Helmut Reimer
Norbert Pohlmann
Wolfgang Schneider *Eds.*

ISSE 2015

Highlights of the Information Security Solutions Europe 2015 Conference

EEMA
ISSE
INFORMATION SECURITY SOLUTIONS EUROPE
TeleTrusT
Pioneers in IT security.
Springer Vieweg

ISSE 2015

Helmut Reimer · Norbert Pohlmann ·
Wolfgang Schneider
Editors

ISSE 2015

Highlights of the Information Security Solutions Europe 2015 Conference

Springer Vieweg

Editors

Helmut Reimer
Bundesverband IT-Sicherheit e.V.
TeleTrusT
Erfurt, Germany

Norbert Pohlmann
Westfälische Hochschule
Gelsenkirchen, Germany

Wolfgang Schneider
Fraunhofer SIT
Darmstadt, Germany

ISBN 978-3-658-10933-2
ISBN 978-3-658-10934-9 (eBook)
DOI 10.1007/978-3-658-10934-9

Library of Congress Control Number: 2015951350

Springer Vieweg

Typesetting: Oliver Reimer, Großschwabhausen

Printed on acid-free paper

Springer Fachmedien Wiesbaden GmbH is part of Springer Science+Business Media
(www.springer.com)

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 range of topics has changed enormously since the founding of ISSE. In addition to our ongoing focus on securing IT applications and designing secure business processes, protecting against attacks on networks and their infrastructures is currently of vital importance. The ubiquity of social networks has also changed the role of users in a fundamental way: requiring increased awareness and competence to actively support systems security. ISSE offers a perfect platform 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 twelfth ISSE book – another mark of the event's success – and with about 22 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** (TeleTrusT/Sirrix AG)
- **John Colley** ((ISC)²)
- **Jos Dumortier** (time.lex)
- **Walter Fumy** (Bundesdruckerei)
- **David Goodman** (EEMA)
- **Michael Hartmann** (SAP)
- **Marc Kleff** (NetApp)
- **Jaap Kuipers** (Id Network)
- **Patrick Michaelis** (AC – The Auditing Company)
- **Lennart Oly** (ENX)

- **Norbert Pohlmann** (TeleTrusT/if(is))
- **Bart Preneel** (KU Leuven)
- **Helmut Reimer** (TeleTrusT)
- **Wolfgang Schneider** (Fraunhofer Institute SIT)
- **Marc Sel** (PwC)
- **Jon Shamah** (EEMA/EJ Consultants)
- **Franky Thrasher** (Electrabel)
- **Erik R. van Zuuren** (TrustCore)
- **Claire Vishik** (Intel)

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. With this book TeleTrusT aims to continue documenting the many valuable contributions to ISSE.

Norbert Pohlmann *Helmut Reimer* *Wolfgang Schneider*

TeleTrusT – IT Security Association Germany

TeleTrusT is a widespread competence network for IT security comprising members from industry, administration, research as well as national and international partner organizations with similar objectives. With a broad range of members and partner organizations TeleTrusT embodies the largest competence network for IT security in Germany and Europe. TeleTrusT provides interdisciplinary fora for IT security experts and facilitates information exchange between vendors, users and authorities. TeleTrusT comments on technical, political and legal issues related to IT security and is organizer of events and conferences. TeleTrusT is a non-profit association, whose objective is to promote information security professionalism, raising awareness and best practices in all domains of information security. TeleTrusT is carrier of the "European Bridge CA" (EBCA; PKI network of trust), the quality seal "IT Security made in Germany" and runs the IT expert certification programs "TeleTrusT Information Security Professional" (T.I.S.P.) and "TeleTrusT Engineer for System Security" (T.E.S.S.). TeleTrusT is a member of the European Telecommunications Standards Institute (ETSI). The association is headquartered in Berlin, Germany.

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 again being organized in collaboration with TeleTrusT's partner organisation eema and supported by the European Commission.

Contact:

TeleTrusT – IT Security Association Germany
Dr. Holger Muehlbauer
Managing Director
Chausseestrasse 17, 10115 Berlin, GERMANY
Tel.: +49 30 4005 4306, Fax: +49 30 4005 4311
http://www.teletrust.de

EEMA

EEMA is a non-profit membership association registered in Brussels. For over 25 years, from the dawn of the digital age, EEMA has helped European companies gain a competitive advantage and make informed technology choices and business decisions. Today it is the place where professionals gather to meet, network and define best practice in the areas of identity management and cybersecurity. EEMA's member representatives are drawn from leading corporate and multi-national end-user organisations, service providers, consultancies, academia, as well as local, national and European governmental agencies

In addition to a regular online newsletter and other information dissemination activities, EEMA benefits its members through conferences, thought leadership seminars and workshops, often in collaboration with partners such as ENISA, OECD, BCS, TDL, LSEC, TeleTrusT, ECP, Chamber of Commerce, CEN/ETSI, Digital Policy, ITU, Alliance, e-Forum, FAIB, FEDICT, IDESG, ISC2, United Nations, Oasis, SANS, SECEUR, GSMA, OIX and the Kantara Initiative. Recent EEMA events include 'Digital Enterprise Europe - Managing Identity for the Future' in London, 'Trust in the Digital World' in Vienna (in partnership with Trust in Digital Life) as well as special interest group meetings on 'Evolution & Future of eSignature & eSeal' and 'Cybersecurity – State of Play' in Brussels.

With its European partners, EEMA also participates in several high profile EU-sponsored projects including STORK 2.0 (Large scale pilot for e-ID interoperability between governments), SSEDIC (Scoping the single European digital identity community), Cloud for Europe (Public sector pre-commercial procurement in the Cloud) and FutureID (Shaping the future of electronic identity).

Visit www.eema.org or contact EEMA directly on +44 1386 793028 or info@eema.org

The EDPS Strategy – Leading by Example

Giovanni Buttarelli · Wojciech Wiewiórowski · Christopher Docksey

Rue Wiertz/Wiertzstraat 60
B-1047 Bruxelles/Brussel, Belgique/België
edps@edps.europa.eu

Abstract

The European Data Protection Supervisor (EDPS) is the independent supervisory authority monitoring the processing of personal data by the EU institutions and bodies, advising on policies and legislation that affect privacy and cooperating with similar authorities to ensure consistent data protection.

The current Supervisor, Giovanni Buttarelli, and Assistant Supervisor, Wojciech Wiewiórowski, were appointed in December 2014 by the European Parliament and the Council of the EU.

At a crucial moment for data protection, the EDPS has presented a strategy for 2015-2019 which identifies the major data protection and privacy challenges over the coming years, defines three strategic objectives and 10 accompanying actions for meeting those challenges and ways to deliver the strategy, through effective resource management, clear communication and evaluation of performance.

His three strategic objectives and 10 actions are:

1 **Data protection goes digital**

(1) Promoting technologies to enhance privacy and data protection;

(2) Identifying cross-disciplinary policy solutions;

(3) Increasing transparency, user control and accountability in big data processing.

2 **Forging global partnerships**

(4) Developing an ethical dimension to data protection;

(5) Speaking with a single EU voice in the international arena;

(6) Mainstreaming data protection into international policies.

3 **Opening a new chapter for EU data protection**

(7) Adopting and implementing up-to-date data protection rules;

(8) Increasing accountability of EU bodies collecting, using and storing personal information;

(9) Facilitating responsible and informed policymaking;

(10) Promoting a mature conversation on security and privacy.

As a first milestone in implementing his strategy, the EDPS adopted in July 2015 an opinion on the state of the data protection reform, setting out red lines and providing his advice for the on-going legislative negotiations. Building on discussions with the EU institutions, Member States, civil society, industry and other stakeholders, it addresses the GDPR in two parts:

- the EDPS vision for future-oriented rules on data protection, with illustrative examples of recommendations; and
- an annex with a four-column table for comparing, article-by-article, the text of the GDPR as adopted respectively by Commission, Parliament and Council, alongside the EDPS recommendation.

H. Reimer, N. Pohlmann, W. Schneider (Eds.), *ISSE 2015*, DOI 10.1007/978-3-658-10934-9_1

1 Introduction

This is truly a historic moment for data protection.

Over the last 25 years, technology has transformed our lives in positive ways nobody could have imagined. Big data, the internet of things, cloud computing, have so much to offer to enhance our lives. But these benefits should not be at the expense of the fundamental rights of individuals and their dignity in the digital society of the future. So big data will need equally big data protection.

The EU has a window of opportunity to adopt the future-oriented standards that we need, standards that are inspiring at global level.Europe has to lead the conversation on the legal and ethical consequences of the new technologies. This means adopting the data protection reform this year. A modern, future-oriented set of rules is key to solving Europe's digital challenge. We need EU rules which are innovative and robust enough to cope with the growing challenges of new technologies and trans-border data flows. Data protection must go digital.

Data protection will remain a relevant factor in most EU policy areas, and is the key to legitimise policies and increase trust and confidence in them. The EDPS will help the EU institutions and bodies to be fully accountable as legislators, to build data protection into the fabric of their legislative proposals.

To develop a single European voice on strategic data protection issues, the EDPS will cooperate with fellow independent data protection authorities.

2 Data Protection in the Digital Era

Digital technology is an extraordinary catalyst for all forms of social expression and social change. From amusing videos and games to revolutions powered by social media, technology can enable the powerless to challenge the powerful. There is no doubt that technology brings many benefits, both individual and social.

Data protection regulators need to identify the opportunities in terms of prosperity, well-being and significant benefits, particularly for important public interests.

On the other hand, the widespread collection and use of massive amounts of personal data today -made possible through cloud computing, big data analytics and electronic mass surveillance techniques- is unprecedented.

The digital environment is determining:

- how people communicate, consume and contribute to social and political life in the post big data world;
- how businesses organise themselves to make profits;
- how governments interpret their duty to pursue public interests and protect individuals;

and

- how engineers design and develop new technologies.

Encrypted Communication

The Public Key Muddle – How to Manage Transparent End-to-end Encryption in Organizations

Gunnar Jacobson

Secardeo GmbH
gunnar.jacobson@secardeo.com

Abstract

We discuss the business requirements and available solutions for end-to-end encryption in the application areas of electronic mail, instant messaging, file exchange and voice over IP. We will show that many applications today rather fulfil the security requirements of a private user than those of an organization. Our special focus is on the provided key management schemes that often do not satisfy the business needs. Combining encryption products from different vendors can then lead to a public key muddle. For key management a universal X.509 based PKI meets today's business requirements best. We show how the consistent distribution of certificates and private keys to encryption applications on all user devices can be done. This will help to consolidate and automate key management processes leading to reduced operational security costs and high user satisfaction.

1 Introduction

1.1 Public Key Cryptography

Public key cryptography is available for almost forty years, now. Bob can publish his public key so anybody can use it to send him encrypted messages and only Bob may decrypt them using his private key. The promised scenario is that a user can exchange end-to-end encrypted messages with anybody in the world, reliably and without any efforts – from any device of that user. This scenario, however, has not become a reality, yet. What are the reasons?

Besides the ongoing academic discussions about cryptographic properties of asymmetric and symmetric ciphers or hash functions on one side and political interests and leverage on the other side there are two main practical issues that still defer the breakthrough of global end-to-end encryption:

1. The diversity of data formats and protocols using public key cryptography (encryption mechanisms)
2. The variety of trust models and distribution, retrieval and validation methods for public and private keys (key management)

H. Reimer, N. Pohlmann, W. Schneider (Eds.), *ISSE 2015*, DOI 10.1007/978-3-658-10934-9_3

Two major public key encryption standards are being used since their publication in the early 1990s: Pretty Good Privacy (PGP) and Secure Multipurpose Internet Mail Extensions (S/MIME) together with the X.509 framework [CDF+07] [RaTu10] [ITU12]. These standards are rather incompatible with respect to data formats and trust models and limitations of both have been shown up in the past. Many organizations have invested huge efforts in the establishment of X.509 PKIs while PGP is popular for academic and private users. There have been other messaging encryption standards before like X.400 and Privacy Enhanced Mail (PEM), but they did not succeed. On the other hand we see a number of new concepts in the fields of encryption for electronic mail, instant messaging or cloud based file exchange. Most of them are proprietary with new data formats, protocols and key management models and their major features and the consequences of using them are often not well understood.

In the following we will discuss the requirements for end-to-end encryption and its key management from a business perspective and we will show mechanisms and services that will satisfy the needs.

1.2 Business requirements for end-to-end encryption

Two years after Snowden's exposures many IT managers have accepted, that encryption is the only way to prevent from data interception by powerful attackers like intelligence agencies or professional industrial spies. They are also aware of the fact, that meanwhile the attackers place their tools inside the corporate network and that therefore end-to-end encryption of data becomes more and more mission critical. End-to-end encryption (E2EE) means, that a message is encrypted at its source and it cannot be decrypted until it reaches its final destination where it will be decrypted [Shir07]. Solid encryption is also a frequent requirement from compliance regulations like HIPAA, PCI-DSS, SOX or national data privacy laws.

What are the preconditions for a high level of distribution of E2EE?

- Encryption must be legally permissible and must not be bypassed by governmental backdoors.
- Encryption should be done completely transparent to the user.
- The efforts for a public key system should be as low as possible.

So, what are the typical business applications that require end-to-end encryption? In the following the major communication applications are listed:

1. Electronic Mail (e-mail)
2. Instant Messaging (IM)
3. File Exchange
4. Voice over IP (VoIP)

In the following we will discuss these applications, the relevant standards and popular products.

Cloud Security

On Location-determined Cloud Management for Legally Compliant Outsourcing

Bernhard Doll[1] · Dirk Emmerich[2] · Ralph Herkenhöner[2] · Ramona Kühn[1] · Hermann de Meer[1]

[1]University of Passau
Innstraße 43, 94032 Passau
{dollbern | kuehnram | demeer}@fim.uni-passau.de

[2]Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Str. 8, 80807 München
{dirk.emmerich | ralph.herkenhoener}@ts.fujitsu.com

Abstract

When organisations are outsourcing their data processing to clouds, the cloud providers have to support them in achieving legal compliance. This is particular challenging in globally distributed clouds where the data centres are located in multiple countries with different legislation. Here, the cloud providers have to implement technical constraints based on the legal requirements which apply individually for each cloud customer. In this paper, the legal requirements of cloud customers and their corresponding technical constraints are modelled in a technically decidable and enforceable manner, using information flow control in virtual resource management, and a solution to implement the support of legal requirements in cloud environments is proposed. The solution proposed covers the translation of legal requirements of cloud customers into technical security policies which are applied in virtual resource management of clouds. For these purposes an information model, denoted as the *Cloud Security Matrix*, is defined using the methods of information flow control. In the model, cloud resources (virtual and hardware) are classified and the allowed information flows are defined. The information model is capable to express both location and security constraints including authenticity, integrity and availability. The technical feasibility of a location-based assignment of virtual resources is shown in a proof-of-concept implementation based on OpenStack.

1 Introduction

Legally compliant data processing is one of the key requirements when the outsourcing of data processing to a cloud is considered. Although the cloud customers are responsible for legally compliant processing of their data, the cloud providers (external service providers running the cloud environment) have to provide the technical measures to fulfil all constraints requested by the customers. Particularly challenging are globally distributed clouds where the data centres are located in multiple countries. The key to legally compliant cloud computing is to understand the legal requirements which are applicable to cloud customers and how cloud providers have to implement and operate cloud environments.

H. Reimer, N. Pohlmann, W. Schneider (Eds.), *ISSE 2015*, DOI 10.1007/978-3-658-10934-9_6

Industry 4.0 and Internet of Things

Industry 4.0 – Challenges in Anti-Counterfeiting

Christian Thiel[1] · Christoph Thiel[2]

[1]FHS University of Applied Sciences St. Gallen,
christian.thiel@fhsg.ch

[2]University of Applied Sciences Bielefeld
christoph.thiel@fh-bielefeld.de

Abstract

As part of the evolution of industrial production and automation processes referred to as industry 4.0, new developments in information technologies such as the Internet of Things and cloud computing grow together with real (physical) objects and classic industrial processes. In production processes following the Industry 4.0 approach large amounts of data are generated from RFID's, sensors, embedded systems, the components itself to be manufactured, the machines, but also of the management and control functions of computer units. They contain information about the production process, place, time and condition of the product to be produced, even on the design documents and used materials and parts. By an unauthorized derivation of these information (in the simplest case by just observing the production facilities), the entire production process and the properties of the material produced can be disclosed. This simplifies the work of pirates and calls for new approaches to protect against counterfeiting and know-how loss.

In our work we identify new requirements on Industry 4.0 processes and production facilities. These requirements comprise both the protection of the whole production process and the usability and cost effectiveness from the different viewpoints of all stakeholders down the supply chain. We match these requirements with existing protective measures and close existing gaps. For that we develop new protocols and propose adaptations of existing processes and components.

1 Introduction

Counterfeiting and piracy have a strong impact on businesses and the global economy, jeopardizing investments in creativity and innovation, undermining recognized brands and creating consumer health and safety risks ([VDMA13]). Counterfeiters are producing fake foods and beverages, pharmaceuticals, electronics, auto parts and everyday household products. By 2015, the International Chamber of Commerce ICC expects the value of counterfeit goods globally to exceed $1.7 trillion. That's over 2% of the world's total current economic output ([ICC11]).

This problem has grown hand-in-hand with globalization of the economy. Along with trade liberalization, the growth of sophisticated logistics networks and information sharing through data networks and the Internet has dramatically increased the volume of products and information moving around the world. The value chains have become increasingly global and longer both geographically and in the number of value chain links, i.e. players in the value chain like raw

H. Reimer, N. Pohlmann, W. Schneider (Eds.), *ISSE 2015*, DOI 10.1007/978-3-658-10934-9_10

materials and component suppliers, transport operators, and landlords and property or infrastructure owners. Consequently, these trends have also created significant challenges for rights holders in detecting, investigating and stopping the flow of counterfeited and pirated materials. In particular, it is much more difficult for rights holders to know, manage, and control every player (chain link) involved in their value chains and to see their every transaction. Players of a value chain face similar challenges with their sub-players, e.g. suppliers and customers (cf. [CGM+12]).

This situation has exposed a number of value chain vulnerabilities, and criminal agents have seized the opportunity to exploit them (cf. [ICC11]). As a result of this, reliance threats to value chains have attracted more attention, including the threat of intentional tampering during development, distribution or operations, or the threat of substitution with counterfeit (including cloned or overproduced) components before or during delivery.

To make things even worse traditional industrial processes and modern technologies of information technology have started to grow together. An ongoing industrial revolution referred to as the fourth industrial revolution, or short 'Industry 4.0' initiates the conglomerating of the horizontal integration of inter-corporation value networks, the end-to-end integration of value chains, and the vertical integration of factory inside (which is called smart factory). While still in the beginning it is obvious that Industry 4.0 will lead to new challenges in fighting against counterfeits.

It would be difficult in a single paper to cover all facets of counterfeiting and product piracy. Here we will not discuss the different kinds of potential damages nor give detailed technical descriptions of the possible approaches of counterfeiters. Thus the emphasis of this paper is to illustrate the impact of Industry 4.0 on counterfeiting and product piracy by discussing new challenges in comparison with the pre Industry 4.0 era and describing showcase threats and possible countermeasures.

2 Counterfeiting in the pre Industry 4.0 era

One of the most interesting questions in the context of counterfeiting and product piracy is, where counterfeiters and product pirates do get the know-how to counterfeit or copy products as they do, i.e. the know-how about the products and the necessary production processes. In general the counterfeiter or pirate is applying one or more of the following five approaches to get and use this kind of information:

- Reverse engineering: The product itself contains a lot of information. One way to imitate a product is therefore reverse engineering. The more technologically sophisticated the products are and the more difficult product features can be understood by disassembly, all the more challenging is reverse engineering. For example hard to understand manufacturing processes (such as in heat treatment processes) could hinder the successful product creation. Or an original product could not be disassembled without simultaneous destruction.
- Industrial espionage: Illegal direct attacks on know-how or information through industrial espionage (hacking, corruption of insiders, etc.)
- Loss of know-how: The right holder or company loses know-how via former personnel, clients, or suppliers.
- Competitive Intelligence: Outflow of corporate knowledge that is not protectable by industrial property rights. Offender try systematically to obtain information about objec-

tives, strengths and weaknesses, tactics, risks and opportunities, products and services, sales channels and sales success as well as new developments, pending property rights and technologies of the companies which should be copied.
- Overbuilding: That means the foundry or system integrator in charge of manufacturing the devices produces more of them than originally specified by the designer.

According to [VDMA] most right holders point to reverse engineering as a means of gaining know-how. Forty-two percent of companies believe that imitating the products needed no specific information. Frequently, counterfeiters copy protected brands or designs (color, form etc.). The third most common source of information (at 31 percent) lies in the loss of know-how, e.g. via former personnel, clients, or suppliers

Measures which may take the right holder or Original Equipment Manufacturer (OEM) to prevent the copyist / pirate of his projects are grouped under the term reduction of imitation attractiveness ([Neem07]). This includes all measures that seek to ensure that the potential pirate no longer wants to imitate resp. clone the product of the original provider, e.g. technical or organizational concepts making the reproduction to expensive, to complex or even impossible. When the potential pirate has decided to imitate resp. clone, he will – additionally to the information gathered so far – try to acquire the necessary know-how of the innovator. This includes both the product know-how and the necessary process know-how. Measures of the innovator who are trying to hinder this process, are listed under the term aggravation of know-how acquisition. This includes all measures that obstruct the pirate in his intention to acquire the necessary know-how about the products and the necessary production processes.

Following the successful know-how acquisition the pirate has all the theoretical knowledge necessary for the manufacture of the product and will try to reproduce the product with his own resources. Measures that try to limit this are referred to as measures to aggravation of reproduction.

After a successful reproduction the pirate will begin with the marketing of the produced imitations. Also in this phase, the Innovator has opportunities to hinder the offender in his activities. Measures of this kind will be treated under the term aggravation of marketing.

There are some process approaches that have been created for the purpose of deriving concepts to protect against product piracy ([VDMS13], [Meiw11]). These guidelines offer solutions in the form of a structured procedural model, designed to reveal the requirements and possible protective means for relevant key areas of businesses.

Among the technical solutions are marking technologies to differentiate the plagiarism from the original, or constructive protection technologies making the reproduction of devices, machines and control systems more difficult and therefore preventing possible attacks by pirates. Therefore most concepts focus on (cf. [VDMA13]):
- Product identification: Identification technologies comprise visible and invisible security features aimed at proving product originality and authenticity. Examples include holograms, data matrix codes, RFIDs, special printing methods, or added materials.
- Detection and authentication of protected products: This refers to devices, equipment and systems able to recognize, read, check and verify the originality of security features.
- Tracking and tracing systems: Systems to track and trace products through the supply chain and the entire lifecycle with unique security markers.

Cybersecurity and Cybercrime

Making Sense of Future Cybersecurity Technologies: Using Ontologies for Multidisciplinary Domain Analysis

Claire Vishik[1] · Marcello Balduccini[2]

[1]Intel Corporation
claire.vishik@intel.com

[2]Drexel University
marcello.balduccini@drexel.edu

Abstract

Security experts have difficulties achieving quick vulnerability mitigation because cybersecurity is a complex multi-disciplinary subject that yields itself with great difficulty to traditional methods of risk analysis. In particular, the effectiveness of mitigation strategies depends on an accurate understanding of the relationships among the components of systems that need to be protected, their functional requirements, and of the trade-off between security protection and core functionality. Mitigation strategies may have undesired ripple-effects, such as unexpectedly modifying functions that other system components rely upon. If some of the side-effects of a mitigation strategy are not clearly understood by a security expert, the consequences may be costly. Thus, vulnerability mitigation requires a deep understanding of the subtle interdependencies that exist between domains that are different in nature. This is especially difficult for new technology use models, such as Cloud-based computing and IoT, in which cyber and physical components are combined and interdependent. By their own design, ontologies and the associated inference mechanisms permit us to reason about connections between diverse domains and contexts that are pertinent for the general threat picture, and to highlight the effects and ramifications of the mitigation strategies considered. In this paper, we position ontologies as crucial tools for understanding the threat space for new technology space, for increasing security experts' situational awareness, and, ultimately, as decision-support tools for rapid development of mitigation strategies. We follow with the discussion of the new information and insights gleaned from the ontology-based study of the root of trust in cyber-physical systems.

1 Introduction

Modern processes and technologies are cross-domain, merging together approaches created for different contexts. Complexity is intrinsic. Even activities resulting in identical or similar outcomes – e.g., sending electronic mail, processing identical datasets or payments, using e-commerce applications, or assessing the data quality collected from sensors – could be executed in very different environments, resulting in different risks. Thus, it is sometimes necessary to assume different risk postures in response to similar events or in the course of the same process.

H. Reimer, N. Pohlmann, W. Schneider (Eds.), *ISSE 2015*, DOI 10.1007/978-3-658-10934-9_12

Trust Services

A pan-European Framework on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market

Olivier Delos · Tine Debusschere · Marijke De Soete · Jos Dumortier · Riccardo Genghini · Hans Graux · Sylvie Lacroix · Gianluca Ramunno · Marc Sel · Patrick Van Eecke

DLA Piper, Avenue Louise 106, 1050 Brussels, Belgium
patrick.van.eecke@dlapiper.com

Abstract

This article is summarizing the results of the European study SMART 2012/0001 commissioned by the European Commission..

1 Introduction

1.1 Scope and objectives of the project

The objective of the project was to perform a study to support the implementation of a pan-European framework on electronic identification and trust services for electronic transactions in the internal market.

The Commission adopted on 4 June 2012 a proposal for a Regulation on "electronic identification and trust services for electronic transactions in the internal market". The proposal was adopted on 23 July 2014 by the European Parliament and Council as Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC[1] (hereinafter referred to as 'Regulation').

In parallel with the ordinary legislative procedure with a view to adopting the proposal, there was a need to:

1. Start working on the analysis of the elements that would help develop secondary legislation (delegated and implementing acts) envisaged in the proposal for a Regulation;

1 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN)

H. Reimer, N. Pohlmann, W. Schneider (Eds.), *ISSE 2015*, DOI 10.1007/978-3-658-10934-9_15

Authentication and eID

Architectural Elements of a Multidimensional Authentication

Libor Neumann

ANECT a.s., Vídeňská 125, 619 00 Brno, Czech Republic
Libor.Neumann@anect.com

Abstract

Today's ICT environment is significantly different from the environment, where the currently used eID architectures were developed. Mobile devices (such as tablets or phones) are available for anyone today. These devices use advanced application management systems, leading communication mediums and ever-growing range of peripherals.

Attackers have ever-increasing incentives as the assets on the Internet, and specifically in "the cloud", grow in value with the overall growth and development of the Internet. They employ a higher computation force, more sophisticated methods and unique tools. Moreover, these attackers often operate from countries, where the violation of cybercrime laws holds little or no penalty. There is also the increasing risk of a cyber-war.

The paper describes selected elements of a new eID architecture and the experience from their practical implementation. The eID architecture is based on published Distributed Identity Infrastructure (DII) concept, which is remarkable for its fully automated life cycle of electronic identities, user-friendly experience and easy integration to ICT systems.

The presentation deals with two main ideas:

- Replacing the static protection of an electronic identity with a dynamic protection
- Complex protection of the cyber/electronic identity in its whole life cycle (including emergency situations) and the protection of the communication channel itself.

1 Introduction

In recent years, important events took place in the area of ICT, especially in the field of eID. Here are some of them:

- The progress of ICT and the Internet in particular has reached a state, in which the possibilities of the most widely used method of authentication, loginname/password, were definitively exhausted. The reason is that the requirements imposed on a user in real life exceeded human capabilities. This is one of the reasons for significant increase in number of successful cyber attacks.
- There is an apparent shift from understanding eID from authentication alone to an eID ecosystem, it means to the knowledge that the attacker always uses the weakest element of the whole ecosystem. Therefore new methods how to evaluate the quality of the eID ecosystem, such as AAL or QAA, were created [WiBu11, HuLE09].
- There have been successful attacks on manufacturers specializing in security hardware via the Internet or their own internal ICT systems [HuLE09, Zett15].

H. Reimer, N. Pohlmann, W. Schneider (Eds.), *ISSE 2015*, DOI 10.1007/978-3-658-10934-9_19

Regulation and Policies

Information Security Standards in Critical Infrastructure Protection

Alessandro Guarino

StudioAG
a.guarino@studioag.eu

Abstract

The standards applicable to Information Security are legion, from the purely technical, low-level specification of crypto protocols to the high-level organisational management frameworks. Industrial Control Systems - among them the Information Systems in Critical Infrastructure - still present their own set of challenges and quirks, despite the convergence trend towards mainstream information technologies and networking. Among these challenges we can recognise the still widespread use of legacy and proprietary systems with a long life and often poor documentation, the geographical spread, the fact that ICSs control physical equipment with all the related consequences (safety risk, difficulty of testing), the lack of IT and especially security training among the personnel, the legal and regulatory environment. The paper analyses the application of standards in Critical Infrastructure Information Protection, both from an organisational and technical perspective, their choice, their implementation and economic cost and benefits, in the context of the existing legal landscape, in particular in the European Union context. A brief theoretical excursus will examine a cost-benefit model for policymakers called to formulate the best policy in mandating - or not - the use of standards.

1 Introduction

Industrial plants, factories and infrastructures – be they "critical" or not – have become today heavily dependent on Information and Communications technologies for their control and operations. This holds true even for traditional sectors like for instance freshwater delivery or railway transportation. ICTs used in this applications can be labeled in general as Industrial Control Systems (ICSs) and are quite different in many ways than office networks and mobile appliances.

While ICSs are widely used in many context, we are concerned here in particular with their use in operating infrastructures and even more specifically, "critical" infrastructures. According to the common definition infrastructures constitute the basic framework needed for a society to function properly. It goes without saying that modern, developed countries need more than a basic road network and freshwater wells to function, all the way up to airports and air traffic control, oil and gas distribution, smart power grids, wide-area information networks – of which the Internet is the ultimate example. Among infrastructures, "Critical Infrastructures" are informally defined as those systems the failure of which could seriously impair the lives of the citizens or the national security of a country. While the exact list varies by country, even inside the EU, some are unanimously considered critical: the power grid, energy supply, transport systems, water supply. In European legislation Critical Infrastructure are defined as follows:

H. Reimer, N. Pohlmann, W. Schneider (Eds.), *ISSE 2015*, DOI 10.1007/978-3-658-10934-9_22

> *[...]an asset , system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.*

Standards and best practices are one of the means used to elevate information security levels and their implementation is more and more mandated, in various ways by governmental policies. Policies however can assume many different forms and they are not always chosen by rational means. The tools provided by economics can help policymaker to make rational choices; economics applied to the formerly purely technological field of information security has already helped better understand many phenomenons and behaviours.

2 Available Standards

The world of standardisation is very fragmented and complex. As a broad overview standards can be categorised along two variables: technical level and the presence of certification schemes. In the information security field specifications of cryptographic algorithms are examples of technical standards and risk assessment schemes are examples of organisational standards. Some organisational schemes are certifiable, meaning that a third party independently assesses the organisation and declares that the it is in compliance with the standard requirements: ISO/IEC 27001 is an example of such a standards. A standard for which a certification scheme is not establishes is commonly referred to as a "guideline", but this is not at all a usage accepted by everyone and many non-certifiable guidelines as termed standards as well.

Among the standard developing organisations ("SDOs") the most relevant in the European context are the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunications Standards Institute (ETSI). These are also officially recognised by the European Commissions and can legally be the recipient of standardisation requests. Their area of competence can overlap – information security and cyber security being a case in point – but their constituency and operations are quite different. While CEN-CENELEC membership is composed of national standardisation bodies part of the ISO system, ETSI membership is mainly industry-based, while also including academic institutions and national administrations. All operate by trying to reach a consensus among members. The ETSI process and products tend to be more technically-oriented, market driven and faster. In the cyber security field however, ETSI is a comparative newcomer, having formed a dedicated group in 2014. A Cyber Security Coordination Group [CSCG13], fathered by all three European SDOs, has been established to help reduce overlaps and duplication of efforts.

The American effort in cyber security standardisation has been comparatively more directly driven by the government, in the wider context of national security. Executive branch involvement in Critical Infrastructure Protection began with the Presidential Decision Directive 63 (PDD-63) in 1998, later superceded by HSPD-7 in 2003 [DHS03]. The standardisation bodies most relevant to CI protection are the National Institute of Standards and Technology (NIST) and The North American Electric Reliability Corporation (NERC).

In the next section we'll review the standards most relevant to cyber security and critical infrastructure information protection, with a bias toward the organisational frameworks.