental bodies, standards organisations and interoperability initiatives throughout Europe to further e-Business and legislation.

EEMA's remit is to educate and inform over 1,500 Member contacts on the latest developments and technologies, at the same time enabling Members of the association to compare views and ideas. The work produced by the association with its Members (projects, papers, seminars, tutorials and reports etc) is funded by both membership subscriptions and revenue generated through fee-paying events. All of the information generated by EEMA and its members is available to other members free of charge.

Examples of recent EEMA events include The European e-ID interoperability conference in Brussels (Featuring STORK, PEPPOL, SPOCS & epSOS) and The European e-Identity Management Conference in Tallin.

EEMA and its members are also involved in many European funded projects including STORK, ICEcom and ETICA

Any organisation involved in e-Identity or Security (usually of a global or European nature) can become a member of EEMA, and any employee of that organisation is then able to participate in EEMA activities. Examples of organisations taking advantage of EEMA membership are *Volvo, Hoffman la Roche, KPMG, Deloitte, ING, Novartis, Metropolitan Police, TOTAL, PGP, McAfee, Adobe, Magyar Telecom Rt, BBS, National Communications Authority, Hungary, Microsoft, HP,* and the *Norwegian Government Administration Services* to name but a few.

Visit www.eema.org for more information or contact the association on +44 1386 793028 or at info@eema.org

The new German ID Card: An Innovative System Gains Acceptance

Ulrich Hamann

Bundesdruckerei GmbH
Oranienstrasse 91, 10969 Berlin, Germany
info@bdr.de

Abstract

Introduction of the new ID card in Germany on 1 November 2010 also marked the start of one of the world's largest IT projects. In the meantime, around 6 million of these state-of-the-art multifunction cards are in circulation, and the infrastructures created for the new online ID function are rapidly becoming established on the market.

1 A sovereign document – the key to greater identification security

Introduction of the new ID card and its background systems is making electronic identity the key issue for reliable and trustworthy internet activities. For the first time ever, people can authenticate themselves just as well in the "virtual" world as in the "real" world, while at the same time being able to verify the identity of their vis-à-vis on the internet. Many individual processes were needed to engrain this new quality of trustworthy mutual reciprocity in the awareness of the general public and in the everyday activities of official authorities and commercial enterprises. In the meantime, the German ID card system has stood the test, and its introduction represents an important milestone on the way to greater ID security in the digital world – both on a national and an international scale.

2 Trust must be mutual

In order to guarantee safe exchange of confidential data, the new ID card system was developed according to the *mutual authentication* principle. The sovereign document, with its reliable identity data, supports the mutual transfer of information using so-called authorisation certificates, which certify institutions and companies as being trustworthy service partners.

In this way, business sectors that depend on their customers providing reliable information about identity or age for online transactions can be sure of obtaining reliable data without additional authentication procedures. Vice versa, the internet user obtains precise information about registered eGovernment and eBusiness services. Furthermore, the new ID card's so-called *pseudonym*

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2011), 1-8
N. Pohlmann et al. (Eds.), *ISSE 2011 Securing Electronic Business Processes,*
DOI 10.1007/978-3-8348-8652-1_1,

function allows the user to log in anonymously to selected websites. This is of particular advantage in online social networks, since it allows the user to make use of all the provided functions without leaving an unwanted personal data trail.

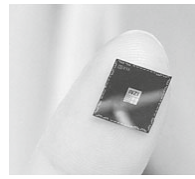

Fig. 1: The new ID card contains a security chip. This is used to store the digital photo and personal data of the card holder.

The technological core of the new eID management concept is a contactless security chip. This is embedded inside the new polycarbonate card and supports three added electronic functions:

- the online ID function,
- the qualified electronic signature (QES) and
- the sovereign biometrics function.

3 Secure authentication in the internet

The primary new function is so-called *online ID function* (or in short: eID function) which can be activated at any time, as the card holder wishes. Users can for example take advantage of the online ID function to sign an Internet petition without having to change over to another medium[1]. In local urban and rural administrations, German citizens can call up selected services on their home PC, for example ordering copies of birth, marriage and death certificates, registering their dog at the tax office, library services or enquiries to the land survey register. Other information (for example on child allowances or traffic offences) can also be called up safely using the online ID function of the respective authority.

At the same time, an increasing number of companies are showing interest in the new online authentication processes. Apart from simplifying log-in and registration procedures – customer data such as name and address no longer have to be captured manually – what is important for them is the certainty that the person or company on the other side of the virtual "shop counter" really does exist and that they are dealing with a business partner whose data security credentials have already been checked. One of the first companies to use mutual authentication processes was the "Gothaer Allgemeine" insurance company, which has been offering its customers a variety of eID functions ever since November 2010. The German pensions authority "Deutsche Rentenversicherung" has also been working along similar lines. With their new ID cards, insured persons and retirees can now review their pensions account or call up the current status of their future pension online.

1 www.openPetition.de

Cloud Computing & Enterprise Security Services

How Cloud Security Strongly Depends on Process Maturity, Automation and Scale

Eberhard von Faber [1(+2)] · Michael Pauly [1]

[1] T-Systems
{Eberhard.Faber | Michael.Pauly}@t-systems.com

[2] Brandenburg University of Applied Science
Eberhard.vonFaber@fh-brandenburg.de

Abstract

Security is the most discussed topic in cloud computing. Therefore, the (enterprise) users ask their provider about antivirus protection, firewalls and access control. But only a few of them know the processes inside a data centre needed to produce scalable, dynamic and flexible ICT-services on large scale. The essential elements here are centralization and consequent re-use, virtualization on all levels of the ICT stack, as well as interoperability and standardization to ensure that this will work. By considering principles of modern ICT production, it is shown that process maturity, automation and large scale are essential to achieve an adequate level of security.

1 Introduction

Cloud computing is - from a provider's point of view - characterized by resource pooling and rapid elasticity, in order to realize scalable, flexible and dynamic IT services. ICT service provisioning from a cloud require the ICT service provider to use modern technology and industrial ways of production. The essential elements are (i) centralization and consequent re-use, (ii) virtualization on all levels of the ICT stack, and (iii) interoperability and standardization to ensure that this will work. Of course, all systems are interconnected as a prerequisite.

This paper takes a look behind the curtain of the production of cloud services. By considering principles of modern ICT production, it is shown that process maturity, automation and large scale are essential to achieve an adequate level of security.

Cloud computing obviously also require the application of standard ICT security solutions such as firewalls, intrusion prevention, anti-malware, monitoring, and access control. The management of these security solutions is subject to and common to all types of service provisioning and not specific to cloud computing. However, delivering secure cloud computing requires more than such standard technology. It is necessary to use specific technology for ICT service provisioning which in turn gives rise to additional challenges. This becomes apparent when considering the specific methods of modern ICT production.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2011), 23-33
N. Pohlmann et al. (Eds.), *ISSE 2011 Securing Electronic Business Processes,*
DOI 10.1007/978-3-8348-8652-1_3,

In chapter 2 the production of cloud services is described from a provider's perspective. Chapter 3 focused on the central role of interconnection of all ICT resources for cloud service provisioning. Chapter 4 describes challenges of dynamic resource allocation and sharing. Standardised software images are used here. Chapter 5 addresses the security issues related to software engineering and provisioning.

Database and storage services are fundamental for cloud computing. Some of the security issues of the database and storage management are depicted in chapter 6. A precise assignment of responsibilities and tasks as well as an identity and access management system is essential to ensure that security requirements are met. This is the focus of chapter 7. Cloud computing has consequences in terms of security. There are advantages as well as critical issues for user organisations. The make or buy decision is discussed in chapter 8. A summary is given in chapter 9.

2 ICT Production and Cloud from a Provider's View

With cloud computing in its pure form the whole infrastructure moves from the customer site into a provider operated data centre. The provider is in charge of the hardware and software as well as the whole production process. The customers only use a – thin or fat – client workplace to work with or use the IT service needed for business.

The ICT service provider delivers this kind of services to a variety of customers often on a global basis. This is required since economies of scale and other benefits from the division of labour are the central motivation for users for "ICT outsourcing" of any kind. Consequently, ICT must be produced in an industrial way with a one-to-many business model. The data centre typically provides an area for ICT equipment which is as large as a football / soccer pitch.

Fig. 1: Modern Data Centre for industrialised ICT Production

The whole design of the data centre is in the authority of the provider (Fig. 1). He is the only who is responsible for the provision process, the automation as well as the hard- and software he use for the realization. The difference between conventional outsourcing and cloud computing is, that using cloud services the producing ICT fabric is a black box or a non-transparent obscure cloud. Refer for instance to [EvFMiP10] for more detail.

The black box approach gives the provider the degrees of freedom he needs to realize the economies of scale [vFab2011]. That means he has to select the sort of resources on the one hand and to choose the sharing model of the resources on the other hand. The common base for the most cloud resources is a x86 infrastructure in combination with a scalable storage system. For the virtualization of the server layer hypervisor based software is used.

Sharing resources between different user organisations efficiently include two points: "doing the right thing" and "doing the things right". "Doing the right things" means, from the provider perspective, to select the "right" hardware and software in order to build up large scalable environments, which can be operated using a high level of automation. Note that this selection is a first important issue in terms of ICT security. "Doing the things right" means to choose the right automation and to optimize the processes. The utilization has also to be precisely predicted to avoid oversubscription or vacancy of resources.

3 System Interconnection as a Basis

Economies of scale result from sharing resources between user organisations. In order to distribute costs of acquisition (and operation) over user organisations, they have to share hardware and software. A cloud being reserved for one single organisation (wrongly called "private" by NIST, refer to [NIST2011]) may scale, but the one user organisation must carry all costs themselves. Where are the economies of scale expected to come from?

The sharing of hardware and software has the other advantage that the production is made flexible and resource allocation can easily follow demands. In case of a large number of users and voluminous resources, the continuous reorganization of server resources is required – also for maintenance. But how does this work? Virtualisation allows sharing resources between different user organisations.

Building up a large and flexible infrastructure, it is necessary to use virtualization techniques at every layer: network, compute and storage. We start with the security issues in network virtualisation.

Sharing a computing infrastructure and storage requires that every user must potentially have the ability to get connected to every system. Consequently, all systems must be interconnected. This seems to directly contradict to basic security requirements such as confidentiality and integrity of data. But actually, on the Internet, for example, this is common practise. So, there are solutions for most security issues, e.g. the use of Virtual Private Networks (VPN) to share the existing network.

Awareness, Education, Privacy & Trustworthiness

pohlmann@internet-sicherheit.de

Information Security Awareness Campaign "Sicher gewinnt!": A Joint Action of the German Federal Administration

Käthe Friedrich[1] · Lydia Tsintsifa[2]

[1]Federal Academy of Public Administration
at the Federal Ministry of the Interior
Willy-Brandt-Str. 1, 50321 Brühl, Germany
kaethe.friedrich@bakoev.bund.de

[2]Federal Ministry of the Interior
Alt-Moabit 101 D; 10559 Berlin, Germany
Lydia.Tsintsifa@bmi.bund.de

Abstract

Information security is decided every day in every workplace. The human factor can constitute the weakest link in an information security framework. Improvement of the technical security measures shifts humans more and more into the target of attackers in order to compromise the information assets of an organization. High personal awareness of information security risks and well-trained security managers therefore constitute the first line of information security defence. To achieve this aim, a significant change in user perception and the establishment of an organizational information security awareness culture are necessary. This includes the users' comprehension and application of information security measures in an effortless and intuitional way.

This article provides an overview of our experience in conceiving and implementing an effective Awareness Security Campaign for a very heterogeneous and decentralized, large organization, as is the federal administration.

1 Introduction

The rapid pace of changes in information technology and the increasing dependence on it have made information security requirements within the federal administration increase continuously in the recent years. A variety of threats and security problems can be avoided by the use of technical defence systems. However, this is not sufficient to prevent information security incidents.

The human risk source is now considered to be at the forefront of information security risks [KES]. Moreover, the responsibility of the individual grows with increasing information security demands.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2011), 79-87
N. Pohlmann et al. (Eds.), *ISSE 2011 Securing Electronic Business Processes*,
DOI 10.1007/978-3-8348-8652-1_8,

1.1 Framework conditions for information security awareness in the federal administration

In 2007 the federal administration adopted a unified information security strategy to implement the objectives of the "National Plan for Information Infrastructure Protection in Germany" in the area of Information and Communication Technologies [BMI1]. This included creating an institutional structure for information security for the entire federal domain. Thus, information security officers were appointed in each federal public agency. Furthermore, a unified information security management system, based on the application of the BSI Standards for information security [BSI1] and the IT-Grundschutz Catalogues [BSI2], has been made mandatory for the federal administration.

To meet the recommendations, all federal authorities had to implement appropriate information security awareness and training measures. These recommendations are also put to the forefront by the new Federal Cyber Security Strategy for Germany, published in February 2011 [BMI2].

The need for a concerted awareness campaign of the federal administration has been identified as a priority action within the framework of the joint information security strategy. Budget autonomy and distributed responsibility for information systems, high diversity of security requirements and a very large variety of tasks posed a challenge, though. To handle it efficiently, a comprehensive awareness campaign that builds on the common circumstances and conditions of the federal administration, has an organization branding and yet leaves room for adjustments to individual requirements was needed.

In early 2009 the "Act to Safeguard Employment and Stability in Germany" made it possible to set up a package of measures to improve IT and information security, the "IT Investment Programme", as part of the Recovery Plan mandated by the Federal Government. This provided the opportunity for the federal agencies to get access to a common budget for different purposes. As the improvement of information security was a main focus of the programme, the financing of a joint awareness campaign was approved, with a funding of € 3 million.

1.2 The Federal Academy of Public Administration

The planning and implementation of the awareness campaign "Sicher gewinnt!" ("security wins") is carried out by the Federal Academy of Public Administration (Federal Academy, "BAköV") in cooperation with the Federal Office for Information Security (BSI).

The Federal Academy was founded in 1969 as a central training body of the Federal Government. Working closely with the federal administration, industry and academia, the Federal Academy is responsible for providing practice-oriented advanced training for federal administrative staff and for advising agencies in personnel development and training matters.

For nine years, the Federal Academy has been offering IT training. Since 2006 also the training series "Information security officer in the public administration" has been offered in cooperation with the BSI. This is structured in three levels and can be completed with a certificate degree, which is recognized and meets the quality requirements for IT security managers in the public administration. Information security officers of the federal administration are recommended to successfully complete an appropriate training programme before taking up their duties.

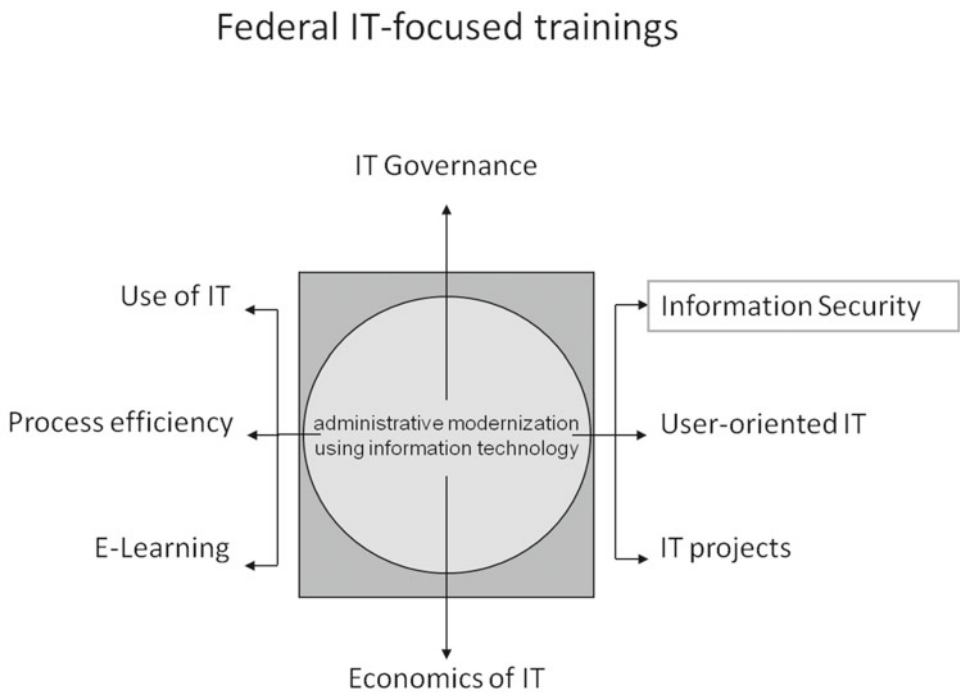

Fig. 1: The structure of the IT training offered by the Federal Academy.

The concept of training and certification of "IT security officer in the public administration" has been also adopted by the University of Applied Sciences North-West Switzerland Olten, the University of Applied Sciences Wildau, the Cooperative State University Baden-Württemberg and the University of Cooperative Education Gera.

Furthermore, the Federal Academy offers also information security trainings for IT administrators and awareness courses for IT users.

2 Compilation and commissioning of services

The main concern of the campaign "Sicher gewinnt!"was to give each agency the opportunity to plan and adapt its measures according to its needs and culture. It is clear that awareness-raising can be successful only if its messages reach the individuals and the learning processes work in an emotional and motivating way.

Although the planning time provided was very short, the Federal Academy managed to plan, compile and procure a well-concerted package of awareness modules, which could start within a few months. The following factors have contributed decisively

- The Federal Academy had already conceived a plan for the compilation of the campaign. The basic structure and content of the campaign as well as the concept of central modules had already been set up. As a result, a call for tender could be launched for certain parts immediately.

- A flexible model for the commissioning of services, the "three-partner model", which is often used in the federal administration, could be applied. The process is illustrated below:

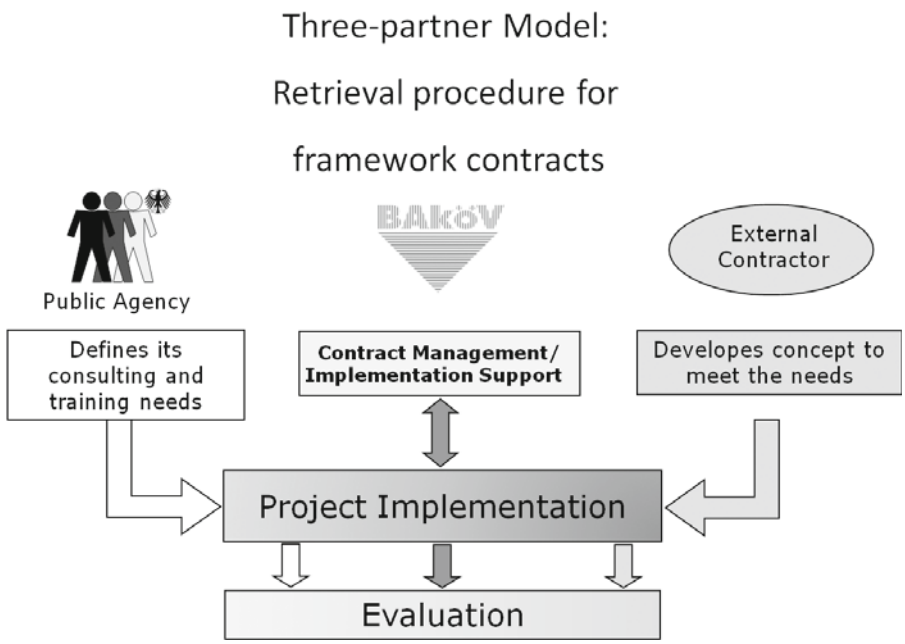

Fig. 2: Processes within the "three-partner model".

The Federal Academy provides a framework contract for the implementation of services in the field of information security awareness. The control and coordination of these contracts is carried out by the Federal Academy. For the retrieval of the services, public agencies place individual orders directly at the Federal Academy.

The use of the "three-partner model" helps achieve a centralized and efficient supply as well as a target-oriented adaptation of services, since the agencies define their needs themselves.

The framework contracts include the following services:

- Support in individual preparation, planning and implementation of actions in the agencies. This includes events for specific target groups, such as managers or IT professionals, as well as the design of flyers and posters or the evaluation of awareness measures.
- Seminars on "Information Security at Work", adapted to the needs of the respective agency.
- Creation of awareness modules (seminars, events etc.) and other material (documents, media).

3 Structure and contents of "Sicher gewinnt!"

To meet a wide range of the individual agencies' needs, the campaign has been conceived to include adaptable modules. These vary from planning tools, awareness and training modules and instruments, to communication material and interactive elements. All of them can be customized to the needs of an agency.

Smart Grids, Mobile & Wireless Security

Security Policy Automation for Smart Grids: Manageable Security & Compliance at Large Scale

Ulrich Lang · Rudolf Schreiner

ObjectSecurity
Cambridge, UK, and Palo Alto, CA, USA
{ulrich.lang | rudolf.schreiner}@objectsecurity.com

Abstract

A smart grid is an electricity network that has been infused with information and digital communications technology to provide greater control, stability, reliability and flexibility of the power grid. Technology has been added from the consumer premise which includes appliances, thermostats, home energy managers and load control switches all the way back to the generation facilities. The combination of these technologies could potentially optimize demand management, save energy, reduce costs, increase reliability, connect alternative and home-generated energy sources to the grid (i.e. transmitting a bi-directional flow of energy), and evolve into a powerful platform for new business opportunities. In order for smart grids to achieve all objectives, cyber security and risks (e.g. cybercrime or cyber warfare) and privacy concerns must be overcome. The smart grid adds new entry points to the older technologies that are already vulnerable but were previously protected from exploit by physical isolation. Theoretical concerns have become practical realities as a number of vulnerabilities in the smart grid and power complexes have been exploited. After a general introduction to smart grids and smart grid security, this paper analyses security (control) and compliance (visibility) requirements for smart grids. In order to justify the need for security policy automation, the paper focuses on the hard-to-implement least privilege, information flow enforcement, and security incident monitoring/reporting/auditing requirements. The paper then presents "model-driven security policy automation" (control) and "model-driven security incident monitoring/analysis automation" (visibility) within the context of smart grids, and explains how alternative approaches such as identity and access management and authorization management are necessary but not sufficient on their own. The presented "model-driven security" (MDS) policy automation solution uniquely helps solve the challenge of capturing, managing, enforcing, and monitoring/analysing fine-grained, contextual technical authorization policies for small to large scale smart grids.

1 Smart Grids

Smart grids are being promoted by many governments as a way of addressing energy independence, global warming issues, emergency resilience issues, and the attempt to phase out nuclear power in several countries. A smart grid is a form of electricity network combined with information technology – across generation at power plants, distribution and transmission along electrical lines, and delivery and consumption at the customer homes or businesses of a utility. A smart grid transmits electricity intelligently using two-way digital communications to continuously monitor the bi-directional flow of electricity and to control a number of devices across the grid,

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2011), 123-137
N. Pohlmann et al. (Eds.), *ISSE 2011 Securing Electronic Business Processes,*
DOI 10.1007/978-3-8348-8652-1_12,

including appliances at consumers' homes; this could potentially optimize demand management, save energy, reduce costs, increase reliability, and connect alternative energy sources to the grid – if the risks inherent in executing massive information technology projects are mitigated. The smart grid is envisioned to integrate today's electrical grid with large scale deployments of Information and Communications Technologies (ICT) and smart meters. Smart meters support quick and precise measuring and information gathering to allow easy, real-time control of electricity consumption (e.g. power, heating, and cooling devices, and appliances). One of many examples for the use of smart grids is that new technologies (e.g. electric vehicles, air conditioning and household appliances) will require more intelligent energy demand management, as well as involvement of users (e.g. through home automation). Because the final end-state is still unknown, today's smart grid rollouts can be viewed as the deployment of a general energy ICT platform that forms the basis for future energy-related applications. Because smart grids can potentially mitigate growing energy and environmental concerns, significant investments are being made. For example, the worldwide smart grid market in 2009 was $69 billion, with tens of millions of smart meters installed across the world. By 2014, it could reach about $170 billion. In the U.S., a chunk of the federal stimulus spending in 2009-10, some $3.4 billion, was directed to investment in, and modernization, of smart grids [Rick09]

Relevant for this paper, from an IT perspective, the authors expect that smart grids will have several unique features compared to "normal" IT environments, including: critical infrastructure reliability expected; extremely large scale/distribution/interconnectedness; many embedded devices (e.g. smart meters, SCADA based devices); many stakeholders involved; dynamic stakeholder roles (e.g. buyer, seller); increasingly dynamic/agile interactions between stakeholders; many utilities have very immature security practices or security practices that are not being included in the solutions development processes. This is mostly due to the lack of need prior to the incorporation of technology and network connectivity. Many projects are advancing through the lifecycle to the point of deployment before security is aware of what has happened.

2 Smart Grid Cyber Security

The smart grid vision can only become a reality if cyber security risks are sufficiently mitigated. This is because power grids are absolutely critical infrastructure – if power goes down for extended periods, the affected geographic area stands still. New cyber security challenges (e.g. cybercrime or cyber warfare) become a major risk factor due to the convergence of the information technologies (IT) with the electric power grid, the critical reliance on IT for smart grids, and the fact that parts of the smart grid will be connected to the internet (which makes them susceptible to many of the same malicious attacks that regularly occur against computer networks outside the electrical and energy sectors). The smart grid technologies are introducing in many cases millions of new points of entry into the electric grid by placing meters on every home that have connectivity back to the corporate network and its infrastructure. Some organizations are making attempts to ensure that the paths to the critical cyber assets are separated from the advanced metering infrastructure (AMI) networks, but others just do not appear to understand the risks.

There are also increased privacy concerns, as smart meters and other tools could leak personal and financial data on a consumer to utilities and attackers alike. Many organizations are not transmitting the account information over the networks, where the major issues lie in the usage information itself. Usage information could lead someone to be able to identify patterns that may

lead them to know when the consumer is present or away from the premise. However, because of a potential of lack of understanding of how their networks may be interconnected a utility could potentially expose its entire network to the AMI environment creating a vector to their critical infrastructure.

This changing environment poses a major challenge to power utility IT departments, which are not ICT/internet focused and currently mostly operate closed tried-and-tested legacy mainframe/server systems. In general, there is often a "culture gap" between the employees of IT shops and those of electrical and other infrastructure facilities, and government regulators.

A few examples of potential risks associated with the evolution of the smart grid include [Nist10]:

- Greater complexity and interconnectedness increases exposure to potential attackers and unintentional errors;
- Previously closed networks are now opened up and may span multiple smart grid domains ("system of systems"), which increases the attack surface and the risk of cascading attacks;
- More interconnections increase "denial of service" and malware related attack risks;
- Increasing number of attacker entry points and paths as the number of network nodes increases;
- Increased potential for data confidentiality and privacy breaches due to more extensive data gathering and two-way information.
- In deregulated areas the utility may not have control over the devices being utilized on the AMI or Home Area Network and therefore do not control the security requirements for those devices or even the kinds of devices that may be introduced to the environment.
- Unauthorised privileged access to AMI could provide the opportunity to send control commands or create denial-of-service in order to prevent the utility from issuing control commands
- Unauthorized access to meter could be exploited in many ways, e.g. readings could be altered for monetary benefit, spoofing the meter and injecting bogus responses to utility command as in denial-of service attacks, forging meter readings to gain monetary benefits

Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable, potentially safety-hazardous ways. A cyber-attack aimed at energy infrastructure "could disable trains all over the country and it could blow up pipelines. It could cause blackouts and damage electrical power grids so that the blackouts would go on for a long time" [Clar10]. A hacker with a basic knowledge of electronics and a few hundred dollars in hardware could interfere with, and get control over, the smart meters that are essential to managing the two-way interaction.

Theoretical concerns have become practical realities, as a number of exploits involving smart grids and power complexes have taken place. In particular in 2010, Stuxnet [Wiki11], a sophisticated malware attack that targets Siemens WinCC, industrial control software popular in the utility sector and other industries, via a Microsoft Windows vulnerability, infected at least a dozen systems worldwide (and specifically suspected nuclear weapons facilities in Iran) and represents the first publicly-known rootkit to specifically target industrial control systems. There are many other reported attacks on industrial control systems, e.g. [Cbsn10] [[Sans08]. Electric Power Research Institute (EPRI) has compiled a database of more than 170 infrastructure cyber incidents [Epri11].

Security Management, Identity & Access Management

Security Architecture in a Collaborative De-Perimeterised Environment: Factors of Success

Yulia Cherdantseva[1] · Omer Rana[1] · Jeremy Hilton[2]

[1]Cardiff University
{y.v.cherdantseva | o.f.rana}@cs.cardiff.ac.uk

[2]Cranfield University
j.c.hilton@cranfield.ac.uk

Abstract

Security Architecture (SA) is concerned with such tasks as design, development and management of secure business information systems. These tasks are inherently complex and become several orders of magnitude more sophisticated in a Collaborative De-Perimeterised Environment (CDePE). Although significant research exists about the technical solutions that may be used in a CDePE, we believe there is an important gap in current literature in addressing the specifics of collaboration and de-perimeterisation at the stages of design and management of a SA. This paper discusses how a CDePE is addressed in the ISO/IEC 27000 series of standards and identifies ten factors, besides technical ones, that are important for the success of a SA. This paper emerged as a result of an analysis of the current state of the information security discipline and of the modern trends in the discipline.

1 Introduction

Many disciplines have adopted the term *Architecture* from the science of designing and erecting buildings. The term is widely used in computer and information sciences; the field of information security is not an exception. As town building architecture defines rules for the construction of buildings, Security Architecture (SA) is concerned with the design and development of secure business information systems, i.e. systems that are free from danger and damage, reliable and resistant to failures and attacks [ShCL05: p.2].

The main aim of a SA is overall business security. A SA generally provides a framework for enabling security controls of different layers to operate coherently together and depends on three aspects [ShCL05: pp.19-24]:

- The business goals of an organisation implementing it;
- The environment in which an organisation operates;
- The technical capabilities available at the current phase of Information and Communications Technologies (ICT) evolution.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2011), 201-213
N. Pohlmann et al. (Eds.), *ISSE 2011 Securing Electronic Business Processes*,
DOI 10.1007/978-3-8348-8652-1_18,

A SA is often investigated purely from a technical viewpoint, whereas the impact of the business goals and the environment on a SA is ignored. We believe that the environment in which an organisation operates is very important and should be taken into account while developing and maintaining a SA. The tasks of SA as a science are inherently complex and become several orders of magnitude more sophisticated in the present environment, which we refer to as a Collaborative De-Perimeterised Environment (CDePE) and describe below.

The term *De-Perimeterisation* was coined by the Jericho Forum (JF), an international association of organisations that concentrates on the issues of secure business in a networked environment. The term refers to the erosion of an organisation's hard perimeter in response to the evolution of ICT and consequent change of business needs. Formally, the JF describes De-Perimeterisation as "the concept of architecting security for the extended business boundary and not an arbitrary IT boundary" [OGJF07].

Thus, a CDePE is an environment where third parties gain access to data and services hosted by the organisation internally and, similarly, the organisation accesses data and services hosted by other organisations. Previously, the distinction was clear: there were people inside the perimeter (staff) who were fully trusted and people outside the perimeter (non-staff) who were not trusted. At present, organisations need to allow access to data not only to its staff - remote and mobile, but also to service providers, collaborators, authorities and customers. Any organisation, to a greater or lesser degree, participates in collaboration and information sharing, works in a distributed environment and has started to exploit Cloud computing capability (mostly for remote data storage, but also, in some instances, for outsourcing high throughput computation) in order to reduce costs and to increase efficiency and commercial profit. As a result, in a CDePE perimeters of organisations erode and "closed" systems no longer exist.

We do not consider a de-perimeterised environment as an equivalent of a distributed environment. A distributed environment may also have a hard perimeter, whereas de-perimeterisation accentuates a need even for a distributed environment to soften its boundaries. Nor do we consider Cloud computing to be the only idiosyncratic feature of the stated environment. Cloud computing is only one many aspects of a CDePE and we discuss it in Section 3.8. A CDePE reflects the complexity that emanates from a plethora of activities, including collaborative information sharing, Cloud computing, remote and mobile working and from the cascading impact of the intensive linkages between them.

An open architecture of an organisation with a softened perimeter provides business opportunities, but, at the same time, makes information security a greater challenge. With the unprecedented level of interconnectivity available today, previously used strategies of perimeter security are unsustainable. An approach to information security is required that allows an organisation to operate within a soft perimeter and to protect information outside of the organisation's perimeter as well as inside it. This new approach is based on multi-layered security and accumulates protection capabilities of technologies, organisational measures, human factors and legislation.

Currently, within de-perimeterisation research a strong emphasis is placed on technologies [OGJF07]. However, de-perimeterisation is a socio-technical phenomenon worthy of detailed research not only from the standpoint of technical network specialists, but also from the standpoint of managers, system and security architects. Although significant research exists about technical solutions that may be used in the CDePE, there is an important gap in the current literature in addressing peculiarities of this environment at the stages of design, development and management

of a SA. Therefore, to cover this gap, we attempt to summarise and debate information security issues relevant to managers, system and security architects. Our aim is not a development of a new framework for a SA, but rather an identification of factors that are essential for the success of a SA in addition to any existing framework.

The remainder of this paper is structured as follows: Section 2 discusses how a CDePE is addressed in the ISO/IEC 27000 family of standards that provides a widely used framework for a SA. Section 3 outlines the factors that deserve to be taken into account while designing, implementing and managing a SA. Section 4 draws conclusions from the preceding discussion.

2 How the ISO/IEC 27000 Series of Standards Addresses a CDePE

The ISO/IEC 27000 series of standards is published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and reserved for information security matters. ISO/IEC 27001:2005 emulates the success of its predecessor BS7799 and sets the trend for this growing family of standards. It specifies the requirements towards an Information Security Management System (ISMS) and covers a wide range of issues, such as risk assessment; management responsibilities and commitment; resource management and provision; training, awareness and competence. Another constituent of the series is ISO/IEC 27002:2005 that contains a code of practice for information security management.

Both ISO/IEC 27001 and ISO/IEC 27002 were developed at the time when the business world was not so considerably affected by de-perimeterisation. Although the ISO/IEC 27000 family provides some basic recommendations that are applicable in a CDePE, these recommendations should be significantly extended and updated by an organisation wishing to make use of them in the present environment. Below we consider how a CDePE is addressed in ISO/IEC 27001 and ISO/IEC 27002, as well as we discuss any omissions in the standards. We start our analysis with ISO/IEC 27001:2005, where Section 4.2.1 a) suggests that an organisation shall

> *"Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusions from the scope."*

In the case of a "closed" system, it is easy to assume that the boundaries of the ISMS are equal to the boundaries of an organisation, whereas the task of defining the boundaries and the scope of the ISMS in the de-perimeterised environment is more complicated. According to the definition, the ISMS is a "part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security" and as such it "includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources" [BSIS05]. In the CDePE practices, procedures and policies may spread over multiple organisations that work together in order to achieve a common goal. Therefore, to define the boundaries of the ISMS an organisation should decide whether it should include service providers, collaborators and customers in the scope and to what extent they should be included. Neither ISO/IEC 27001, nor ISO/IEC 27002 provides any further details about establishing the scope and boundaries of the ISMS.

eID & eGovernment

pohlmann@internet-sicherheit.de

ETSI STF 402 – Standardizing the pan-European Infrastructure for Registered Electronic Mail and e-Delivery

Juan Carlos Cruellas[1] · Jörg Apitzsch[2] · Luca Boldrin[3] · Andrea Caccia[4] · Santino Foti[5] · Paloma Llaneza[6] · Gregory Sun[7]

[1]Universidad Politécnica de Cataluña
cruellas@ac.upc.edu

[2]bremen online services
ja@bos-bremen.de

[3]InfoCert
luca.boldrin@infocert.it

[4]UNINFO
andrea.caccia@studiocaccia.com

[5]Critical Path
Santino.Foti@criticalpath.net

[6]Llaneza & Asociados
pll@palomallaneza.com

[7]Macau Post eSign Trust Centification Authority
gregsun@seps.macaupost.gov.mo

Abstract

This paper outlines the main achievements of the ETSI STF-402 in the area of Registered Electronic Mail (REM henceforth), related to the provision of means for achieving interoperability between solutions that make use of S/MIME for structuring messages and SMTP as transport and some identified solutions using SOAP on HTTP respectively for the same purposes.

The paper provides details of 2 new technical specifications defining means for allowing exchange of messages between REM providers using SMIME on SMTP and systems that are compliant with Universal Postal Union (UPU henceforth) S52-1 specifications, as well as with implementations of Business Document Exchange Network (BUSDOX henceforth). It also provides details of a binding profile specifying how providers may exchange REM Messages and evidence as XML messages within SOAP structures transported over HTTP. SPOCS LSP and STF-402 have very closely cooperated in its generation, following a model that both

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2011), 267-278
N. Pohlmann et al. (Eds.), *ISSE 2011 Securing Electronic Business Processes,*
DOI 10.1007/978-3-8348-8652-1_24,

entities firmly believe could be exportable in the future within the EU context for speeding up the production of EU standards tuned to actual needs of the market.

The paper also provides hints on a report documenting test suites for supporting REM interoperability tests and the new version of ETSI TS 102 640 on REM.

1 Background

Early in 2006, ETSI identified an increasing need across Europe for a trustable electronic mail system, suitable to exchange electronic messages with a similar reliability to paper Registered Mail, i.e. systems able to generate trusted electronic evidence attesting that certain events had taken place (submission by a sender of a message to a recipient, delivery of the message to the recipient, etc). By that time, there were already implementations at national level within a number of European countries (like Posta Elettronica Certificata –PEC- in Italy, Electronic Court and Administration Post Office (EGVP) in Germany, IncaMail in Switzerland), and even legislation providing legal value to the evidence set generated by such kind of systems. Those systems also address end to end security issues (authentication, confidentiality, and electronic signatures of messages). They, however, were designed as "closed circuits" and not able to interoperate, so it was not possible to provide evidence on the transmission and/or delivery of one e-mail to senders and recipients subscribed to different systems.

ETSI Specialist Task Force 318 (STF 318 henceforth), a project funded directly by the ETSI membership formalized the concept of Registered Electronic Mail (REM henceforth) and delivered in January 2010 the ETSI Technical Specification (TS) 102 640 on "Registered Electronic Mail (REM)", a document to enable implementations of REM systems issuance of reliable evidence endorsed by relevant legislation, which was structured in the following five parts:

- Part 1: "Architecture" – specifying the architectural elements of Registered E-Mail.
- Part 2: "Data requirements, Formats and Signatures for REM" – specifying data requirements and syntax for the different types of REM messages, evidence and signatures.
- Part 3: "Information Security Policy Requirements for REM Management Domains" - specifying requirements on the security of a Provider of Registered E-Mail (REM Management Domain –REM-MD henceforth).
- Part 4: "REM-MD Conformance Profiles" specifying requirements that any provider claiming REM services provision must accomplish.
- Part 5: "REM-MD Interoperability Profiles" specifying requirements allowing interoperability among different REM service providers.

When the STF-318 was near of finalizing its work, it ascertained that an ever increasing number of Registered E-Mail (REM) and REM-like systems based on SMTP were already operational under development or in the design phase throughout the EU and the EEA (in Italy, Switzerland, France, Belgium, Germany, Spain), and this meant that it could be assessed that over 50% of the EU population already had or shortly would have SMTP based REM like systems available.

At the same time, the Universal Postal Union (UPU) was also developing a SOAP-based mailing system, and the European Commission was supporting and funding a number of very relevant Large Scale European Projects, which had to deal in one way or the other, with the reliable exchange of electronic documents between different parties in different contexts: PEPPOL (Pan-European Public eProcurement On-Line), SPOCS (Simple Procedures Online for Cross-border

Services) and STORK (Secure identity across borders linked) being the most relevant ones at that time. All of them had already decided to use SOAP on HTTP as the technical means for implementing such an exchange, which lead to conclude that SOAP based systems will in the future likely affect most of the EU Member State Public Administrations and, in a time lapse that is still difficult to foresee, possibly nearly all the postal authorities at the global level.

ETSI identified the real risks of a lack of interoperability between those systems based on different protocols. Indeed, if no mechanism suitable to allow mails exchange "across the technical borders" were commonly developed, two possible alternative situations might have occurred:

1. each EU Member State (or group of EU Member States) independently would have developed a mechanism of this type;
2. in those EU Member States where this did not occur, SMTP based and SOAP based mailing systems would not interoperate.

In the first case the consequence would be a multiplication of efforts and disbursement. In the second case there would be a strong penalisation of users, in particular of citizens and SMEs that would need to resort to a duplicated application to interface both systems, yet without even achieving full operations between the two mechanisms.

If, instead, it was decided to develop one EU solution, this interface would allow both "worlds" to take benefit from it with far lower costs.

In the view of the former considerations, ETSI got funding from the European Commission for setting up in March 2010 the Specialist Task Force 402, in charge of developing technical specifications for solving the interoperability between REM solutions based on different transport protocols. The present paper:

- Reviews the fundamental concepts formalized by STF-318 in the ETSI TS 102 640 specification.
- Provides an overview of the major goals of the STF-402
- Provides details of the specifications produced by the STF 402.

2 Review of Registered Electronic Mail fundaments as per STF-318

The ETSI TS 102 640 developed by the STF-318 specified an architecture encompassing the functional model shown in Figure 1.

The core entities in such model are the REM service providers. For them, the STF-318 coined the term Registered Electronic Mail Management Domain (REM-MD henceforth), adopting "Management Domain" term from X.400 specifications. This figure shows two REM-MD systems interacting and one REM-MD system interacting with Standard (i.e. conventional not registered) Electronic Mail providers (SEM-MD).

Device & Network Security

pohlmann@internet-sicherheit.de

Objectives and Added Value of an Internet Key Figure System for Germany

Sebastian Feld · Tim Perrei · Norbert Pohlmann · Matthias Schupp

Institute for Internet Security
Gelsenkirchen University of Applied Sciences
{feld | perrei | pohlmann | schupp}@internet-sicherheit.de

Abstract

This work is motivated by the fact that the Internet can be seen as a critical infrastructure, whose on-going operation is particularly worth protecting. Problematic when considering the state of the Internet are two things: On the one hand, there are many dependencies in the context of the Internet, on the other hand there are only a few key figures that allow comprehensive statements. In the course of this work, a Key Figure System will be described in which the control object is the Internet by itself. The complex structure of the Internet is to be made more transparent and the condition, changes and future potential are to be expressed. In addition to the various objectives that are to be achieved during the design and implementation of such an Internet Key Figure System, this work describes the problems that have to be solved. These are less technical, but in fact organisational and legal nature. Each Key Figure System requires a control object, that is a clearly defined scope, which the data collection, data processing and data visualisation refer to. In the following the definition of an „Internet Germany" is given and the appropriate stakeholder and criteria are described. This work concludes with an explanation of the different added value of an Internet Key Figure System for the various addressees.

1 Motivation

Today's Internet consists of a variety of networks, called Autonomous Systems (AS), which are operated by Internet Service Providers (ISPs), large companies and universities. There are currently more than 37,000 AS[1], which build the Internet with more than 70,000 connections. For a more detailed consideration and a proper assessment of the significance of each AS, it is important to see what role each AS occupies in the interaction of the Internet. AS are acting completely independent, so the operators have different strategies on how to organise the communication of IP packets on their network with the help of routing protocols.

Not only within Germany, the Internet as a part of the information and telecommunications technology is reckoned to the critical infrastructures [BMI09]. The impairment or loss of parts of the Internet can have an enormous impact. For example, the disturbance of IP telephony as the Skype outage in 2007[2] can lead to sustainable economic damages if a company is no longer able to conduct telephone business.

1 See, amongst others, the routing table of the project "Route Views" under [Rout11].
2 See [Skyp07].

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2011), 341-351
N. Pohlmann et al. (Eds.), *ISSE 2011 Securing Electronic Business Processes,*
DOI 10.1007/978-3-8348-8652-1_30,

Currently, an on-going operation of the Internet is essential. To ensure the most trouble-free operation, it is necessary to be able to observe the current state and also to estimate the future development of the Internet. It is the only way to face novel events (both positive and negative) optimally.

Basically the motivation for an Internet Key Figure System can be divided in two aspects: First, it is about the many different dependencies in the context of the Internet and second, it is about the barely available, pre-existing key figures.

1.1 Dependencies in the context of the Internet

There are many different dependencies in the context of the Internet, and in some cases, a dependency on a country – often the United States of America – can be noted. The dependencies can occur at various levels, including:

- Technical dependencies, such as the combination of parts of the Internet by means of intercontinental-laid undersea cable
- Dependencies at the service level, for example the „web surfing“ without the transparent use of the Domain Name System (DNS) is hardly feasible
- Administrative dependencies, for example the Internet Corporation for Assigned Names and Numbers (ICANN) coordinates, among other things, the management of top-level domains

In the following two examples of dependencies in the context of the Internet are highlighted.

There are few very large AS (so-called Tier 1 providers) that connect large parts of the Internet and thus achieve a connectivity of almost all end systems all over the Internet. These are enormously important for the stability of the Internet. Currently the largest and most important AS are American. The largest German AS, the one of Deutsche Telekom, can be found in the lower places of the TOP25 sorted by the number of connections[3].

Another example are Border Gateway Protocol (BGP) router, which are necessary for the smooth operation of the Internet. Under certain circumstances, the failure of particular BGP router can cause many user of the Internet to be unreachable. These may be customers of an ISP or an entire nation[4].

The idea of introducing an Internet Key Figure System is to make the complex architecture of the Internet more transparent and to express its condition, changes and future potential. The Internet economy receives a common Internet Key Figure System, with which the current state of the Internet can be represented with respect to different scales (see section „5.2 Stakeholder and criteria“).

1.2 Barely statistical key figures

There are barely statistical key figures for the critical infrastructure Internet. Though there are local data silos, these are not in a broader context.

3 See, amongst others, the routing table of the project “Route Views” under [Rout11].

4 Libya can serve as an example, which was completely separated from the rest of the Internet for some time in the spring of 2011. See, amongst others, [Heis11].

For example, large website operator or services for web traffic analysis (such as „Alexa Internet“ [Alex11]) can make statements about the distribution of the website visitors' used operation systems, web browsers, software and the like. E-mail provider or blacklist operators can provide statistics on the current amount of spam. Additionally, projects such as „Route Views“ [Rout11], BGPmon [Bgpm11] or „RIPE Atlas“ [Ripe11a] provide information regarding the connection of Autonomous Systems or the availability of Internet services.

The various information on aspects of the Internet offer, due to the lack of a global or comprehensive nature, only a limited statement. Many findings can only be generated when different data are linked. For example, a message about a serious vulnerability in a web browser is more relevant if the software is actually used by many users. If there would be this global or at least "higher" perspective, one could measure the current state of the Internet, assess the development of the Internet better and thus make better-informed decisions for the future.

2 Basic idea of an Internet Key Figure System

Key Figure Systems are used in the area of business administration for the quick receipt of concentrated information about a company's performance and efficiency. They can also assist in planning, monitoring and controlling of a company.

Such a **Key Figure System** describes an ordered set of interdependent business key figures. It aims to inform as fully as possible about a given situation. Thus a Key Figure System groups and processes logically related key figures. Thereby the information content of the Key Figure System is about to be higher than the sum of the information content of the individual key figures.

Basically a **key figure** describes an exact quantifiable measure, which results from a reproducible measurement of a parameter, state or process. In the context of a Key Figure System a comprehensible collection of the key figures is most important. Key figures can be divided into two areas: Absolute (atomic) key figures and relative key figures. Absolute key figures are those that are integrated from outside into the Key Figure System and can not be disaggregated further. Relative key figures, however, arise from the relationship of other key figures and are formed within the Key Figure System.

An **Internet Key Figure System** is in conclusion a Key Figure System in which the situation subject to investigation is not a company, but the Internet itself. It collects key figures that relate to the Internet or that are generated by the Internet.

The idea of introducing an Internet Key Figure System is to make the complex structure of the Internet more transparent and to express its condition, changes and future potential. The Internet economy receives a common Internet Key Figure System, with which both the current state of the Internet can be represented and a retrospective consideration with respect to the measured scales can be carried out. In the course of this work the objectives, problems and added value in the design, implementation and use of an Internet Key Figure System will be treated in detail.