Helmut Reimer
Norbert Pohlmann
Wolfgang Schneider *Eds.*

ISSE 2014 Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe 2014 Conference

eema
www.eema.org

ISSE
INFORMATION SECURITY SOLUTIONS EUROPE

TeleTrusT
Pioneers in IT security.

Springer Vieweg

ISSE 2014 Securing Electronic Business Processes

Helmut Reimer • Norbert Pohlmann
Wolfgang Schneider (Eds.)

ISSE 2014 Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe 2014 Conference

Springer Vieweg

Editors

Helmut Reimer
TeleTrusT – IT Security Association
Berlin, Germany

Wolfgang Schneider
Fraunhofer Institute SIT
Darmstadt, Germany

Norbert Pohlmann
Institute for Internet Security
Westfälische Hochschule
Gelsenkirchen, Germany

ISBN 978-3-658-06707-6
DOI 10.1007/978-3-658-06708-3

ISBN 978-3-658-06708-3 (eBook)

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

Library of Congress Control Number: 2014952087

Springer Vieweg

Typesetting: Oliver Reimer, Großschwabhausen

Printed on acid-free paper

Springer Vieweg is a brand of Springer DE.
Springer DE is part of Springer Science+Business Media.
www.springer-vieweg.de

Contents

About this Book xi

SAFECode Whitepaper: Fundamental Practices for Secure Software Development 2nd Edition 1
Editor: Stacy Simpson

Security Management, CISO Inside 33

In-House Standardization of Security Measures: Necessity, Benefits and Real-world Obstructions 35
Eberhard von Faber

An Effective Approach for Assessing the Risk of Acquired IT Products 49
Eric Baize · Steve Lipner

IT-Security in Railway Signalling Systems 56
Christian Schlehuber · Erik Tews · Stefan Katzenbeisser

13+ Real Ways to Destroy Business by Breaking Company's SAP Applications 65
Alexander Polyakov

Trust Services, eID and Cloud Security 79

Achieving the eIDAS Vision Through the Mobile, Social and Cloud Triad 81
Francisco Jordan · Helena Pujol · David Ruana

Security Versus Usability – User-Friendly Qualified Signatures Based on German ID Cards 94
Gregor Bühler · Enrico Entschew · Marcel Selhorst

Using the Semantic Web to Generate Trust Indicators 106
Marc Sel

Cybersecurity, Cybercrime, Critical Infrastructures

Cybersecurity, Cybercrime, Critical Infrastructures 121

Hidden and Uncontrolled – On the Emergence of Network Steganographic Threats 123
Steffen Wendzel · Wojciech Mazurczyk · Luca Caviglione · Michael Meier

Restricting Excessive State-on-State Cyber Espionage under International Law: A Quest of Futility? 134
Murdoch Watney

Securing Cloud: Elastic Key Management and Homomorphic Encryption 144
Alexander W. Koehler

Secure Communication and Digital Sovereignty in Europe 155
Norbert Pohlmann · Michael Sparenberg · Illya Siromaschenko · Kilian Kilden

The need of European White Knights for the TLS/SSL Certificate System 170
Arno Fiedler · Christoph Thiel

BYOD and Mobile Security 175

Emerging Technologies, Disrupt or be Disrupted 177
Steven Ackx

Hardware Intrinsic Security to Protect Value in the Mobile Market 188
Vincent van der Leest · Roel Maes · Geert-Jan Schrijen · Pim Tuyls

On Cross-Border Mobile Government Systems 199
Milan Marković · Goran Đorđević

Privacy, Data Protection, Human Factors 209

Privacy for Cloud Storage 211
Anders Andersen · Trygve Hardersen · Norbert Schirmer

Enforcing Data Privacy in the Age of Google Glass 220
Christian Thiel · Christoph Thiel

Internet of Trucks and Digital Tachograph – Security and Privacy Threats 230
Marc Sel · Dusko Karaklajic

Regulation & Policies 239

Towards eIDAS as a Service 241
Detlef Hühnlein

What now? Data Retention Scenarios After the ECJ Ruling 249
Alessandro Guarino

From Research Results to Strategy: A Mapping Exercise. 256
Michele Bezzi · Frances Cleary · Luca Compagna

Index 265

About this Book

The Information Security Solutions Europe Conference (ISSE) has been 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 eleventh ISSE book – another mark of the event's success – and with 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)
- **Marijke De Soete** (Security4Biz)
- **Jos Dumortier** (KU Leuven)
- **Walter Fumy** (Bundesdruckerei)
- **David Goodman** (EEMA)
- **Michael Hartmann** (SAP)
- **Marc Kleff** (Unify)
- **Jaap Kuipers** (Id Network)
- **Patrick Michaelis** (AC – The Auditing Company)
- **Lennart Oly** (ENX)

- **Norbert Pohlmann** (TeleTrusT/Institute for Internet Security – 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** (Deloitte)
- **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 – 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

SAFECode Whitepaper: Fundamental Practices for Secure Software Development 2nd Edition

(Extract – for the full paper see *www.safecode.org*)

Editor: Stacy Simpson

Authors:

Mark Belk, Juniper Networks
Matt Coles, EMC Corporation
Cassio Goldschmidt, Symantec Corp.
Michael Howard, Microsoft Corp.
Kyle Randolph, Adobe Systems Inc.
Mikko Saario, Nokia
Reeny Sondhi, EMC Corporation
Izar Tarandach, EMC Corporation
Antti Vähä-Sipilä, Nokia
Yonko Yonchev, SAP AG

info@safecode.org

Introduction

A review of the secure software development processes used by SAFECode members reveals that there are corresponding security practices for each activity in the software development lifecycle that can improve software security and are applicable across diverse environments. The examination of these vendor practices reinforces the assertion that software security must be addressed throughout the software development lifecycle to be effective and not treated as a one-time event or single box on a checklist. Moreover, these security methods are currently in practice among SAFECode members, a testament to their ability to be integrated and adapted into real-world development environments.

The practices defined in this document are as diverse as the SAFECode membership, spanning cloud-based and online services, shrink-wrapped and database applications, as well as operating systems, mobile devices and embedded systems. This extract from the Whitepaper contains its main chapters in full.

- Secure design principles,
- Secure coding practices,
- Testing recommendations and
- Technology recommendations

To aid others within the software industry in adopting and using these software assurance best practices effectively, this paper describes each identified security practice across the software development lifecycle and offers implementation advice based on the experiences of SAFECode members.

H. Reimer et al. (eds.), *ISSE 2014 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-06708-3_1, © Springer Fachmedien Wiesbaden 2014

1 Secure Design Principles

1.1 Threat Modeling

The most common secure software design practice used across SAFECode members is Threat Modeling, a design-time conceptual exercise where a system's dataflow is analyzed to find security vulnerabilities and identify ways they may be exploited. Threat Modeling is sometimes referred to as "Threat Analysis" or "Risk Analysis."

Proactively understanding and identifying threats and potential vulnerabilities early in the development process helps mitigate potential design issues that are usually not found using other techniques, such as code reviews and static source analysis. In essence, Threat Modeling identifies issues before code is written—so they can be avoided altogether or mitigated as early as possible in the software development lifecycle. Threat Modeling can also uncover insecure business logic or workflow that cannot be identified by other means.

Rather than hope for an analysis tool to find potential security vulnerabilities after code is implemented, it's more efficient for software development teams to identify potential product vulnerability points at design time. This approach enables them to put in place defenses covering all possible input paths and institute coding standards to help to control the risk right from the beginning. It is worth noting that an analysis tool lacks knowledge of the operating environment in which the system being analyzed executes.

By their nature, systemic architectural issues are more costly to fix at a later stage of development. Thus, Threat Modeling can be considered a cost-efficient, security-oriented activity, because fixing issues early in the process may be as easy as changing an architecture diagram to illustrate a change to a solution yet to be coded. In contrast, addressing similar issues after coding has begun could take months of re-engineering effort if they are identified after code was committed, or even a major release or a patch release if an issue was identified even later by customers in the field.

Leveraging the full benefits of Threat Modeling when designing systems can be challenging as software designers and architects strive to identify all possible issues and mitigate them before moving forward. This can be difficult to achieve, so the focus must be on the high-risk issues that can be identified at design time. In addition, Threat Modeling results should be continuously updated as design decisions change and added threats may become relevant, and threats may be mitigated during development or by virtue of documentation or clearly visible use case limitations.

Threat Modeling can be done at any time in the system's lifecycle, but to maximize effectiveness the process should be performed as early in the development process as possible. Distinct software development methodologies will have different points where system design may change: in a traditional "waterfall" development model, Threat Modeling would be performed when the design is relatively well established but has not yet been finalized, and in the Agile model, the activity could occur during initial design or be a recurring activity during each iteration or sprint—when the design is most likely to undergo change.

Security Management, CISO Inside

In-House Standardization of Security Measures: Necessity, Benefits and Real-world Obstructions

Eberhard von Faber [1(+2)]

[1] T-Systems
Eberhard.Faber@t-systems.com

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

Abstract

The business demands cost reduction, flexible sourcing and customary quality when it comes to getting IT services. Internal and external IT service providers must therefore industrialize their IT production. Industrialization in turn requires standardization of all components in modern IT production. This includes standardizing the security measures that are used to protect the IT service provisioning. Areas and elements are identified that can be standardized. Needs and benefits are described for each. Additionally, this study focuses on real-world obstacles which need to be considered and surmounted in order to secure IT services in an efficient and flexible way. Practical advice is provided to support the standardization of security measures used in-house to protect IT services.

1 Understanding Standardization

First of all it is required to analyze the origin of standardization and the motivation to use standards in general. The term "in-house standardization" is explained. The topic of this paper is further narrowed down by briefly discussing the possible nature of the standards. In the second part of this chapter the term "standard" is defined which is needed in order to discuss benefits later.

1.1 In-house motivation

Many people associate with a standard that they must use it or adhere to it. This understanding leads into the wrong direction. Standards, as being the subject of this paper, are not a "must" – they are not a "law". It is the nature of standards to provide benefits to whom who is using it. As a result, it is simply disadvantageous to ignore the standard. These disadvantages may cause an enterprise to enforce the use of standards and to punish people who are not using them. However, the sequence of causes is important here:

- Standards (as described in this paper) primarily provide benefits such as competitive advantages that should motivate to use them.[1]

[1] The obstacles to get these benefits are discussed later.

H. Reimer et al. (eds.), *ISSE 2014 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-06708-3_2, © Springer Fachmedien Wiesbaden 2014

Trust Services, eID and Cloud Security

Achieving the eIDAS Vision Through the Mobile, Social and Cloud Triad

Francisco Jordan · Helena Pujol · David Ruana

World Trade Center Barcelona, S4, Barcelona, Spain
Safelayer Secure Communications S.A.
{jordan | helena.pujol | david.ruana}@safelayer.com

Abstract

The new EU regulation on electronic identification and trust services for electronic transactions in internal market aims to overcome cross-border barriers regarding identity and signature services. According to the Head of the European Commission DG CONNECT Task Force "Legislation Team", the eIDAS regulation sets out to "strengthen EU single market by boosting TRUST and CONVENIENCE in secure and seamless cross-border electronic transactions".

Although the proposed regulation is technology-neutral, we believe that the technology used by the Mobile, Social and Cloud triad can greatly boost the deployment of applications and, therefore, may accelerate the achievement of the eIDAS vision. Mobile devices have become the something-you-have authentication factor that has been generally delegated to hardware tokens. Smartphones allow deploying highly-secure yet user-friendly mechanisms that can complement existing national eIDs and overcome user-experience drawbacks. Furthermore, identity services are not solely useful for backing up identities provisioned and managed by Member States but can also enhance services by federating and elevating trust on social and other consumer identities. Finally, light Web formats and modern user-centric and privacy-aware standards like OAuth and OpenID Connect make it easy for developers to combine identities and functionality and may revolutionize the quantity and quality of applications, owing both to the plethora of access devices and the advantages of Cloud computing delivery.

1 Background

Since before 1999, when the EU Directive on Electronic Signatures [EU99] was released, an effort has been made to establish and regulate a technology and legal framework that enables, in EU member states in particular but also globally, secure and trustworthy electronic interactions. Today, 15 years later, we can say with all honesty that the aim pursued by the Directive has not been achieved. We have a universal telephone communication system, a universal Internet access system, etc., but we lack a universal system of identification, authentication and eSignature.

Following various consultative processes, numerous workgroups and accumulated experience, in April 2014, the European Parliament's new regulation on eIDAS [EU14] was passed that updates the old eSignature Directive. It will come into effect on July 1, 2016, automatically repealing the old Directive.

H. Reimer et al. (eds.), *ISSE 2014 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-06708-3_6, © Springer Fachmedien Wiesbaden 2014

Cybersecurity, Cybercrime, Critical Infrastructures

Hidden and Uncontrolled – On the Emergence of Network Steganographic Threats

Steffen Wendzel[1] · Wojciech Mazurczyk[2] ·
Luca Caviglione[3] · Michael Meier[1]

[1] Cyber Defense Research Group, Fraunhofer FKIE, Bonn, Germany
{steffen.wendzel | michael.meier}@fkie.fraunhofer.de

[2] Institute of Telecomm., Warsaw University of Technology, Warsaw, Poland
wmazurcz@elka.pw.edu.pl

[3] Institute of Intelligent Systems for Automation (ISSIA),
National Research Council of Italy (CNR), Genoa, Italy
luca.caviglione@ge.issia.cnr.it

Abstract

Network steganography is the art of hiding secret information within innocent network transmissions. Recent findings indicate that novel malware is increasingly using network steganography. Similarly, other malicious activities can profit from network steganography, such as data leakage or the exchange of pedophile data. This paper provides an introduction to network steganography and highlights its potential application for harmful purposes. We discuss the issues related to countering network steganography in practice and provide an outlook on further research directions and problems.

1 Introduction

Steganography is known to be a technology used since thousands of years; its purpose is to embed a secret message into an innocent looking carrier. Digital media steganography embeds secret data into digital structures, including digital videos, digital audio files, and digital image files. Within recent years, a novel part of steganography arose, namely *network steganography*. Network steganography transfers secret data over a network by hiding secret information into legitimately appearing transmissions [LuWS10].

In comparison to cryptography, steganography aims at hiding the existence of a secret message while cryptography aims on hiding the content of a message. Both technologies cryptography and steganography are orthogonal and can be combined, i.e. a secret message can be encrypted and afterwards it can be hidden using steganography.

H. Reimer et al. (eds.), *ISSE 2014 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-06708-3_9, © Springer Fachmedien Wiesbaden 2014

BYOD and Mobile Security

Emerging Technologies, Disrupt or be Disrupted

Steven Ackx

PwC, Woluwegarden – Woluwedal 18 B – 1932 BRUSSELS
steven.ackx@be.pwc.com

Abstract

Emerging technologies are transforming and will transform the way we do business almost at the speed of light. When talking about emerging technologies we are looking at Social, Mobile, Analytics and Cloud, but also Internet of Things (IoT), New Way Of Working (NWOW), wearables, drones, advanced analytics, etc. These emerging technologies are not just IT challenges but are business imperatives. Emerging technology innovation is coming from all angles – it's easy to become overloaded with the rapid pace of technological change. Digital developments are one of the main drivers of change, reshaping customer expectations, making products, services and prices easier to compare and opening up the market to a new breed of data-rich entrants and start-ups.

Most businesses are in markets where the depth of customer-centricity is the key differentiator, digital also opens up sharper ways to engage customers, understand their needs and provide customised solutions. In short, effective emerging technologies are now a disruptor and should become a competitive advantage. There are so many opportunities – each with its own costs, risks and complications – that it is difficult to cut through the noise and find the best way forward.

Because of these challenges, organizations often find themselves with two options:

- Invest in an unproven strategy which could result in a significant loss in time, money and opening new security threats.
- Wait for proven concepts in the market and potentially lose market share to innovative competitors.

This paper is about what's happening and will be happening (emerging trends and technologies). How to respond as an organisation in a controllable and secure manner, without the risk of being too late in a highly competitive world.

Case: What will be the impact of the Internet of Things (IoT) on security and privacy?

1 Emerging technologies / trends

When looking at emerging technologies we see a lot of evolutions and trends that could/will have an impact of the way you are doing business and the risks your business is facing. Here you will find a flavour of some emerging technologies PwC identified as having a possible impact on the way you are doing business; this is not a limitative list.

1. **SMAC** – Today, there are four key drivers affecting the constantly evolving social economy: Social, Mobile, Analytics, and Cloud (SMAC). Social features like chats, wikis, rich media, and community work spaces changes who individuals work with, crossing functional, hierarchical and organizational boundaries. Mobile applications provide a new

H. Reimer et al. (eds.), *ISSE 2014 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-06708-3_14, © Springer Fachmedien Wiesbaden 2014

way to work and access information – from anywhere and at any time. Analytics provide companies a way to understand analyse enormous amounts of data collected in order to understand work. Finally, cloud computing, like mobile, affects where individuals work and how they access their information and be productive.

2. **Wearables** – A smartphone-based wearable – either worn as a band, part of your clothing or embedded in your body – that can read temperature, pulse rate, heart rate, blood oxygenation, etc. This data is transmitted to the cloud where it can be analysed for anomalies, accessed by your personal doctor, and aggregated with similar data from millions of others Wearable or embedded sensor that transmits data via Bluetooth to a smartphone-based app. The app stores, reports, and notifies based on information shared with the cloud.
3. **Sensors** – Using an array of in-store sensors ("beacons") to micro-locate the position of a participating customer, retailers can track interest in specific products and services, provide notifications about events and promotions, and enable contactless payments.
   a. Apple iOS and Android devices with Bluetooth 4.0 Low Energy (BLE); Location-based Services.
   b. Retailers: Can offer more specific, targeted information to customers, which aids sales and customer service; Obtain hyper-local data regarding customer behaviour within a store.
   c. Customers: New levels of interaction and engagement with a brand; discounts and promotions more relevant to their interests; speedier payments and customer service.
4. **NWOW** – The world of work is changing within organizations. They are facing many different challenges as work-life balance, stress, homeworkers; bring your own device, traffic jams, expensive offices, labour shortage, commitment to organisation, etc. All these challenges make that we have to look at the way of working in a new way. As a business you have to continuously monitor what your workforce is expecting and how this will affect the way you do business.
5. **Internet of things** – The term "Internet of Things" was coined by Kevin Ashton, a British technology pioneer, to describe the attachment of micro machine readable devices to items to automate identification processes.
6. **Data analytics & Big Data** – We are generating massive volumes of data for analysis. Cisco estimates that 50 billion objects will be connected to the Internet by 20201 producing a massive volume and variety of data at unprecedented velocity.
   The Brontobyte (1027 bytes of information) is expected to be the measurement to describe the type of sensor data that will be generated from IoT devices.
   Big Data tools will be used to collect, store, analyse and distribute these large data sets to generate valuable insights, create new products and services, optimize scenarios and so on.

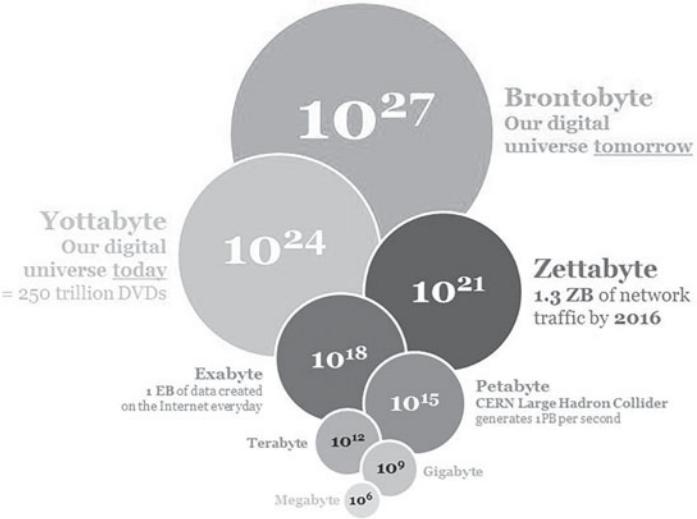

Fig 1: Big Data

7. **3D printing & 3D scanning** – 3D printing and scanning will have an impact on parts of our business, like stock management and very specific developments which could be create (printed) remotely.

2 Future trends

1. **Smart Cities** – especially with the further development of Internet of Things or Internet everywhere, cities will become more and more interconnected. Being more and more interconnected could lead to smart management of operating of cities; this could be in the area of utilities, transport, leisure, retail & consumer, etc.
2. **Dreams** – will we be able to analyse our dreams, being sensoning at night how we sleep?
3. **Cars** – the google car, will our cars be capable of driving independently and being taxed accordingly?

3 Challenges on business

1. Data analysis & decision making are the foundational areas which will impact traditional business models. The Internet of Things will disrupt physical industries with 6 key capability enhancements. The capabilities are divided into two groups; Sensor Generated Data – and Automation.

Privacy,
Data Protection,
Human Factors

Privacy for Cloud Storage

Anders Andersen[3] · Trygve Hardersen[1]
Norbert Schirmer[2]

[1]Invenia AS
P. Box 540, 9256 Tromsø, Norway
trygve.hardersen@invenia.no

[2] Sirrix AG
Im Stadtwald D3 2, D-66123 Saarbrücken, Germany
n.schirmer@sirrix.com

[3] UiT The Arctic University of Norway
9037 Tromsø, Norway
anders.andersen@uit.no

Abstract

Cloud Security Infrastructure (CSI) is a joint research project between Invenia AS and Encap AS of Norway, and Sirrix AG of Germany, where the goal is to come up with a scalable architecture that addresses the security and privacy concerns of cloud storage. In CSI we promote client side end-to-end encryption of all user data. No user data exists unprotected outside the client devices, and the encryption keys are not stored within the storage cloud. Hence there is no means for a cloud provider to access user data. In CSI we apply public key encryption and two-factor authentication to existing cloud storage solutions, providing a highly scalable and secure collaboration environment allowing secure sharing of data. This is integrated with enterprise wide directory services to provide key management within enterprises.

1 Introduction

Cloud storage technologies such as Dropbox and Google Drive are proving very popular with users because they provide convenient solutions to real life problems. Originally adopted by consumers, enterprises are now looking to utilize cloud storage in their daily business activities. But a few questions quickly come to mind:

- How secure are these solutions?
- How is information kept confidential in the cloud?
- How can confidential and scalable sharing be achieved?

It is good reason to be concerned of the security when using cloud storage. The privacy of user data has been compromised at the cloud storage services, the SSL transport is coming under increasing pressure, and simply relying on passwords for authentication is no longer sufficient. How can we still utilize the power of these services?

H. Reimer et al. (eds.), *ISSE 2014 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-06708-3_17, © Springer Fachmedien Wiesbaden 2014

Regulation & Policies

Towards eIDAS as a Service

Detlef Hühnlein

ecsec GmbH
Sudetenstraße 16, 96247 Michelau, Germany
detlef.huehnlein@ecsec.de

Abstract

Cloud computing promises to provide great advantages and many analysts expect a significant growth of the cloud services market. In a similar manner the forthcoming European regulation on electronic identification and trusted services for electronic transactions in the internal market [**eIDAS-EP**] is expected to ease electronic identification, authentication and signatures (eIDAS) in Europe. The present contribution discusses whether and how the two approaches can be combined in order to provide services for electronic identification and authentication of entities, the creation, verification, validation and preservation of electronic signatures and the registered delivery of documents in an efficient manner using cloud computing techniques.

1 Introduction

Cloud computing is deemed to save costs, boost efficiency, improve user-friendliness as well as security and accelerate innovation [**TC-Europe**]. Furthermore the market for cloud services is expected to grow significantly [**MaM14**]. In a similar manner the forthcoming European regulation on electronic identification and trusted services for electronic transactions in the internal market (eIDAS) is expected to boost user convenience, trust and confidence in the digital world (cf. [**eIDAS-PR**], [**COM(2012)238**]). Against this background it seems to be very rewarding to combine the two approaches and use trusted cloud techniques to provide services addressed by the forthcoming eIDAS-regulation. The present contribution discusses whether and how the different services addressed by the proposed regulation, which has recently been adopted by the European Parliament [**eIDAS-EP**], can be provided in a secure and trustworthy manner as cloud service.

The rest of the paper is structured as follows: Section 2 contains the necessary background on the eIDAS-regulation and trustworthy cloud computing. Section 3 focusses on the different services addressed by the proposed regulation and in particular discusses whether and how electronic identification and authentication, electronic signatures and registered delivery can be provided as trustworthy cloud service. Based on related work from respective research projects Section 3.1 will introduce a reference architecture for the cloud-based provision of eIDAS-services and Section 4 will finally summarize the main results and draw conclusions.

H. Reimer et al. (eds.), *ISSE 2014 Securing Electronic Business Processes,*
DOI 10.1007/978-3-658-06708-3_20, © Springer Fachmedien Wiesbaden 2014