

Norbert Pohlmann
Helmut Reimer
Wolfgang Schneider

Securing Electronic Business Processes

Highlights of the
Information Security Solutions Europe 2010
Conference

Contents

About this Book	vii
Welcome	xi
Germany on the Road to Electronic Proof of Identity	1
Ulrich Hamann	
Identity and Security Management	11
Security Analysis of OpenID, followed by a Reference Implementation of an nPA-based OpenID Provider	13
Sebastian Feld · Norbert Pohlmann	
New Authentication Concepts for Electronic Identity Tokens	26
Jan Eichholz · Dr. Detlef Hühnlein · Dr. Gisela Meister · Johannes Schmölz	
A Simplified Approach for Classifying Applications	39
Lenka Fibikova · Roland Müller	
Technical and Economical Aspects of Cloud Security	51
Single Sign-on(SSO) to Cloud based Services and Legacy Applications “Hitting the IAM wall”	53
Marcus Lasance	
Cloud & SOA Application Security as a Service	61
Ulrich Lang	
Authentication and Trust: Turning the Cloud inside out	72
Christian Brindley	
User Risk Management Strategies and Models – Adaption for Cloud Computing	80
Eberhard von Faber · Michael Pauly	
Security and Compliance in Clouds	91
Kristian Beckers · Jan Jürjens	
Applying BMIS to Cloud Security	101
Rolf von Rössing	

Security Services and Large Scale Public Applications _____ 113

Critical Infrastructure in Finance PARSIFAL Recommendations _____ 115

Bernhard M. Hämmerli · Henning H. Arendt

The SPOCS Interoperability Framework: Interoperability of eDocuments and eDelivery Systems taken as Example _____ 122

Thomas Rössler · Arne Tauber

STORK: Architecture, Implementation and Pilots _____ 131

Herbert Leitold · Bernd Zwattendorfer

Secure Networking is the Key to German Public e-Health Solution: Migration Towards an Integrated e-Health Infrastructure _____ 143

Bernhard Weiss

Advanced Security Service cERTificate for SOA : Certified Services go Digital ! _____ 151

J-C. Pazzaglia · V. Lotz · V. Campos Cerda · E. Damiani · C. Ardagna · S. Gürgens · A. Maña · C. Pandolfo · G. Spanoudakis · F. Guida · R. Menicocci

Privacy and Data Protection _____ 161

Data Protection and Data Security Issues Related to Cloud Computing in the EU _____ 163

Paolo Balboni

The Mask of the Honorable Citizen _____ 173

Johannes Wiele

Towards Future-Proof Privacy-Respecting Identity Management Systems _____ 182

Marit Hansen

Privacy Compliant Internal Fraud Screening _____ 191

Ulrich Flegel

Threats and Countermeasures _____ **201**

Malware Detection and Prevention Platform: Telecom Italia Case Study _____ **203**

Luciana Costa · Roberta D'Amico

Defining Threat Agents: Towards a More Complete Threat Analysis _____ **214**

Timothy Casey · Patrick Koeberl · Claire Vishik

A Mechanism for e-Banking Frauds Prevention and User Privacy Protection _____ **226**

Rosalia D'Alessandro · Manuel Leone

Countering Phishing with TPM-bound Credentials _____ **236**

Ingo Bente · Joerg Vieweg · Josef von Helden

Smart Grid Security and Future Aspects _____ **247**

Security Challenges of a Changing Energy Landscape _____ **249**

Marek Jawurek · Martin Johns

Privacy by Design: Best Practices for Privacy and the Smart Grid _____ **260**

Ann Cavoukian

A Policy-based Authorization Scheme for Resource Sharing in Pervasive Environments _____ **271**

Roberto Morales · Jetzabel Serna · Manel Medina

Visual Representation of Advanced Electronic Signatures _____ **280**

Nick Pope

DSKPP and PSKC, IETF Standard Protocol and Payload for Symmetric Key Provisioning _____ **291**

Philip Hoyer

Silicon PUFs in Practice _____ **300**

Patrick Koeberl · Jiangtao Li · Anand Rajan · Claire Vishik

Biometrics and Technical Solutions _____ 313**Visa Applications in TG Biometrics for Public Sector Applications _____ 315**

Dr. Sibylle Hick · Fares Rahmun · Ernest Hammerschmidt

Taking Signatures Seriously – Combining Biometric and Digital Signatures _____ 323

Santiago Uriel Arias

Automatic Configuration of Complex IPsec-VPNs and Implications to Higher Layer Network Management _____ 334

Michael Rossberg · Günter Schäfer · Kai Martius

SCADA and Control System Security: New Standards Protecting Old Technology _____ 343

Scott Howard

A Small Leak will Sink a Great Ship: An Empirical Study of DLP Solutions _____ 354

Matthias Luft · Thorsten Holz

eID and the new German Identity Card _____ 365**The New German ID Card _____ 367**

Marian Margraf

AusweisApp and the eID Service/Server – Online Identification Finally more Secure _____ 374

Werner Braun · Dirk Arendt

Postident Online with the new Personal Identity Card _____ 385

Jens Terboven

The eID Function of the nPA within the European STORK Infrastructure _____ 392

Volker Reible · Dr. Andre Braunmandl

Polish Concepts for Securing E-Government Document Flow _____ 399

Mirosław Kutylowski · Przemysław Kubia

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 eighth ISSE book – another mark of the event's success – and with about 40 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 and GI e.V. (Germany)
- **Gunter Bitz**, SAP (Germany)
- **Ronny Bjones**, Microsoft (Belgium)
- **Lucas Cardholm**, Ernst&Young (Sweden)
- **Roger Dean**, eema (United Kingdom)
- **Steve Purser**, ENISA
- **Jan De Clercq**, HP (Belgium)
- **Marijke De Soete**, Security4Biz (Belgium)
- **Jos Dumortier**, K.U. Leuven (Belgium)

- **Walter Fumy**, Bundesdruckerei (Germany)
- **Robert Garskamp**, Everett (The Netherlands)
- **Riccardo Genghini**, S.N.G. (Italy)
- **John Hermans**, KPMG (The Netherlands)
- **Jeremy Hilton**, Cardiff University (United Kingdom)
- **Francisco Jordan**, Safelayer (Spain)
- **Frank Jorissen**, McAfee (Belgium)
- **Bernd Kowalski**, BSI (Germany)
- **Jaap Kuipers**, DigiNotar (The Netherlands)
- **Matt Landrock**, Cryptomathic (Denmark)
- **Marian Margraf**, BMI (Germany)
- **Madeleine McLaggan-van Roon**, Dutch Data Protection Authority (The Netherlands)
- **Norbert Pohlmann (chairman)**, University of Applied Sciences Gelsenkirchen (Germany)
- **Bart Preneel**, K.U. Leuven (Belgium)
- **Helmut Reimer**, TeleTrusT (Germany)
- **Joachim Rieß**, Daimler (Germany)
- **Volker Roth**, Freie Universität Berlin (Germany)
- **Wolfgang Schneider**, Fraunhofer Institute SIT (Germany)
- **Jean-Pierre Seifert**, TU Berlin (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. www.teletrust.de

TeleTrusT Germany (“TeleTrusT Deutschland e.V.”) was founded in 1989 as a not-for-profit organisation promoting the trustworthiness of information and communication technology in open systems environments.

Today, as an IT security association, TeleTrusT counts more than 100 members from industry, science and research as well as public institutions. Within the last 20 years TeleTrusT evolved to a well known and highly regarded competence network for IT security whose voice is heard throughout Germany and Europe.

In various TeleTrusT working groups ICT 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, authentication and signature (IAS) schemes in electronic business and its processes.

TeleTrusT facilitates information and knowledge exchange between vendors, users and authorities. Subsequently, innovative ICT security solutions can enter the market more quickly and effectively. TeleTrusT aims on standard compliant solutions in an interoperable scheme.

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 German Federal Ministry of the Interior.

Contact:

Dr. Holger Muehlbauer

Managing Director of TeleTrusT Deutschland e.V.

holger.muehlbauer@teletrust.de

eema www.eema.org

For 23 years, **eema** has been Europe’s leading independent, non-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 London in partnership with OASIS

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.

Welcome

Ladies and gentlemen,

It is a particular honour to invite you to the twelfth ISSE Conference, taking place in Berlin on 5 - 7 October 2010, this year hosted by the Federal Ministry of the Interior.

The independent ISSE Conference focuses on secure information systems solutions in a globally networked world. Since the advent of the Internet, countless business, administrative and consumer solutions have transformed our society and the base of economic co-operation around the world. Without doubt, secure and trustworthy information systems are key for the reliability of any ICT infrastructure and future economic prosperity, particularly since more and more fixed and mobile business processes use the Internet.



The ISSE Conference offers the best environment to discuss innovations and new technical solutions for IT security in Europe. We expect more than 400 specialists, researchers, business leaders and policy makers from all over Europe to join us at ISSE to share information and best practices through thoughtful discussions and thorough debates.

Best wishes for a successful and productive conference. I look forward to seeing you in Berlin!

A handwritten signature in black ink, which appears to read 'Thomas de Maizière'.

Thomas de Maizière
Federal Minister of the Interior

Security in many layers

Technically speaking, the new polycarbonate card that is centrally produced at Berlin-based Bundesdruckerei is designed according to the multi-layer principle. The document chip is embedded in several layers of security foil placed on top of each other. These individual layers of foil are irreversibly bonded together in a special production process and using a colour personalisation method, so that the chip, the printed data and the card body form a self-contained unit. Any attempt to manipulate the data would involve damaging the material and hence destroying the document as a whole.

Trust based on reciprocity

According to BITKOM, the German Federal Association for Information Technology, Telecommunications and New Media, more than 70 percent of all Germans go online on a regular basis. In Germany, just like in any other country around the globe, the Internet has become one of the most important sources of information and social platforms for many people. In order to be able to make the best possible use of the growing digital diversity, reliable information regarding the identity of the process participants is becoming increasingly important. At the same time, the sometimes very complex and error-prone control processes are limiting the efficiency and economic feasibility of many online applications, not just in Germany, and are resulting in a sheer endless flood of data.

This is all set to change fundamentally when the new ID card is introduced in November 2010. All new document holders over the age of 16 will have the option to also use the handy card in ID-1 format – comparable to the size of a credit card – for everyday online shopping, to register on online platforms and for digital communications with public authorities. This is based on the principle of mutual authentication, i.e. the user and supplier must identify themselves to each other and hence clearly prove that they are who they claim to be (refer also to Fig. 3).

More than 170 German companies and institutions who have been preparing their new online services since October 2009 in various application tests will be ready to start regular business when the new document is officially launched. Citizens will then be able to experience for themselves the security and convenience which the new eID card (eID: electronic identity) has to offer.


New ID card	Electronic functions
	<div>1. Biometrics<ul style="list-style-type: none">Digital photo and two electronic fingerprints (optional)Exclusively for authorities entitled to check identities, e.g. police and border control officers</div> <div>2. Electronic proof of identity<ul style="list-style-type: none">For eBusiness and eGovernmentPIN and authorisation certificate required</div> <div>3. Qualified electronic signature<ul style="list-style-type: none">Certificate can be loaded later on the chipSupplied not by the state, but by the market (pursuant to the Act on Digital Signature)</div>

Fig. 2: The new German ID card combines the conventional function of the photo ID card with new electronic functions – in handy ID-1 document format

Give and take – the principle of networked system chains

By today's standards, the German model is now already seen to be one of the most secure and demanding solutions in Europe.

This is primarily due to the *eCard API Framework* developed in Germany, an IT framework structure that has been specified by the German Federal Office for Information Security (BSI). The framework defines new interfaces for electronic identity and signature cards (Application Programming Interface / API) and enables simple platform-independent communication between different eCards and their applications. The so-called *PACE* (Password Authenticated Connection Establishment) method, another component of the new eID infrastructure, will permit additional password-based data release.

This will make it possible to have personal data read directly from the integrated chip of the document and used for online transactions. These transactions are only possible when both the document holder and the online supplier selected by the holder use the same system components and when both partners have identified themselves to each other.

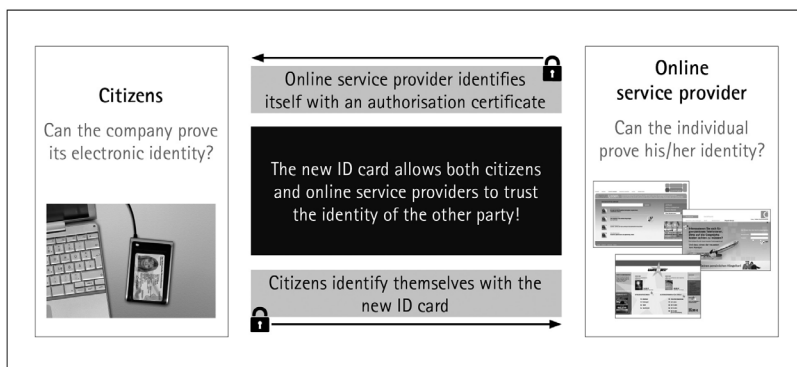


Fig. 3: The electronic functions and security mechanisms bring security to a new level and generate more trust in transactions and communication in the digital world

Full control over data for citizens

The main goal of the new German ID card system is to warrant the informational self-determination of each citizen that is anchored in German constitutional law. Extended Access Control (EAC), for instance, a security protocol already in use in the German electronic passport, will be used. This means that before any data is exchanged, Terminal Authentication and Chip Authentication first check the scope and type of access authorisation as well as the integrity and authenticity of the document chip (refer to diagram).

Identity and Security Management

Security Analysis of OpenID, followed by a Reference Implementation of an nPA-based OpenID Provider

Sebastian Feld · Norbert Pohlmann

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

Abstract

OpenID is an open, decentralized and URL-based standard for Single Sign-On (SSO) on the Internet. In addition, the new electronic identity card (“Neuer Personalausweis”, nPA) will be introduced in Germany in November 2010. This work shows the problems associated with OpenID and addresses possible solutions. There is also a discussion on how to improve the OpenID protocol by the combination of the nPA respectively the Restricted Identification (RI) with an OpenID identity. The concept of an OpenID provider with nPA support will be presented together with its precondition. The added value created by the combination of the two technologies nPA and OpenID in different directions is discussed.

1 OpenID as a standard for SSO on the Internet

1.1 Problem

Today, users of IT systems in both the private and the business environment have to memorize more and more access information.

In the private environment this arises from the fact that more and more services move into the Internet. The served applications range from e-mail clients and office suites to social networks. There is a login (the claim and the subsequent proof of identity) in almost every service before it can be used. This becomes a problem if a user chooses too short or simple passwords, uses the same password for different services (for convenience) or writes down the passwords.

But even in business environment, employees have to take care of the subject Identity Management (IdM) and its implications. Through the personal use of services an employee will perform various logins often several times a day. Examples are the login to the operating system, to customer databases and e-mail accounts or the use of the corporation’s Internet. A company may establish password policies that define a minimum length for certain passwords or the need to change them at regular intervals. According to experience an increase in security often leads to a decline in user friendliness or efficiency as well. In addition, there are costs resulting from non-

productive time (an employee returns from vacations and forgot the password), or the operation of a user help-desk (a central place to restore forgotten passwords amongst others).

There are different remedy approaches for the problem described. This work deals in particular with the idea of Web Single Sign-On (Web SSO) and the so-called strong authentication. On Web SSO there is only one identifier and a unique authentication using, for example, a strong password. The disadvantage is the single point of failure (the identity manager's service) and the urgent risk of phishing. OpenID is an example of a Web SSO protocol. On strong authentication (also multi-factor authentication), multiple factors like knowledge, possession and property are used to determine identity. A classic example is the use of smart cards with digital certificates. A concrete implementation of this strategy is the eID feature of the new electronic identity card in Germany.

1.2 Overview of OpenID

OpenID is an open, decentralized and URL-based standard for SSO on the Internet [ReRe06]. In version 2.0 of the specification (since 2007), a user can freely choose both the identity and the identity manager [ReRe07]. The identification of a user takes place via the proof of the possession of a URL, called OpenID identity.

The great benefits of Web SSO in general, and OpenID in particular is the one-time login at the identity manager (OpenID provider, OP) and the subsequent use of any OpenID-supporting services (relying party, RP). The credentials of a user (client, C) are not longer deposited at many points on the Internet, but only at a central and trusted authority, the OP. Consequently, the digital identity of a user is no longer distributed and redundant, there is only one identifier – the OpenID identity (Identifier, I).

The biggest danger in context of OpenID is the high vulnerability to phishing when using passwords. If an attacker acquires the password of an OpenID identity, all connected services are available to him or her. This can be done, for example, through phishing or by the fact that a user chooses a weak password. Another problem is the possibility of profiling on the part of the OP. The OP knows both the services utilized by the user and the frequency of use and thus could sell these information as user profiles.

1.3 Course of the protocol

The execution of OpenID consists of seven steps which are described more detailed below (see Figure 1):

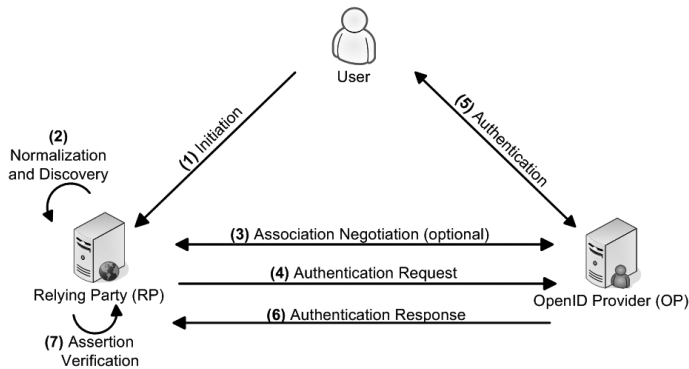


Figure 1: Course of the OpenID protocol

Initiation is the transfer of the user-chosen identifier to the relying party which starts the login process. A user calls the website of the service provider (RP), and names only an OpenID identity (the identifier) instead of a user name and password. An example could be <https://openid.internet-sicherheit.de/johnDoe>. The submission of the HTML form to the RP ends the first step.

Normalization/Discovery describe the process by which the relying party converts the OpenID identity entered by the user in a standardized form on the one hand and obtains information about the responsible OpenID provider on the other hand. The RP starts with normalizing the identifier entered by the user (see [BeFM05], chapter 6). An example is the addition of a missing schema such as <https://> to openid.internet-sicherheit.de/johnDoe. Subsequently, the RP executes the Discovery in which the information needed for generating an authentication request are determined. The XRDS or HTML document identified by the Discovery contains information about the location of the OpenID service on the part of the OP (OP Endpoint URL), the version of the supported OpenID protocol (Protocol Version), the name of the claimed identity (Claimed Identifier) and an alternative representation of the identifier (OP-Local Identifier).

Association Negotiation (optional) establishes a communication link with secured integrity between relying party and OpenID provider. RP and OP negotiate a shared secret in order to digitally sign and verify subsequent OpenID messages. If a RP is not capable of creating or saving associations (optionality of this step), the so-called “stateless mode” is used. For this, the OP creates a private secret for signing OpenID messages. The RP verifies messages received through direct communication with the OP (see [ReRe07], chapter 11.4.2).

Authentication Request is the request of the relying party to the OpenID provider to authenticate the user. The RP forwards the user’s web browser together with the OpenID authentication request to the OP.

Authentication is the actual verification of the user’s identity. The OP checks whether the user is in possession of the OpenID identity and whether he or she wishes to perform the current authentication. The characteristic of the user’s authentication is not specified in the standard ([ReRe07], chapter 3). The responsibility is entirely with the OP, on whose statement a RP has confidence in. The execution of authentication is effectively outsourced. These days the combination of user name and password is a common mechanism for authentication.

Technical and Economical Aspects of Cloud Security

Single Sign-on(SSO) to Cloud based Services and Legacy Applications “Hitting the IAM wall”

Marcus Lasance

Phillipssite 5, 3001 Leuven, Belgium
Verizon Business
marcus.lasance@verizonbusiness.com

Abstract

With the advent of the de-perimeterized organization and increased scepticism around ‘Cloud Security’ is SSO still a viable worthwhile goal for organisations?

Single Sign-On (SSO) projects are a special case of Identity and Access Management (IAM) projects. They are usually undertaken with the aim of increasing the user friendliness of Corporate IT systems’ user log-on processes. This should result in abolishing the use of multiple username and password combinations the user has to remember and change at different intervals. The SSO aim should be achieved without jeopardizing information security in any way. Increasing user convenience in such a manner will increase user satisfaction with the IT department along with general productivity levels.

Cost control related to IT help desks resetting forgotten passwords should follow.

SSO can also help organizations address information security compliance requirements, through the central logging (and audit facilities) of all access attempts and authorization decisions granted in relation to the organization’s restricted information resources. Sometimes compliance objectives are in fact the major business driver for SSO.

In the consumer space customer loyalty and retention rates are often cited as an important commercial driver for SSO projects.

With the advent of the de-perimeterized organization¹ and increased scepticism around ‘Cloud Security’ is SSO still a viable worthwhile goal for organisations?

This paper takes a closer look at special security issues arising when an organization attempts to create an Enterprise Single Sign-On (ESSO) solution that includes both legacy applications hosted within traditional organizational firewalls and a new breed of ‘Cloud Based’ solutions that are following the Software as Service (SaaS) model and therefore can be hosted with any number of Service Providers (SP) ‘in the cloud’.

1 Examining the role of IAM as SSO enabler

When thinking about SSO and Information Security two conventional wisdoms often come to mind. The first is the concept of avoiding dependence on ‘the weakest link’ in your organizations defences. The second is the concept of not wanting to put all your eggs in one basket.

¹ <http://www.opengroup.org/jericho/deperim.htm>

For the weakest link in protecting information assets read ‘Username and Password’ which, like no other authentication method, is highly vulnerable to social engineering attacks, malware key loggers and yellow ‘post-it’ notes left by lazy PC users for office cleaners to read.

In a homogenous single organization from an IT perspective the weakest link argument against SSO can be quickly countered by giving, as part of the project, all users a much stronger form of authentication. This usually means replacing ‘Username and Password’ with two factor authentication.

In other words, the bar is raised for everyone, without exception. This in itself can of course be a costly exercise, wiping out any potential cost savings of an SSO project.

Another question is: “Will all the business partners in a given federation be able to set the bar for information protection at the same high level?”

The question is not just related to the available budget in other parts of the federation, e.g. to purchase authentication tokens, but also a question of compatibility of security policies and audit capabilities between partners.

In the UK a ‘fly on the wall’ TV documentary recorded the unauthorized access of client financial records by call center employees from a marketing agency contracted by a well know high street bank. The call centre had a high staff turnover and was in fact ‘recycling’ a number of not individually assigned network access tokens to access client accounts. This is of course not the kind of federated SSO we want, as any audit log would prove absolutely nothing except that the bank was not really in control!

The ‘putting all your eggs in one basket’ paradigm could be used to make a case against SSO, with the argument that if one individual computer system’s security was to be breached at least the integrity of most other systems could be presumed still to be intact.

This is a very weak argument. How many users use the same username password combination for many of the corporate applications they access? For the simple reason they cannot begin to remember them all and writing them down is prohibited? The added protection provided by multiple sign-on(s) may be just an illusion!

2 No SSO without solid Identity Management!

As the example in the frame above illustrated, once SSO is enabled with a strong authentication form factor (RSA SecureID Token, PKI smartcard or OTP) it becomes of paramount importance to manage the users’ entire life cycle with the organization. An ex-employee logging in with a token that was not decommissioned is still a security breach. This means, not only are we aiming to provide the right levels of access from day one with the organization and making the new employee immediately productive; we also need to ensure that access is removed the very instant an employee leaves the company, sometimes well before! The same applies to partner employees.

Security Services and Large Scale Public Applications

Critical Infrastructure in Finance

PARSIFAL Recommendations

Bernhard M. Hämmerli¹ · Henning H. Arendt²

¹Acris GmbH & HSLU
bmhaemmerli@acris.ch

²@bc*
henning.arendt@atbc.de

Abstract

The PARSIFAL projekt (Protection and Trust in Financial Infrastructures) project is a Coordination Action funded within the FP7 European Research Programme Joint Call for Information and Communications Technologies and Critical Infrastructure Protection. Project Coordinator is ATOS Origin Sae/Spain, partners are ACRIS GmbH/Switzerland, @bc, - Arendt Business Consulting/Germany, Avoco Secure Ltd,(UK, EDGE International BV/Netherlands, Waterford Institute of Technology/Ireland. This article summarizes the recommendations for future research how to better protect Critical Financial Infrastructures (CFI) in Europe. It should be a valuable guidance to initiate projects that address these stakeholders' recommendations.

1 PARSIFAL – An Overview

The European Programme for Critical Infrastructure Protection (EPCIP) [2] lists 11 sectors of critical infrastructure including the Critical Financial Infrastructure. The PARSIFAL (Protection and Trust in Financial Infrastructures) project is a Coordination Action funded within the European Research Programme Joint Call for Information and Communications Technologies and Critical Infrastructure Protection. Project Coordinator is ATOS Origin Sae/Spain, Partners are ACRIS GmbH/Switzerland, @bc, - Arendt Business Consulting/Germany, Avoco Secure Ltd,(UK, EDGE International BV/Netherlands, Waterford Institute of Technology/Ireland. Cooperation partners of PARSIFAL are the European Finance Forum and another FP7 project Communication Middleware for monitoring Financial Critical Infrastructure (CoMiFin). The duration of the project was 18 months. It started September 2008 with the following project objectives

- Bringing together CFI research stakeholders
- Contributing to the understanding of CFI challenges
- Developing longer term visions, research roadmaps, CFI scenarios and best practice guides
- Coordinating the relevant research work, knowledge and experiences

This summary serves for both: for executives of the finance industry to initiate projects that address the stakeholders' recommendations, and for the research community to address the topic and find partners in the financial sector. The methodology (section 2) describes the process which

led to the mapping of challenges to scenarios (section 3) and the eight overall recommendations (section 4). The dependencies and interrelation of the eight recommendations are analysed (section 5) in order to generate a consecutive order of projects. The prioritization process of the eight recommendations (section 6) is discussed and the three key documents with background and detail level information created by the project partners are presented (section 7). Finally conclusions are taken.

2 PARSIFAL Methodology

PARSIFAL strengthened engagement between the European Commission and the Financial Services Industry in terms of trust, security and dependability. For Critical ICT infrastructures, directions for future research programmes were elaborated.

PARSIFAL established an Experts Stakeholders Group (ESG) to align research in this area to the needs of the Financial Services Industry. The ESG includes key actors in the CFI protection with sub-groups representing the financial industry, academia and government. ESG topics covered financial, IT, R&D, 'Trust, Security and Dependability' (TSD), and service providers' perspectives. Members include high level decision-makers as well as managers and experts related to the topics. PARSIFAL engaged closely with other R&D projects in the ICT/CIP/CFI domains, most specifically the CoMiFin project funded in the same call. The activities of the project centred on two ESG workshops, where stakeholders exchanged their views directly and discussed future scenarios and challenges from various perspectives in a first workshop in which the research challenges of the financial sector were discussed in the following three topics related expert groups:

1. Controlling Instant On Demand Business in CFI: Authentication, identity management, resilience and denial of service;
2. Entitlement Management and Securing Content in the Perimeterless Financial Environment: Identity, policy, privacy and audit;
3. Business Continuity and Control in an Interconnected and Interdependent Service Landscape: Compliance, protecting critical processes.

The three stakeholder working groups used written exercises and discussion to define future scenarios and challenges in CFI protection.

The discussions in the groups were twofold. First, the future scenarios were discussed, which need a change in security or more attention. The scenarios are the justification of why something could be more important in the future. Second, expected technology developments, technology related innovations, and research challenges were discussed. Finally, a mapping of the challenges to the scenario helped to eliminate technology visions without any clear relation to improvements in the financial infrastructure.

3 Mapping CFI Challenges to Scenarios

As a result of their first workshop, PARSIFAL mapped challenges in CFI protection to appropriate scenarios. This action compared and clarified the challenges of securing CFI.

Figure 1 is a condensed re-representation of a 30 scenarios by 30 challenges matrix that shows the main areas of concern, as directly expressed by the stakeholders.

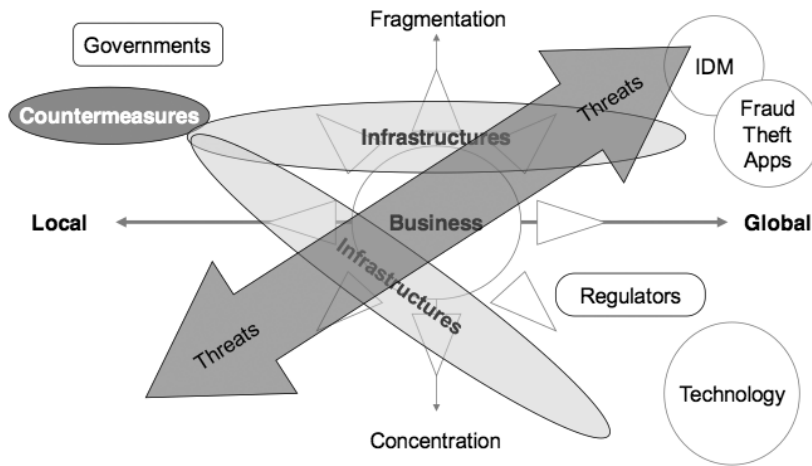


Fig. 1: Mapping Scenarios and Challenges

The **key ideas** and **paradigms** in this diagram are:

- Infrastructure - technology platforms, increasing complexity
- Infrastructure - business practises and working patterns, increasing complexity
- Infrastructure - data security methodology, highly distributed networks and borderless environments
- Countermeasures - robust Identity Management (IDM), new threat/ fraud recognition methods
- Systems - identity mechanisms and identity management
- Compliance - highly distributed networks and borderless environments, data security in highly distributed networks
- Global threats versus local measures

4 PARSIFAL Recommendations and Research Directions

The project results in the form of recommendations for future research are results from preparation papers of the project team, the presentations at the workshops, the written work done at the workshop and the post processing in the research team.

As a result of the discussions on CFI challenges and scenarios, PARSIFAL formulated eight recommendations for future research in the area of CFI protection:

Table 1: Work-Streams and Recommendations

Stream 1: Instant on Demand Business	1. Classification of identity attributes for wired on-line and mobile users of financial services should be defined and well understood by providers of these services and their customers.
	2. Trust indicators need to be developed, which allow for the various gradients of trust any entity might achieve when using specific financial services.
	3. Support platforms are needed for the management of multiple identities to allow consumers to authenticate themselves with various professional and private identity attributes.
Stream 2: Entitlement Management	4. Digital identities are required that are highly standardised across the financial services sector, with the introduction of mandatory IDs for all financial institutions, cross border interoperability and a “single/global” identity issuing authority.
	5. Data Security measures are required, such that (1) a digital identity links directly with a security policy to a data object, (2) data is secured as encapsulated entities, and (3) with flexible security policies that are based on individual access rights plus Digital Rights Management (DRM) for enterprise content to allow for flexible security policies and geographic boundary control.
	6. New Computing Paradigms need to be analysed, which allow for de-perimeterization of the organisation, e.g. Cloud Computing, supported by any new security focus. Predictive models need to be created to understand security risks. Cross border legal issues need to be resolved.
Stream 3: Business Continuity	7. Design and implementation of secure platforms and applications should be researched, such that an alternative and secure communication system/infrastructure will be available, including an adequate coordination response team(s) at a national and international level.
	8. Testing, design and implementation of such secure platforms should be elaborated as well as applications- and infrastructures- test through trustworthy multilateral exercises between CIP-sectors and governments. Models for business continuity need to be extended to (1) sharing risks and (2) end-to-end communication between trade participants, as well as to (3) the volume and the complexity of specific financial markets. These models should be “crash” tested, regularly evaluated and updated.

The target population of our recommendations can be divided into four groups:

1. The European Commission.
2. Providers of financial services and operators of financial infrastructures.
3. EU Member States Governmental agencies and regulators.
4. IT security experts and researchers.

5 Dependencies between the Recommendations

In a complex process with consideration of the stream and sense of urgency figure 2 was developed showing the timeline (starting with recommendation six), the dependencies and interrelation of the recommendations.

The eight recommendations are dependent, time- and content-wise. These dependencies should be considered in more detail when deciding which area of research to emphasize. Figure 2 takes into account these dependencies and outlines the research program which might result from the recommendations, where each recommendation could be a 2-3 year Specific Targeted Research Project (STREP).

Privacy and Data Protection

Data Protection and Data Security Issues Related to Cloud Computing in the EU

Paolo Balboni

Via Mascheroni 2, 20122, Milan, Italy, Avv. Dr. Paolo Balboni Law Firm
European Privacy Association, Italian Institute for Privacy, Tilburg University
paolo.balboni@paolobalboni.eu

Abstract

We are in the midst of a revolution within computing. It goes under the name of cloud computing. Analysts estimate that in 2012, the size of the enterprise cloud-computing business may reach \$60 billion to \$80 billion – or about 10% of the global IT-service and enterprise-software market [DeSa09]. Such inevitable revolution brings about a lot of benefits but also several legal concerns. It has emerged from a recent study that security, privacy and legal matters represent the main obstacles that are encountered when implementing cloud computing, because the market provides only marginal assurance. This paper briefly describes the main legal issues related to cloud computing and then focuses on data protection and data security, which are by far the biggest concerns for both cloud service providers (CSPs) and (potential) customers. I build on the work done last year as contributor to the European Networks and Information Security Agency (ENISA) ‘Cloud Computing Risk Assessment’ to further analyse data protection and data security issues. It is worth clarifying that the present paper analyses cloud computing services offered by CSPs to businesses (as opposed to consumers), i.e., B2B cloud computing.

1 Introduction

We are in the midst of a revolution in computing. It goes under the name of cloud computing. In a nutshell, cloud computing is “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or services provider interaction.” [McGr09] Analysts estimate that in 2012, the size of the enterprise cloud-computing business may reach \$60 billion to \$80 billion – or about 10% of the global IT-service and enterprise-software market [DeSa09]. Such inevitable revolution brings about a lot of benefits but also several legal concerns.

It has emerged from a recent study that security, privacy, and legal matters represent the main obstacles that are encountered when implementing cloud computing, because the market provides only marginal assurance¹. [ChHe10]

¹ In this respect, it is worth pointing out the project: ‘Common Assurance Maturity Model’ (CAMM) <http://common-assurance.com>, which aims at serving as the new business barometer to assess, measure, and qualify the security profiles of selected Cloud Service Providers. CAMM’s objective is to provide business users, and security professionals with granular articulations of the level of security associated with a particular cloud provision. Culminating with assured and tested information which may then be leveraged to gain insight as to how a Cloud Providers profiles meet with (potential) customers’ overall organisation security, governance, and compliance expectations.

This paper briefly describes the main legal issues related to cloud computing (Section 2) and then focuses on data protection and data security (Section 3), which are by far the biggest concerns for both cloud service providers (CSPs) and (potential) customers. I build on the work done last year as contributor to the European Networks and Information Security Agency (ENISA) ‘Cloud Computing Risk Assessment’ [BaMS09] to further analyse data protection and data security issues.

The following specific questions will be addressed:

- a. When does Directive 95/46/EC apply (Subsection 3.1)?
- b. How are data protection roles (i.e., data controller and data processor) distributed in the cloud environment, and thus the related duties, obligations, and possible liabilities (Subsection 3.2)?
- c. Which data security measures need to be applied (Subsection 3.3)?
- d. What are the possible ways to lawfully transfer personal data to countries outside the European Economic Area (EEA) (Subsection 3.4)?
- e. How can data subject rights be guaranteed (Subsection 3.5)?

Section 4 hosts the conclusions.

It is worth clarifying that this paper analyses cloud computing services offered by CSPs to businesses (as opposed to consumers), i.e., B2B cloud computing (as opposed to B2C). For an analysis of data protection issues related to B2C cloud computing services I recommend reading the paper entitled “Cloud Computing and Its Implications on Data Protection” drafted for the Council of Europe by a group of researchers led by Yves Poullet of the Research Centre on IT and Law (CRID). [PGG+10] Whereas, for an analysis of technical and legal issues related to the use of cloud computing services by Governments, a dedicated ENISA study “Security and resilience in Gov clouds” will be published by the end of 2010.²

2 Main Legal Issues Relate to Cloud Computing

Cloud computing can be defined as the ultimate expression of outsourcing. Whereby the customer contracts out to the CSP computing resources (e.g., networks, servers, storage, applications, and services), which are fundamental to run customer’s business. Inevitably, the stability and the results of customer’s business become very dependent from the CSP correct performance. Moreover, considering that the services provided by CSP are mainly e-mail, messaging, desktops, account and finance, payroll, customers’ billing, project management, CRM, sales management, and custom application development, a significant number of customer’s critical information and personal data may circulate in the cloud and thus be managed/processed by the CSP.

The cloud model is strongly based on the concept of ‘location independence’. Fundamentally, “the provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.” [MeGr09] Information and personal data are rapidly transferred from one datacenter to another and the customer invariably has no control or knowledge over the exact location of the provided resources. Exceptionally, the customer may be able to specify the

2 Keep an eye on the ENISA website: www.enisa.europa.eu.

location, but only at a high level of abstraction (e.g., country, state or datacenter) and at additional cost.

The main legal concerns related to the cloud model are related to data protection and data security; confidentiality of the information and intellectual property; law enforcement access; CSP professional negligence; subcontracting of cloud services and CSP change of control; and 'vendor lock in'. [BaMS09]

Data protection and data security issues will be dealt with in Section 3.

Secret information, 'know-how', copyrighted work, and patented inventions may circulate in the cloud. An information security breach in the cloud may directly threaten the customer, and may never be fully restored in subsequent legal proceedings. Therefore, such issues should be addressed in dedicated contractual clauses, i.e., 'Confidentiality/Non Disclosure Clause' and 'Intellectual Property Clause'. Whereby the boundaries of parties' responsibility and related liabilities should be clarified. Service Level Agreements (SLAs) and Technical Annexes may be particularly suitable for specifying technical means of transferring, conserving, processing, accessing, and safeguarding customer's business-sensitive information. [BaMS09] [PGG+10]

As already pointed out, computing resources are usually offered to customers from different locations at different times; information and data related to their businesses can easily and quickly be transferred from one datacenter to another one in an entirely different country. Customers should be aware that requirements and restrictions concerning law enforcement access to data may significantly vary from one country to another. In fact, datacenters can be established in countries that provide little or no protection to personal data in the framework of law enforcement activities. Moreover, exactly "[t]he development of datacenters might provide great opportunities to public authorities to access to a great amount of information pertaining to its citizens or to foreign citizens. Even considering democratic countries, the United States of America constitute a problematic example due to the very controversy third party data issue in the limited scope of the Fourth Amendment protection". [PGG+10] Therefore, if particularly business-sensitive information/data are to be processed in the cloud, customers should consider whether to specify the location (e.g., country, state, or datacenter) where their information/data will be processed. Customers, that request such customization of cloud-computing services, have to be prepared to bear additional costs. Moreover, it will be advisable for the parties to specify in a clause "how a law enforcement entity may be given access and what type of notice will be given to the parties if this occurs." [BaMS09]

By contracting out to the CSP fundamental computing resources, customer's business becomes very dependent from the CSP's correct performance. CSP failures or shortfalls in the provision of the cloud services may significantly impact on customer business and customer ability to meet its own duties and obligations towards clients and employees; potentially exposing the customer to actions for damage in contract or tort. On the other hand, customers' negligence in using cloud-computing services may lead to loss and damage for the CSP. SLAs and "Liability" and "Indemnity" clauses will play a fundamental role in this matter. Detailed SLAs, in which CSP levels of performance are accurately spelled out, coupled with contractual clauses that clearly allocate, on the one side, general parties duties and obligations, and, on the other side, parties' liabilities and responsibilities will be crucial for a fruitful relationship.

Threats and Countermeasures

Malware Detection and Prevention Platform: Telecom Italia Case Study

Luciana Costa · Roberta D'Amico

G. R. Romoli 274, 10148 Turin, Italy – Telecom Italia SpA
{luciana.costa | roberta.damico}@telecomitalia.it

Abstract

This paper illustrates the botnet problem, its impact and the need of security measures. By reviewing the existing literature regarding the botnet detection solutions the paper evidences the important role an ISP could take to better safeguard the user reducing in the meantime the spreading of the botnet phenomenon. The malware detection and prevention platform that Telecom Italia has defined is described. The aim is to minimize the potential harm that bots can inflict upon Internet infrastructure and to provide a detection and notification way to the users when their machines try to access a malware domain or when there is evidence that their computers have been compromised.

The idea is not necessarily to block or delay the users' traffic but to inform the users about the potential security risk on navigating on compromised sites, leaving anyway to the users the final choice to access the malicious domain. A security portal is accessible from a user detected as potentially infected with the aims to provide a common, well-organized set of information useful to clean the compromised system. Following this approach TI intends to prevent damage to its infrastructure while contrasting the malware infection spread.

1 Introduction

Bot networks proliferation and their evolution represent one of the most current alarming security threats for Internet users and also for Internet Service Providers (ISP). Differently from other types of malware, a bot is designed to infect a host and connect it back to an entity called botmaster, using a specific Command-and-Control (C&C) infrastructure. In such way the compromised hosts periodically receive binary updates and attack instructions. The greatest danger is represented by the minds behind those bot networks and the ability through which they can control their infrastructures by preserving their anonymity.

During the last years, we have assisted to a shift of the objectives that motivate the malicious activities of cybercriminals. They are not in search of notoriety but rather they are increasingly focusing on attaining financial gains. This shift is characterized by a new generation of cybercriminals. They don't act individually, but to ensure a stable business model, they began to create sophisticated organizations with different players whose relationship and co-operation is based on a trading system. On one hand there are the suppliers of services, ranging from the malicious code writers to the developers of exploit packets. On the other hand there are the consumers of these services ranging from spammers to cybercriminals that use extortion or the stolen data to

make profits. Within this business system, botnets represent the element of interaction between the service suppliers and the concerning consumers.

The reason is simple. Botnets make possible to the cybercriminals to gain high profits at low costs, if compared to the involved risks. They represent a malicious infrastructure able to provide flexible resources usable to exploit new types of vulnerability and new malware techniques. By relying on the use of malware armies, the botnet owners become the preferred purchasers of malware services, not only to propagate the infections on new hosts and to retrieve new resources but also to perform criminal activities. This increased demand of malicious code has led to an evident and rapid malware evolution regarding the techniques used to avoid antivirus detection and removal and to hinder analysis of malicious code. The use of packing, stealthing, polymorphism and metamorphism are only some examples. For the botnet owners the cooperation with the supplier of malware services gives some economic benefits. Botnet operators can now rely upon the quality of the malicious code that reduces the risks involved in its use. This is very important because the profits of the botnet owners are entirely reliant on the availability, stability and integrity of the botnet infrastructure. Financial gains are achieved by the sell of an entire botnet or by the temporary rent of a group of compromised hosts to third parties, usually used for sending out spam messages or for performing denial of service attacks against a remote target. There is a fast-growing online cybercrime market based on this model of 'botnet-as-a-service' that, just like legitimate commercial Internet service, offers helpdesk support, Service Level Agreement (SLA) and price list. Others services available, in addition to the rent of part of a botnet, include the sale of personal data stolen to the victims (e.g. credit card numbers) and the infection of target systems based on the "pay-per-install" model. The money received by botnet owners, for a successful compromised system, depends on the difficulties in infecting the system.

The evident damage and the potential bad effects of botnets make their detection essential to prevent further infections. Most of the internet users are characterized by low security protection level which allows an attacker to easily penetrate their computers. Internet users are generally not aware of potential risks their malware infected computers are exposed to, such as phishing, online fraud, theft of personal data (like personal credentials for online banking account, credit cards numbers, personal identification data and so on). They can also become an unaware source of spam or a component of online crime network. Most of the time, the actions and measures that the users take to address a machine infection are useful, but have proven to be insufficient to reduce the overall problem. This has shifted the attention to the role that an Internet Service Providers (ISPs) can have as control points for botnet activity.

ISPs, while providing IP connectivity and other services to their Internet customers, are in a privileged position to detect malware infection and propagation in their networks. It is important that the first step toward prevention would be made at the network/ISP level rather than relying only on individual users to keep their machines clean by bot. The benefits are not only related to the Internet users, which would be better protected if their ISPs play a security role, but also for the same ISP.

The presence of a large number of infected hosts is a big problem for an ISP: the bots can be used to send very large volumes of spam, resulting in extra cost for the ISP and in a negative reputation of the IP address space used by the ISP. By causing ISP's mail servers and network links to get blacklisted, bots reduce the quality of service the ISP can provide to its subscribers. For the ISP is then a big benefit to reduce the size of bonets and to mitigate their effects.

The Botnet is known to be an internationally distributed problem which requires a mutual co-operation between all the parties involved: security software vendors, registrars, legal and government entities and also ISPs. Some initiatives in this direction are raised. The Messaging Anti-Abuse Working Group (MAAWG), with the collaboration of the major Internet and email service providers, has issued the first best practices [MoO'09] for managing infected subscribers. Customers with infected computers are redirected to a protected environment, provided by the ISP, where they can download remediation tools to remove the malicious code. The Internet Engineering Task Force (IETF) has published a draft [LiMO09] with recommendations for ISP on the methods usable for alerting the customers whose systems have been compromised. Also the largest ISPs in Australia, under pressure from the government, are preparing a voluntary code, containing guidelines on how ISPs can identify suspicious activity, the contact ways they can use to alert the infected customers and mechanisms for filtering out their connection.

In the next chapter we will provide an overview of the botnet detection approaches currently known. Chapter 3 describes the botnet detection and prevention framework that Telecom Italia has defined with the intent to protect its users and to give them notification of potential security risks. Finally our contribution ends with a conclusion session.

2 Overview of the Botnet detection solutions

The research community is actively looking for effective methods against the botnet phenomenon; in fact the detection represents a complex challenge and some of the proposed solutions cannot sufficiently handle the problem.

Bots can use custom protocols as their communications channel; moreover they can employ encryption and packing mechanism to mask their payload and can use different network topologies to organize themselves. As a result, a number of botnet-specific detection approaches have been proposed. These systems can be applied either on network level or on host level.

Host-based solution can be useful on recognizing malware binaries and anomaly behavior related to system calls or to the creation of specific registry keys. Anyway most of them are signature based and may be ineffective: malware authors are using a vast array of tool and techniques to generate new variants of malware to easily evade their detection. Moreover bots may have the same privilege level of host-based detection systems; they can disable anti-virus tools or use techniques such as rootkits to protect themselves from detection at the local host. Finally, these solutions can involve a system performance overhead which is sometimes significant and not well accepted by the users.

Network-based detection systems that rely on signature have the same problem: they cannot detect new attacks without a proper signature which describes the new threat behavior. On the other hand, anomaly-based detection systems did not have this limitation. Most of these techniques focus on discovering the Command and Control (C&C) channels between botmaster and individual bots. Others approaches look only to specific aspect that characterize the bot infection, for example the detection of scanning activities to detect a local host infection. Because bot agents can infect a system using many different ways other than traditional remote exploitation, there is a risk to have lots of false positives and false negatives.

Smart Grid Security and Future Aspects

Security Challenges of a Changing Energy Landscape

Marek Jawurek · Martin Johns

Vincenz-Priessnitz-Straße 1, 76131 Karlsruhe, Germany SAP Research
{marek.jawurek | martin.johns}@sap.com

Abstract

The German electric energy industry is under change. The Smart Grid, Smart Metering and electric mobility are being researched and implemented. It will have implications for the security and privacy of our every-day-lives if security and privacy are not taken into account during this change. Therefore the identification and mitigation of security and privacy issues of prospective technologies is essential before respective systems are built. In this paper we identify the current legislative measures to induce change, derive the necessary technical changes and analyze them with respect to security and privacy challenges. We identify several security and privacy challenges: New paradigms like mobile energy consumers or bidirectional communication with electrical meters, isolated systems like Industrial Control Systems or Home Automation Networks that will eventually be connected to public networks and huge amounts of privacy-related data that will be created by respective systems. We conclude that the energy sector is an interesting field for security and privacy research and that now is the time to ensure a secure and private future of energy supply.

1 Motivation

In ten years, we drive electric cars with renewable energy. We are now at the point in time where we, as security researchers, need to ensure that this will happen in a secure and privacy-aware manner.

Due to legal and technological changes the electric energy industry is changing rapidly at this very moment to accommodate topics like volatile renewable generation, electric mobility on a wide scale or consumer load shifting while still maintaining stability, affordable electric energy and safety for our society. For the realization of these topics IT-systems will play a crucial role and their security will in turn play a crucial role for the safety of electrical grids. Security in IT-systems for the energy industry is a very interesting topic, as these systems will unlock certain markets for the energy industry that will have impact on our every-day-life and as currently many new technologies are explored in research projects. Different constraints make this endeavour challenging: legal constraints, safety, availability and real-time requirements, the heterogeneity of involved players and the variety of potentially malicious users and their attack vectors.

In this work we list the relevant legal changes for the German energy sector and derive resulting changes for its IT-systems. Based on these prognosed changes we identify emerging security challenges that need to be taken into account now in order to ensure a secure and privacy-aware transformation of the energy sector.

The rest of this paper is structured as follows: Firstly, we list several legislative impulses and their affect on the energy landscape with the help of three snapshots in Section 2. Secondly, in Section 3, we analyze the potential resulting changes in IT-systems. In Section 4 we depict which security challenges can be deducted from the aforementioned changes in IT-systems and give some specific new attack vectors. Finally, after reviewing related work (Section 5), in Section 6 we conclude with a summary.

2 The Energy Landscape under Change

The energy landscape has been under major change in Germany since 1999 although first ground-work was already laid as early as 1991. These changes are mainly driven by politics which in turn realize standards set by the European union and its road map for the energy sector [EUCCO6]. The following is an incomplete list of legal changes that have been mayor drivers for the change of the energy sector:

L1: Liberalization of energy markets: The goal of liberalization was to enable energy consumers to introduce competition into the energy sector and thereby foster efficiency and economic viability. What was previously considered a natural monopoly was divided into pieces where the only natural monopoly, the transport of energy, was subjected to regulation. Vertically organized corporations that owned the whole value-chain from production over transport to sales had to unbundle their operations to correspond to roles that the legislation created. See [Krisp07] for a detailed analysis of legal change.

L2: Support for the decentralized generation of renewable energy: Since 1991 several financial and legal measures were introduced by the legislative to support the decentralized production of renewable electrical energy. The implemented measures have led to an increased amount of decentrally produced renewable energy [BMUE10].

L3: Further liberalization of meter operations: In 2008 a law introduced two new roles for the area of meter installation, operation and meter reading: The metering point operator is responsible for installation, operation and maintenance of the meter while the measurement services provider is responsible for reading the data off the meter and transferring it to respective authorized receivers [GeLe08].

L4: Introduction of Smart Meters: Houses that are newly-connected to the electrical grid or that have been renovated since 2010 must be equipped with a special meter (§21b of [GeLe05]). Although, remote-reading is not mentioned as a requirement in the law, metering point operators want to upgrade directly to full Smart Meters with remote-reading capability (advanced metering).

L5: Free choice of metering point operator: According to §21b (2) of [GeLe05] house-owners have the choice of metering point operator. The metering point operator has to use a meter that fulfils the legal requirements and the technical requirements of the local grid operator.

L6: Tariffs to encourage energy saving: From end of 2010 energy suppliers must offer at least one tariff that supports the saving of energy. This might either be a load-dependent or a time-dependent tariff (§ 40 (3) of [GeLe05]). This might support L4 in the wide-scale distribution of Smart Meters as load/time-dependent metering requires this hardware.

Biometrics and Technical Solutions

Visa Applications in TG Biometrics for Public Sector Applications

Dr. Sibylle Hick¹ · Fares Rahmun² · Ernest Hammerschmidt³

^{1,3}secunet Security Networks AG, Kronprinzenstrasse 30, 45128 Essen
{sibylle.hick | ernest.hammerschmidt}@secunet.com

²Bundesverwaltungsamt, 50735 Köln
fares.rahmun@bva.bund.de

Abstract

The application, issuance and usage of modern electronic identity documents that are connected to biometric data is only possible after a complex process of requirements and regulations has been carried out together with the establishment of a respective infrastructure. Although different governmental eID documents are connected to various requirements, the structure and approach of the *modus operandi* is quite similar. Therefore, synergistic effects can be used to represent the processes connected to these documents.

In Germany, the Federal Office for Information Security has published a Technical Guideline “Biometrics for Public Sector Applications” that encloses requirements, recommendations, and best practices to design processes for the handling of the afore described documents within the context of biometrics. Not only electronic documents but also different applications have to be considered. As a result, a number of Application Profiles have been provided covering these circumstances. The description is based on experiences that were gained in several projects: e.g. the introduction of electronic passports in 2005, the preparation of new electronic national identity cards in Germany, and the experiences gained in the European BioDEV II pilot project for Visa which has been carried out to prepare the central European Visa Information System.

1 Introduction

Introducing new identity documents connected to biometric data, such as e.g. electronic passports (ePassports) in Europe, the new German national identity card, and furthermore visa and electronic residence permits, is a comprehensive and challenging task. Several perspectives as well as a great number of requirements have to be considered on an organisational, technical, and legal level. Agreements have to be made with the target groups; involved processes and the underlying infrastructure have to be adjusted.

In order to develop a common theme and satisfy all different requirements the German Federal Office for Information Security (BSI) has published a number of technical guidelines. For issues concerning biometrics the technical guideline “Technical Guideline TR-03121 Biometrics for Public Sector Applications” [TR_03121] (TG Biometrics) has been developed and published together with a Conformance Test Specification [TR_03122] each consisting of three parts. These documents combine the requirements and recommendations that are relevant for a specific target

group in a modular and structured way. After a short overview of the overall process and further general details the respective party can easily obtain the relevant information.

In this contribution the objectives within the scope of application for a biometric visa are described in section 2 against the background of the technical guideline TG Biometrics [TR_03121]. Afterwards the structure and approach of this guideline are part of section 3. In order to promote reusability, investment security, flexibility, and interoperability a software architecture had to be designed that is able to support all of the afore listed requirements. Therefore, a detailed overview regarding a flexible software architecture is given in section 4. A deeper insight in the approach can be achieved by looking at an example that shows how requirements of the relevant public sector applications are included for biometric visa. This is done in section 5 where experiences from the European pilot project BioDEV II have been taken into account. Finally, a conclusion is given in the last section.

2 Objectives

The association of biometric data with electronic identity documents faces several challenges. A very important part is the acquisition of biometric features within enrolment in order to achieve a uniform and adequate quality of data. It is a precondition in order to apply biometrics in different public sector applications e.g. identification and/or verification in border control scenarios. While ePassports in Europe and the German national identity card store the biometric features in the electronic identity document itself, the visa data including the bio-metric data is stored within a central Visa Information System (VIS) which is operated together with a Biometric Matching System (BMS). Besides quality issues, time needed for the acquisition of fingerprints of an applicant is also an important factor, in particular when it comes to optimised and user friendly processes. Quality and time constraints are in general opposed factors that have to be considered when requirements and recommendations shall be expressed.

Furthermore, addressing the different kinds of involved target groups, such as vendors of hardware and software components, public authorities as well as agencies and integrators is crucial, because the functions and perspective have to be distinguished in such a way that it is obvious to the entities what is relevant to them.

In order to apply an uniform approach the underlying software architecture shall build a solid framework that allows to integrate different kinds of identity documents and public sector applications dealing with biometrics at the same time. Interfaces shall be specified that allow a high flexibility, interoperability, and protection of investment. Thereby, well established international and national standards shall be taken into account. As a consequence, certification procedures and conformity testing can be established for hardware and software components.

3 Overview of the TG Biometrics

As described before, requirements regarding the documents in combination with public sector applications need to be described in a structured but at the same time modular and independent way because different kinds of hardware and software components are used for each specific context. Additionally, organisations and vendors may only be interested in a defined set of requirements regarding their application environment.

eID and the new German Identity Card

The New German ID Card

Marian Margraf

Federal Ministry of the Interior
marian.margraf@bmi.bund.de

Abstract

Besides their use in identity verification at police and border controls, national ID cards are frequently used for commercial applications, too. One objective of the introduction of the new national ID card on 1 November 2010 is to extend the conventional use of ID documents to the digital world. In order to meet this objective, the new ID card offers two electronic functionalities for e-business and e-government service providers: an electronic authentication and a digital signature.

In the following paper we describe the electronic authentication mechanism used by the ID card, explain the differences between authentication and signature and discuss the security and privacy properties of the two applications used for e-government and e-business.

1 Introduction

On 1 November 2010 Germany will start issuing new identity cards. One of the main differences compared to the previous version is the integration of an ISO-14443-compliant chip which contains a government application, e.g. for border control purposes, and two applications for e-government and e-business (authentication and signature).

IT security and privacy considerations played a crucial role during the design phase of the electronic functionalities. Reliable protection for personal information required a coordinated approach to legal provisions, organisational measures and technical implementation.

The legislative framework for the (current) national ID card (*Personalausweisgesetz*) already contains various provisions about the use of the national ID card, including restrictions. Thus, only in exceptional cases it is permitted to make a paper copy of the ID document; the serial number of the ID card must not be used for data mining purposes; and the machine-readable zone (MRZ) and the data in it must only be used for government purposes.

These provisions were transferred into the legal framework for the new, electronic national ID card. However, because of the new electronic functionalities, additional security mechanisms have to be specified and implemented. Therefore, the following requirements were taken into account during the design phase of the chip functionalities:

1. all data transmissions must be encrypted;
2. all transmissions of data have to be approved by the cardholder;
3. an illicit use of the ID card by a third party must be impossible;
4. the cardholder must know to whom their personal data will be transmitted;

5. only personal data that are necessary and approved by the cardholder may be transmitted;
6. the usage of the card cannot be monitored by government institutions or other parties;
7. the ID card must enable pseudonymous authentication;
8. lost ID cards must be revocable;
9. unique identifiers must not be used, neither for the citizen nor for the ID card.

The last three requirements, in particular, require a careful design of the revocation management for lost ID cards which is described in [1].

For an overview of the security mechanisms of the German ID card, please refer to [2]. In [6] you will find an overview of the privacy features and data protection mechanisms of European eID cards.

2 Commercial applications

Besides their use in identity verification at police and border controls, national ID cards are frequently used for commercial applications. In all these scenarios, the cardholder identifies him- or herself, using the ID card (and the biometric information on it), to the business partner or government officer, thereby proving a claimed identity.

In normal situations, the cardholder knows the person to whom he or she proves identity because this takes place either on the premises of the commercial partner or the government, or both persons involved show each other their ID cards. This is usually the basis of the trust between the two persons and/or whether they are acting on behalf of the institution(s) they represent.

In a technical sense, a *mutual* authentication takes place. However, both parties receive just a 'snap shot' of the authentication, and they cannot prove the other person's identity to a third party. A signature, which can, if necessary, be presented to a court or in administrative proceedings, constitutes such a proof.

The objective of the introduction of the new national ID card on 1 November 2010 is to extend the conventional use of ID documents to the digital world. In order to meet this objective, the new ID card offers two electronic functionalities for e-business and e-government service providers:

1. electronic authentication: which enables mutual authentication of two parties via the Internet in such a way that each party knows the person with whom it is communicating;
2. qualified digital signature (Qualifizierte Elektronische Signatur (QES)): which is a digital equivalent to a legally binding, hand-written signature according to the German Digital Signature Act (Signaturgesetz).

The cardholder has full control over the use of both functionalities: the ability of the card to perform an electronic authentication will be enabled or disabled when the citizen receives the card (and can be changed later), and a digital signature requires the prior loading of a (qualified) certificate onto the card.