Speaker Biographies and Paper Precis

Steven Ackx

Director | PwC Advisory Services | Belgium

Steven Ackx is a director at PwC Advisory Services with extensive experience in operational risk management, IT & information security and mobile/payments.

He has been involved in projects on a strategic, tactical and operational level, working on information security management/ governance, information risk management, privacy, program/project management, mobile (business, payments and banking), moving to digital (business, payments and banking), education and awareness.

Today he is leading the PwC offering on SMAC (Social, Mobile, Analytics and Cloud).

BYOD and Mobile Security *Emerging technologies, disrupt or be disrupted*

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. 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. This presentation 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.

Ammar Alkassar

Board Member/Chairman | TeleTrusT/Sirrix AG | Germany

Eric Baize

Senior Director, Product Security Office, EMC Corporation / SAFECode Board member | EMC Corporation / SAFECode | USA

Eric Baize leads EMC's Product Security Office with company-wide responsibility for product security and supply chain assurance, covering vulnerability response handling, security development lifecycle implementation, supply chain risk management, coordination of security certifications and integration of RSA technology in EMC products.

Previously, Mr. Baize pioneered EMC's push towards security. He was a founding member of the leadership team that drove the acquisition of RSA Security in 2006 and later led RSA's strategy for cloud and virtualization. Prior to joining EMC, Mr. Baize held various positions for Groupe Bull in Europe and in the US.

Follow Eric Baize on Twitter: @ericbaize

Security Management, CISO Inside *An effective approach for assessing the risk of acquired commercial IT products*

We are well aware that acquired IT products can introduce new software vulnerabilities into IT environments and customers frequently ask IT vendors how they can be confident in the security of the software they acquire. Current methods for assessing the security of acquired software are disparate and often ineffective. The presentation outlines three approaches for assessing the security of acquired software. The appropriate application of those approaches depends on the maturity of the IT vendor in relation to its secure software development process.

Abbie Barbir

Chair OASIS Trust Elevation Committee Canada

Abbie Barbir, Ph.D., is a VP, Senior Architect and is the Co-chair of OASIS Trust Elevation TC.
Dr. Barbir is involved in many activities within OASIS, ITU-T, Canadian Advisory Committee (CAC) JTC1 SC 38 and JTC1 IoT. Dr. Barbir chairs the Identity Management question in ITU-T SG17. In 2005, he represented OASIS to ITU-T and was instrumental in having the ITU-T consent the SAML and XACML OASIS Standards as ITU-T Recommendations.
Abbie holds a Ph.D. in Computer Engineering from Louisiana State University in Baton Rouge, USA. In his more than 20 years in the software and telecommunication industry, he has been a professor of Computer Science in Western Carolina University, an application developer, data compression and encryption inventor, systems architect, security architect, engineering manager, consultant, author, and inventor of numerous security algorithms.

Trust Services, eID and Cloud Security *End User Panel: Strong Authentication a Must for Mobility*

This Panel will discuss the results of OASIS Trust Elevation TC in its efforts to develop an interoperable standard for enabling step up authentication as a means of securing valuable transactions across devices. The panel will discuss the importance of interoperability and will provide status update on current efforts for integrating step up authentication with SAML, OpenID connect and FIDO.

Markus Bartsch

Business Development TÜViT GmbH Germany

Markus Bartsch studied computer science and has worked for TÜViT GmbH since 1995. Markus Bartsch is in charge of IT topics that affect new industrial technologies like Smart Grid, Automotive Security and Process Control Technologies. Actually he is part of the team that supports the German Ministry of Economics to specify a secure smart meter system. Even for this topic mobile solutions are going to be used.

BYOD and Mobile Security *IT security in mobile apps of smart devices – not only phones*

Enterprise mobility is currently one of the most important IT topics for companies.
The Application Security Center (ASC) is a service that meets all mobile security demands in one single system: The ASC approach gives companies, App developers and system houses the ability to manage their apps and their app infrastructures. This approach does not refer to smart phones only, it should also be used for future smart products and systems.
The presentation explains the approach of a management service like the ASC to improve the security level of mobile and smart devices.

André Beerten

CISO Hospital The Netherlands

André Beerten has worked in IT, Telecommunications & Information security since 1990 as an engineer, consultant, product manager & security officer. In the 3 hospitals he supports as a CISO implementing NEN7510:2011 (the Dutch translation of the ISO27799:2008) meeting a host of challenges.

Security Management, CISO Inside *The life & times of a CISO in healthcare*

In 3 hospitals I am supporting as a CISO implementing NEN7510:2011 (the Dutch translation of the ISO27799:2008) meeting a host of challenges. These challenges is what the presentation is going to be about: scoping, politics, priorities & culture..

Eric Bodden

Head of Secure Software Engineering | Fraunhofer SIT, TU Darmstadt and EC SPRIDE | Germany

I am heading the Secure Software Engineering Group at Fraunhofer SIT, Technische Universität Darmstadt and the European Center for Security and Privacy by Design (EC SPRIDE), as well as the Emmy Noether Group RUNSECURE funded through the DFG. Further I am a Principal Investigator of the Center for Advanced Security Research Darmstadt (CASED), within the research area “Secure Services”. At Fraunhofer SIT I am heading the Attract-Group on Secure Software Engineering. Here we develop code analysis technology for security, in collaboration with the leading national and international software development companies. In 2014, the DFG awarded me the Heinz Maier-Leibnitz-Preis. In 2013, BITKOM elected me into their mentoring program BITKOM Management Club.

I am one of the chief maintainers of the Soot program analysis and optimization framework, a contributor to the AspectBench Compiler, the open research compiler for AspectJ, the inventor of the Clara and TamiFlex frameworks. Together with my research group, I have created the FlowDroid analysis framework for Android and the DroidBench benchmark suite. Our blog gives more information about our current research.

Panel Session Secure Software *Secure software - we need it more than ever: SAFECODE and more*

Developing software with security built in from scratch is the most important contribution to securing the information society. The panellists are experts with lots of experience in secure software development from different organizations. They will discuss and share their experiences on how to develop software securely.

Jordan M. Bonagura

CIO | Hades Coding | Brazil

computer scientist, post graduated in Business Strategic Management, Innovation and Teaching (teaching methodology and research). Works as a teacher and course coordinator. Work too as information security consultant with emphasis to new breaches and its exploration forms. (CEH) Professor in the area of information technology in various institutions, founder of Vale Security Conference, Stay Safe Podcast and Magazine, SJC Hacker Space, member of High Crimes Technologies commission at OAB-SP, member of Cloud Security Alliance (Brazil).

Privacy, Data Protection, Human Factors *CSO Myopia*

Imagine what it would be like to manage your company without your customer’s data or if the data was in your competitors’ hands. The experiences your customers acquire along the years as well as their database are fundamental and represent a great competitive edge in this new corporate era. Keeping this in mind we realize the importance of implementing specific policies in order to build a base to guarantee the safety of these data, but I will show how the “limited” vision of some CSO's can impact on fool vulnerabilities making the company with serious security issues.

Markus Braendle

Group Head of Cyber Security | ABB | Switzerland

Markus Braendle is globally responsible for all aspects of cyber security for the ABB Group. Responsibilities include developing and leading a cross-divisional and cross-functional effort to ensure that ABB products and systems fully support customers' cyber security requirements, ensuring that ABB added-value services enable customers to remain secure, that ABB response to and management of cyber security-related inquiries and incidents will be efficiently and consistently coordinated across ABB,
and strategic collaborations and partnerships.

Cybersecurity, Cybercrime, Critical Infrastructures	*End User Session: Cybersecurity for industrial control systems: addressing a unique set of challenges*
Panel Session Critical Infrastructures	*Industrial control system security what are the issues at hand?*

Sarah Brown

Principal Cyber Security Expert | Fox-IT | The Netherlands

Sarah Brown works as a member of the Fox-IT InTELL team, providing threat intelligence to banks and retailers to keep them in control of hacking, malware, phishing and hybrid attacks. At Fox-IT, she works to the cutting edge information portal where InTELL customers are informed of cyber threats targeting them in real time. One of her key focus areas is cyber threat information sharing and use of STIX for structured threat sharing. From 2004-2013 she held cyber security positions with MITRE supporting the US Government, NATO, and other international partners. She was posted to the NATO Communications and Information Agency (NCIA) in The Hague, NL from 2008-2013.

Cybersecurity, Cybercrime, Critical Infrastructures	*Using criminal actor intelligence to predict cyber attacks*

Specifically looking at three actors : - Paunch - BlackHole; - Rescator - Target; - Slavik - P2P Zeus
These are all significant investigations involving global organisation including law enforcement, Fox worked on these over the past two years and all have become visible to the outside world over the past 12 months. Fox will share the inside information and a unique research which will provide context of how and what these Criminals organisations expedited in the following attacks. Including What lessons have been learned and what and how have these attack vectors evolved since they became public.

John Colley

Managing Director, EMEA | (ISC)² | UK

John Colley, CISSP, is Professional Head, EMEA and Co- Chair of the European Advisory Council for (ISC)2, a not-for-profit professional consortium which represents over 100,000 members worldwide, and 16,500 in EMEA. For the past seven years he has been the Managing Director for (ISC)2 EMEA.He served on the (ISC)2 Board of Directors for eight years including two as chairman. John has over twenty years experience in information security. He has formerly held posts as Head of Risk Services at Barclays Group, Group Head of Information Security at the Royal Bank of Scotland Group, Director of Information Security at Atomic Tangerine and as Head of Information Security at ICL. John has also worked as an independent consultant providing value added advice and guidance to blue chip organisations. He has had numerous articles published in the IT and security press. In 2012 he was inducted into the Infosecurity Hall of Fame.

Luca Compagna

Research Expert | SAP | France

Dr. Luca Compagna joined SAP in 2006. He is Research Expert at SAP Product Security Research, where he is contributing to the SAP research strategy and responsible for various internally- and externally-funded research projects. He received his MSc in Informatics Engineering from the University of Genova and his Ph.D. in Computer Science jointly from the University of Genova and Edinburgh. His area of interests include cyber-security, security engineering, automated reasoning, security testing, and their application to industrial relevant scenarios. He contributed to various projects on information security and he has published various scientific publications in his area of interest.

Regulation & Policies *From research results to strategy: a mapping exercise*

In 2013, the European Commission released the "Cybersecurity Strategy for the European Union" outlining the EU's vision for ensuring strong and effective protection in the digital world. At the same time, research in cybersecurity and trust is very active in Europe, and it is In fact, security research project panorama is very vast and diverse, making extremely challenging to derive a single and comprehensive view of the results. The research project community, facilitated by the CSP Forum project cluster activity of SecCord coordination action, decided to perform a research portfolio analysis', to evaluate how they can contribute to European strategy. The idea of this 'research portfolio analysis' is mapping the research results coming from security projects to the priorities of European cybersecurity strategy and analysing how projects can provide significant inputs.
www.cspforum.eu

Enrique Crespo

Professional Services Director | Safelayer Secure Communications S.A. | Spain

Panel Session eID *eID - new Strategies: EU-Regulation - the FIDO Example*

Jos Dumortier

ICT Lawyer | time.lex | Belgium

Enrico Entschew

Senior Business Developer | Bundesdruckerei GmbH | Germany

Since 1998 Enrico Entschew is professional in contact with the topic of qualified electronic signatures and is deemed to be an approved expert in this area. Since 2009 he works in several rolls for the German Federal Printing Agency (Bundesdruckerei). As a business developer he is part of the product management team and responsible for the solution to sign with the new German ID card ("sign-me") from the idea to the product.

Trust Services, eID and Cloud Security *Security versus usability – user-friendly qualified signatures based on German ID cards*

This talk will present the German ID cards along with their electronic applications. The pilot phase of the signature application will be introduced along with the valuable feedback received during the first year. Finally, a live demonstration will show the process of loading a qualified signature certificate to the ID card concluded by the actually online-signing of documents.

David Etue

VP, Corporate Development Strategy | SafeNet, Inc | USA

David Etue brings together experience and perspective from a number of security roles including security program leadership, management consulting, product management and technical implementation. He is the VP of corporate development strategy at SafeNet, where he is responsible for strategic decisions regarding partnerships, and mergers & acquisitions. He was previously the cyber security practice lead at management consultancy PRTM (now PwC), VP of Products & Markets at Fidelis Security Systems, led General Electric's global computer security program, and held various positions in technology strategy, operations and product management. He is a Certified Information Privacy Professional, a Certified CISO, a graduate of GEís Information Management Leadership Program, and a Six Sigma Green Belt.

Security Management, CISO Inside *Whose cloud is it anyway? Exploring data security, ownership and control*

Arno Fiedler

CEO | Nimbus | Germany

1983 High school diploma from Humboldt-Gymnasium Wilhelmshave, 1983-1985 Education in Navy electronics; NCO with leadership responsibilities destroyer „Schleswig-Holstein“, 1989 diploma as industrial engineer (Diplom-Wirtschaftsingenieur) at FH Wilhelmshaven., 1989-1995 Marketing-, Sales- and Project Manager Bull AG (Compagnie des Machines Bull) , 1995 to 1999 Division Manager „Sales and Marketing Electronic Media Services“ at German Federal Printing Agency (Bundesdruckerei GmbH), In 2000 founder of Nimbus Technologieberatung GmbH with emphasis on creating and implementing market access strategies in reference to Public-Key Infrastructure, IT-Security and biometric devices. , Since 08/2010 certified ISO 27001 Lead Auditor [BSI; IRCA], From 01/2011 until now active in ETSI “Electronic Signature and Infrastructures (ESI) „Specialist Task Forces” within EU Mandate/460, Active participation in the following fora: „Sichere Identität Berlin-Brandenburg“ (vice-chairman), TeleTrusT, ETSI/ESI, CA/Browser-Forum etc..

Panel Session eID *eID - new Strategies: EU-Regulation - the FIDO Example*

Cybersecurity, Cybercrime, Critical Infrastructures *The need of European white knights for the TLS/SSL certificate system*

There are many reasons to be concerned about internet security: For example, we have to worry that formerly trusted security solutions are manipulated by (friendly or hostile) government institutions. We have to discover that classical local security concepts have limits in a globally networked world, and we have to learn that in many (if not most) cases cryptographic protocols are implemented in a poor or wrong way.
Since a strong and secure SSL/TSL ecosystem is still held as an important building block of a secure internet, there are numerous efforts to overcome the security concerns stated above. These new approaches include supporting the development of secure (reference) implementations as well as the expansion of the SSL/TSL ecosystems by Certificate Transparency, Certificate Authority Authorization, or Certificate Pinning, and many more. Not surprisingly, these approaches are mainly driven by companies or organisations with a strong U.S. background.
In this presentation, we will discuss these approaches from a European perspective. We derive that from a European perspective, these approaches will only restore trust in the SSL/TSL ecosystem, if on the one hand, they are covered by the European standardization efforts and on the other hand major European companies or organisations without U.S. background will explicitly construct and operate corresponding solutions.

Cyril Gollain

CEO | BRAINWAVE | France

Privacy, Data Protection, Human Factors

Vendor Session: A smarter way to access rights recertification: how to reduce the risk AND make your users love you

David Goodman

Director | EEMA | UK

Alessandro Guarino

CEO | StudioAG | Italy

Alessandro Guarino is an experienced information security professional and independent researcher. He is CEO of StudioAG, a consulting firm based in Italy whose services were used by the industry and the public sector. He holds a MS in Industrial Engineering and a BS in economics, with a focus on Information Security Economics. He is an ISO active expert in JTC 1/SC 27 (IT Security techniques commitee) and contributed in particular to the development of cybersecurity and digital investigation standards. He represents Italy in the CEN-CENELEC-ETSI Cybersecurity Coordination Group and the ETSI TC CYBER. See more on www.studioag.pro / en

Regulation & Policies

What now? Data retention scenarios after the ECJ ruling

Early this year the European Court of Justice declared the 2006 EU Data Retention Directive invalid. The ruling represents a very important turning point in the ongoing tug-of-war between privacy and security concerns. The presentation examines the reasons for the directive annulment and the consequences of the repealing at various levels and for different actors: policymakers, businesses, service providers, investigators. Also it brings forward some proposals on what can be done to correctly rebalance security and investigation necessities with fundamental liberties.

Trygve S. Hardersen

VP of product management & MOB | Invenia AS | Norway

Trygve S. Hardersen is VP prduct management & MOB at Invenia AS. He has 6 years experience developing cloud storage services. Bsc computer science & business administration CBS.

Privacy, Data Protection, Human Factors

Privacy for cloud storage

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.

Michael Hartmann

Security Expert | SAP | Germany

Gerold Hübner

Chief Product Security Officer (CPSO) | SAP | Germany

Gerold Huebner, Chief Product Security Officer (CPSO) at SAP AG , owns SAP's Product Security Strategy and is the legal advisor for assuring right data protection functionalities in SAP applications. Mr. Huebner authoritatively drives Security Development Lifecycle Processes at SAP across all development units. In his role as CPSO he is the guiding Chief Expert on all product security topics including SAP's internal Product Standard for Security, Static Code Analysis and Testing practices, Security Awareness and Security Development Trainings, Security Research and Security Response.
Mr. Huebner is a member of the board of directors at SAFCode, an international industry cooperation driving best practices for secure product development.

Mr. Huebner's accomplishments before SAP include 11 years with Microsoft in numerous strategic engagements wherein as a member of the Corporate Trustworthy Computing Team he represented the company as a Government Security Director, internationally. Before joining Microsoft Mr. Huebner was a public officer at the data protection supervisor for the state of Baden-Württemberg in Germany. Mr. Huebner has a degree in law and has specialized on data protection and security.

Panel Session Secure Software *Secure software - we need it more than ever: SAFECODE and more*

Developing software with security built in from scratch is the most important contribution to securing the information society. The panellists are experts with lots of experience in secure software development from different organizations. They will discuss and share their experiences on how to develop software securely.

Detlef Hühnlein

CEO | ecsec GmbH | Germany

Dr. Hühnlein has more than fifteen years of professional experience in the area of IT-security, received a doctoral degree in cryptography from TU Darmstadt, gave lectures about electronic signatures, internet security and identity management at various universities, (co-)authored more than 70 papers for refereed journals and conferences and frequently gives talks at national and international IT security events. He has been actively involved in standardization committees within DIN, CEN, ISO and OASIS and is founder and CEO of ecsec GmbH – a specialized vendor of innovative solutions in the sector of security in the information and communication technology, security management, smart card technology, identity management, web security and electronic signature technology. He is actively involved in recent research projects related to eID and cloud security like SkIDentity and FutureID.

Regulation & Policies *Towards eIDAS as a service*

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 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.

Mohit Kalra

Sr. Manager Secure Software Engineering | Adobe | USA

Mohit Kalra is Senior Manager of Adobe's Secure Software Engineering Team (ASSET), a centralized team of Adobe security researchers. As Senior Manager of ASSET, Mohit is responsible for ensuring Adobe's products are designed, engineered and validated using all aspects of product security, including Adobe's Secure Product Lifecycle (SPLC). In addition, Mohit oversees employee security training and incident response coordination for reported vulnerabilities.

Security Management, CISO Inside *Deciding the right metrics and dashboards for security success*

What makes a "good" product security roadmap and how can we ensure they relay useful information to all interested teams? A "good" security roadmap is going to come from an "ear to the ground" approach to security across all teams. It should also reflect current security industry trends. This is essential in creating a multi-faceted, balanced security roadmap. So, how do you build and keep a solid, adaptable security roadmap in place? This presentation will discuss our experience and approach to this common security challenge. We will also discuss several tools we've put in place to help monitor progress in our security roadmaps and provide useful dashboards to management teams.

Stefan Katzenbeisser

University Professor | Technische Universität Darmstadt | Germany

Stefan Katzenbeisser is professor for Security Engineering at the department of computer science at the Technical University Darmstadt and principal investigator at the Center for Advanced Security Research Darmstadt (CASED). After studying computer science at the Technical University of Vienna, he worked as a senior scientist at Philips Research in Eindhoven. Mr. Katzenbeisser is currently working on security of critical Infrastructures, secure embedded systems and issues of data protection.

Security Management, CISO Inside *IT-security in railway signalling systems*

Control and safety systems take a central role in the safe operation of trains in European rail networks since a long time. These have been primarily designed according to safety considerations. Due to the emerging use of common off-the-shelf hardware and software components as well as the use of open communication infrastructures, such as the Internet, IT security has to be considered as well in this critical infrastructure.
In this area only few applicable standards have been proposed. Lately the IEC 62443 standard has been established, which addresses industrial automation systems in general, but lacks important elements for the transportation sector, especially railway applications. In this presentation we introduce a security engineering process for secure railway signalling applications, which builds up on IEC 62443 and addresses the key requirements stemming from the railway domain. Furthermore, we also present a novel approach for determining the required Security-Level (SL) not by estimating the risk for a possible attack but by developing an attacker model based approach. Additionally we extend the according recommendations of IEC 62443 by specific security activities and introduce guidelines for achieving the required SL.

Josh Kebbel-Wyen

Sr. Program Manager – Secure Product Lifecycle | Adobe | USA

Josh Kebbel-Wyen is a senior program manager at Adobe. He manages Adobe's Secure Product Lifecycle (SPLC) and other strategic security initiatives. In 2008, Josh conceptualized the highly successful Adobe Security Certification Program which has been the catalyst of the creation of the SAFECode Security Training Program in 2013.

Privacy, Data Protection, Human Factors

Building security in takes everyone thinking like a security pro

"Changing the security culture of your company requires harnessing both training and experiential learning techniques. Adobe's security certification program, recently open sourced through SAFECode as a building block for others, is an example of how to leverage training and experience to boost things like response time and scaling security initiatives."

Boris Kennes

Director Product Management Intrinsic-ID The Netherlands

Boris Kennes brings 17 years of experience from the hi-tech industry where he worked in various advisory and management roles. Most recently he was responsible for the R&D program of the EU GNSS Agency where he was also in charge of product strategy and market research. He also brings 8 years of strategy consulting experience from McKinsey and Northstream. Boris started his career in product development at Alcatel and holds an M.Sc. in Electrical Engineering, a Postgraduate degree in ICT and completed the CFA program for financial professionals. Boris has an extensive track record in helping fast growing hi-tech organisations and has a passion for emerging technologies.

BYOD and Mobile Security

Hardware intrinsic security to protect value in the mobile market

More and more mobile device manufacturers are recognizing the importance of security for their devices in order to protect valuable information of their customers. However, the security of many mobile devices currently does not suffice to protect against modern sophisticated attackers. This presentation will go into detail on how mobile devices can be protected using Hardware Intrinsic Security (HIS). HIS technology provides an anchor of trust in hardware for data of mobile users, which achieves protection even against highly skilled attackers.

Florian Kerschbaum

Chief Research Expert SAP Germany

Florian is chief research expert at SAP in Karlsruhe, Germany. In the academic year 2011/12 he was on leave as the deputy professor for the chair of privacy and data security at Dresden University of Technology. Before SAP he has worked among others for the San Francisco-based startup Arxan Technologies as a software architect. He holds a Ph.D. in computer science from the Karlsruhe Institute of Technology, a master's degree from Purdue University, and a bachelor's degree from Berufsakademie Mannheim. He holds 40 patents and serves the academic community as a program committee member and keynote speaker.

Trust Services, eID and Cloud Security

Database encryption for the cloud

We present a research report on the implementation of a system that supports execution of queries over encrypted data. Such encryption allows outsourcing of sensitive data to the cloud, since the data owner retains the secret key and still efficient query processing is feasible. While this is not completely new research, the implementation in a real world large scale in-memory database is still challenging. We will provide an overview of our architecture and detail two use cases to give an insight into how we technically realized the implementation. We then discuss three major enhancement necessary for large-scale deployment.

Alexander W. Koehler

CEO ICT Economic Impact Germany

Mr. Koehler has worked for or with numerous industry and government customers, including Hewlett -Packard , Texas Instruments, Seagate, Utimaco Safeware (Sophos), Wave Systems, Dell, BASF, DVB Bank SE, T-Systems , the AOK health insurance company and the Bavarian State Ministry. He is co-founder and CEO of the ICT Group, member of the Trusted Computing Group, and the Information Systems Audit and Control Association (ISACA). In this regard, he published a book on IT Governance, multiple articles mainly on IT security and has presented domestically and abroad a variety of lectures, as to ISSE 2004, Berlin, ISSE 2007, Warszawa, Government Security, New York 2005, or recently to the Vienna Banking Forum, Austria in 2013. Since 2004, Mr. Koehler is CEO of the ICT Group, comprising three companies. His duties include advising on CxO and IT management level to questions of modern IT infrastructures and the provision of products and services to implement those . Mr. Koehler studied Karlsruhe mathematics and computer science at the KIT (Karlsruhe Institute of Technology), is a Certified Information Systems Security Professional (CISSP ISC ²) and Cloud Security Expert (CCSK CSA).

Cybersecurity, Cybercrime, Critical Infrastructures | *Securing cloud: elastic key management and homomorphic encryption*

Going "Cloud" requires new security technologies as requirements are more demanding than "On-Premise". This presentation will show this leading edge technology on how key management can be done without being forced to make compromises on security, manageability and cloud elasticity.

Jaap Kuipers

Owner | Id Network | The Netherlands

Rolf Lindemann

Senior Director Products & Technology | Nok Nok Labs | Germany

Rolf Lindemann brings more than 15 years of experience in product management, R&D and operations from the IT security industry. He works for Nok Nok Labs, Inc. as Senior Director Products & Technology. Prior to Nok Nok Labs Rolf Lindemann worked as Senior Director Product Management in the user authentication group at Symantec where he was responsible for research and product strategy on device authentication in smart grids and mobile networks. Before Symantec's acquisition of TC TrustCenter, he was Executive Director Product Strategy at TC TrustCenter GmbH. Earlier, Dr. Lindemann headed up the Betrusted research team and was development manager at TC TrustCenter GmbH. In that position he was responsible for the architecture and ITSEC evaluation of the PKI core components.

Panel Session eID | *eID - new Strategies: EU-Regulation - the FIDO Example*

Steven B. Lipner

Partner Director of Program Management and Chairman of SAFECode | Trustworthy Computing Security Microsoft Corporation | USA

Steven B. Lipner is Partner Director of Software Security in Trustworthy Computing Security at Microsoft. Lipner leads Microsoft's Security Development Lifecycle (SDL) team and is responsible for the definition, support and application of Microsoft's SDL process and for tools and programs to make the SDL available to organizations beyond Microsoft. He is also responsible for Microsoft's corporate strategies and policies for supply chain security and for strategies related to government security evaluation of Microsoft products. He is coauthor of The Security Development Lifecycle and is named as inventor on twelve U.S. patents and two pending applications in the field of computer and network security. He serves as a board member and chair of SAFECode. - See more at: http://www.rsaconference.com/speakers/steven-lipner#sthash.dIDFo80B.dpuf

Panel Session Secure Software | *Secure software - we need it more than ever: SAFECODE and more*

Developing software with security built in from scratch is the most important contribution to securing the information society. The panellists are experts with lots of experience in secure software development from different organizations. They will discuss and share their experiences on how to develop software securely.

Milan Marković

Information Security Specialist Banca Intesa ad Beograd Serbia

Milan Marković received B.S.E.E., M.S.E.E., and Ph.D. degrees in electrical engineering from Faculty of Electrical Engineering, University of Belgrade, Serbia, in 1989, 1992, and 2001, respectively. He was a leading researcher of the Mathematical Institute SANU, Belgrade and is currently a lecturer on privately owned University Apeiron in Banja Luka for “Secure Computer Networks”, “Cyber Law”, and “PKI systems” courses.He is an associate professor. He has also performed different courses on different faculties, universities and high scholl in the same domain of computer security and PKI in Serbia. He has also performed tutorials from these topics on different international conferences and security events. His research interests are mainly in public key infrastructure, information security, combined SW/HW security solutions, smart cards, cryptographic algorithms, Mobile security, Identity Management, Information Security Management Systems, Busienss Continuity Management, combining authentication and smart payments, EMV, payment systems, contactless and mobile payment system, etc. He published more than 280 scientific papers in international and domestic books, international and domestic journals, as well as in proceedings of international and domestic conferences. He has been included in very sophisticated security projects, such as PKI systems for: National Bank of Serbia, for some commercial banks, for Ministries of Internal and Foreign Affaires, as well as PKI systems for current Serbian smart card ID project (Ministry of Interrior). He was a member of working groups for preparing electronic signature law and electronic document law in Serbia, as well as for corresponding sublegislative acts. He was a leading consultant of Ministry of Telecommunication and Information Society for accreditation of qualified Certification Authorities in Serbia. He is currently in position of Information Security Specialist in Security Department of Banca Intesa ad Belgrade, a leading commercial bank in Serbia.

BYOD and Mobile Security *On cross-border mobile government systems*

In this paper, we consider possible models for cross-border m-governmnet systems and proposed one secure model. In fact, we proposed a possible model for secure mgovernment systems based on secure mobile application and SOA-Based central platform. The model additionally consists of external entities, such as: PKI (Public Key Infrastructure) server, XKMS (Xml Key Management Service) server, Authentication server and Time Stamping server. The proposed model could be used in different local and/or cross-border m-government scenarios. We evaluated the proposed model compared to the other existing cross-border government systems. As a possible example of described secure mobile application we experimentally evaluated a secure Android based Web services application.

Patrick Michaelis

Senior Auditor AC – The Auditing Company Germany

Patrick Michaelis works as a Senior Auditor for AC – The Auditing Company with the focus on Information Security. Patrick Michaelis has 15+ years of experience working in the IT and Telecoms sector.
He has joined AC – The Auditing Company in August 2013 after 5 ½ years working for a Canadian international leading telecommunication and wireless equipment company as a Senior Security Product Manager where he was his groups representative for EMEA and the global product manager for a secure mobile government solution. Prior to that, Patrick Michaelis was a consultant for Mobility and Client-Server solutions within a European leading independent provider of IT infrastructure services with the main focus on consultancy and conceptual design in the areas of Groupware, Mobile Strategy and Mobile Security.
Patrick is Certified Secure Software Lifecycle Professional (CSSLP®) and has graduated at the Georg-August-Universität in Göttingen as a “Diplom-Physiker” in 1998.

Security Management, CISO Inside *Security by design – information security as a cornerstone of IT-project-management*

A consistent implementation of "security by design" as part of IT project management boosts the success rate of IT projects. Due to the increasing number of threats in complex and connected environments, a consistent, strict and repeatable process is needed to drive the infrastructure towards an acceptable security level. The presentation will focus on some key elements like “what are my assets?”, “threat analysis” and “review and approval” to give some best practices which will allow quick wins in terms of an enhanced security level.

Ulrich Middelberg

Lead IT Operations Security & Projects | Axel Springer SE | Germany

Ulrich Middelberg, head of the team IT Security & Projects at Axel Springer SE, has more then 15 years of professional experience in information technology. He received a MSc in Mathematics from the University of Osnabrück (Dipl.-Math.) and started his career in the mid 90s as research assistant for economic theory at the University of Bielefeld. After working as a software architect for Bertelsmann AG, he joined KPMG Consulting and stayed in the financial services consulting area for more than 9 years. Since 2009 Ulrich is working for Axel Springer SE, in 2011 he assumes responsibility for the IT Security within Axel Springer's IT Service Provider and leads a team of six IT Security professionals and four senior project managers. During the past 18 months Ulrich developed Axel Springer's strategy how leverage public cloud service offerings (e.g. AWS, Google Apps, Microsoft Office 365).

Privacy, Data Protection, Human Factors | *End User Session: Privacy-compliant use of Amazon web services*

Axel Springer is running their popular and free-of-charge 1414 App in the AWS cloud. The App enables readers and journalists to share pictures and videos with each other, enabling every reader to be a reporter. They are using the AWS for the file storage and video transcoding. Axel Springer launched the 1414 App in a traditional on-premises datacentre, but as the number of users grew, the amount of storage and compute power they needed grew and they looked to the AWS cloud for increased flexibility and scalability. By moving their 1414 App into the AWS cloud Axel Springer has been able to reduce their (App related) infrastructure spend to approximately one quarter of the original cost.

Kim Nguyen

Managing Director | D-Trust | Germany

Dr. Kim Nguyen studied mathematics and physics at the universities of Göttingen (Germany) and Cambridge (UK) and received a Ph.D. in mathematics for his work on the relation be-tween classical number theory and cryptographic security of elliptic curves. After two years with Phillips Semiconductors working as a cryptographer, he joined the German Federal Print (Bundesdruckerei) in 2003. Here he was responsible for the topics of cryptographic and chip security as well as infrastructure aspects in the ePassport and eID projects in Germany. Since 2012 he is responsible for all technical security topics within Bundesdruckerei as Chief Scientist Security. In June 2012 he additionally took over the position of Managing Director of D-Trust, the trust center of Bundesdruckerei.

Panel Session eID | *eID - new Strategies: EU-Regulation - the FIDO Example*

Lennart Oly

Managing Director | ENX Association | Germany

Lennart Oly studied political science and law at Goethe-University, Frankfurt, Germany. He has been working as management consultant and expert for cross-company business processes in the automotive industry since 1996. Being intensively involved in the establishment of ENX, the ENX Association appointed Lennart Oly as its managing director end of 2002.

Norbert Pohlmann

Chairman/Director TeleTrusT/if(is) Germany

Norbert Pohlmann studied Electrical Engineering, specialized in Computer Science in Aachen, and has written his doctoral thesis on “Possibilities and Limitations of Firewall Systems”
He was founder and Managing Director at the start-up company KryptoKom. After the merger with Utimaco Safeware AG he was a member of the Utimaco Safeware AG management board from 1999 to 2003.
Since 2003 Norbert Pohlmann has been a Professor in the Computer Science Department for distributed systems and information security and since 2005 he has been director of the Institute for Internet Security - if(is) at the Westphalia University of Applied Sciences Gelsenkirchen, Germany.
He is a founding member of the IT Security Association TeleTrusT, which is devoted to the establishment of trusted IT networks and systems, and has been a member of its board since 1994 and chairman of the board since April 1998.
In 1997 Norbert Pohlmann won the city of Aachen’s Prize for Innovation and Technology.
For five years he was a member of the Permanent Stakeholders' Group of the ENISA (European Network and Information Security Agency).
He is a member of the academic council of the Association for Data Protection and Data Security: GDD. He is also a member of advisory board of the ISP Association eco which is the largest ISP Association in Europe.
Norbert Pohlmann is also a member of the steering board: Task Force IT Security from the German Federal Ministry of Economics and Technology.
In 2011 he was Professor of the year in the category Computer and Engineering Sciences.
Numerous publications, lectures and seminars on the subject of information security testify his expertise and commitment to this subject.
From March to June 2013 Norbert Pohlmann was Visiting Professor at Stanford University, Department of Computer Science.

Opening Plenary Keynotes *Welcome and Moderation*

Panel Session Secure Software *Secure software - we need it more than ever: SAFECODE and more*

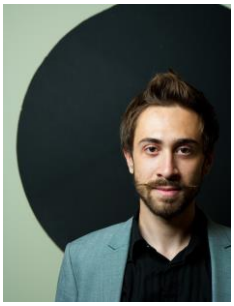
Developing software with security built in from scratch is the most important contribution to securing the information society. The panellists are experts with lots of experience in secure software development from different organizations. They will discuss and share their experiences on how to develop software securely.

Cybersecurity, Cybercrime, Critical Infrastructures *Schengen routing or Schengen encryption?*

Following recent discussions about Europe's digital sovereignty, we will introduce our scientific approach to simulate the effects of routing regulation policies that limit data traffic within the Schengen area to autonomous systems located in the respective countries (covered by the Schengen act).
This controversial concept was proposed by several stakeholders as a countermeasure to the ongoing violation of European data protection policies by well-known governmental and non-governmental parties.
The objective of this presentation is to analyze the current landscape of European Internet interconnections and to compare the fitness for purpose of technical concepts (including AS-level end point encryption), which aim to improve security by protecting integrity and privacy - and thus trustworthiness of communication based on Internet services.

Alexander Polyakov

CTO ERPScan Russia



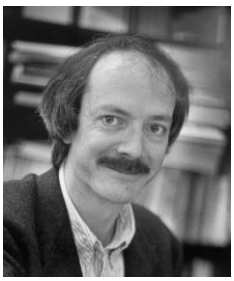
The father of ERPScan Security Monitoring Suite for SAP. His expertise covers the security of enterprise business-critical software like ERP, CRM, SRM, banking and processing software. He is the manager of EAS-SEC.org, a well-known expert on the security of enterprise applications developed by such vendors as SAP and Oracle. He has published a significant number of vulnerabilities and frequently receives acknowledgements from SAP. He is the author of multiple whitepapers and surveys devoted to information security research in SAP, for example, the award-winning ""SAP Security in Figures"". Alexander was invited to speak and train at international conferences such as BlackHat, RSA, HITB, and 50+ others in 25+ countries on all continents as well as at internal workshops for SAP and Fortune 500 companies.

Security Management, CISO Inside *13 Real ways to destroy business by breaking company’s SAP Applications and a guide to avoid them.*

Do you know where all the critical data of your company is stored? Is it possible for attacker to commit sabotage or espionage against your company by breaking into just one of your business critical systems? And if so - what kind of systems could be under attack? Is it easy to break them? Is it a myth that SAP systems could be accessed only internally?

Bart Preneel

Professor KU Leuven Belgium



Prof. Bart Preneel is a full professor at the KU Leuven; he heads the COSIC research group, that is a member of the iMinds Security Department. He was visiting professor at five universities in Europe. He has authored more than 400 scientific publications and is inventor of 4 patents. His main research interests are cryptography, information security and privacy. Bart Preneel has coordinated the Network of Excellence ECRYPT, has served as panel member and chair for the European Research Council and has been president of the IACR (International Association for Cryptologic Research). He is a member of the Permanent Stakeholders group of ENISA (European Network and Information Security Agency) and of the Academia Europaea. He has been invited speaker at more than 90 conferences in 40 countries. In 2014 he received the RSA Award for Excellence in the Field of Mathematics.

Closing Plenary *Post-Snowden Crypto*

In June 2013 Snowden has transferred a set of sensitive documents to journalists, resulting in a continuous stream of revelations on mass surveillance by governments. In this talk we discuss how these revelations impact our understanding of the security of ICT systems. In particular, we discuss the known ways in which sophisticated attackers can bypass or undermine cryptography. We also speculate on how three-letter agencies could be breaking most encryption on the Internet. We relate this to the latest developments in cryptanalysis and discuss which cryptographic algorithms and implementations to select to stay protected.

Ronald Rietveld

Senior Managing Partner (former Head of ISRM, ABN AMRO Bank) KeyDataSecurity.com The Netherlands

Ronald is a senior information security, risk and compliance manager with a drive for implementing practical solutions that benefit the business. He is CISSP and ISSMP certified and has 15 years of experiences in the financial, public and private sector.
At ABN AMRO he developed an IT Risk Control Framework that he successfully rolled-out globally. This increased efficiency and reduced ABN AMRO's cost of compliance significantly.
Currently he is Senior managing partner at KeyDataSecurity.com He manages services and projects that protecting and enable the business success of the clients, while ensuring IT compliance.

Regulation & Policies *Increasing profits with a smart IT risk control framework*

Ensuring the business remains ahead of compliance requirements and how to gain benefits.
- The challenges & lessons learned regarding IT compliance in a complex international environment.
- Our success formula explained, which is based on the Cobit standard with some smart additions
- Ensuring the business remains compliant internally as well as externally through outsource providers
- Delivering compliance in a cost effective manner
- Critical success factors for a successful implementation
- Going beyond just satisfying regulators but also achieving real benefits for the business

Anna Riske

Information Security Manager Volkswagen AG Germany

For the past 15 years Anna Riske has worked in the field of Information Security.
Projects and activities included:

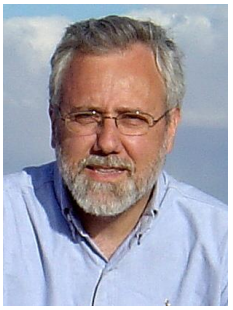
- Information Security Management in both medium and large sized businesses
- Implementation of ISO 27001 certified ISMS
- Certification projects e.g. for manufacturer and partner certifications
- International Information Security Audits/Assessments
- IT and Network Security Projects in various branches (e.g. manufacturing, medical, automotive, education, public/governance)
- IT-journal articles: iX, Lanline, IT-Sicherheit Magazin, ...

Regulation & Policies *End User Session: Transparency and community building: Experiences from establishing a group-wide regulations process*

Information security can only be effectively established across the group via policies and regulations that are binding, collaboratively agreed upon and especially consistently practiced. The global structure and sheer size of an Automotive Group present particular challenges while requiring to link and combine expertise on an international level. Only a transparent process that actively involves all stakeholders and well thought communication structures will lead to success.
Using best practice examples and experience reports, this session provides an insight into the design of such an international process across multiple companies and brands

Corrado Ronchi

Director EISST Ltd UK



Co-founder and CEO of EISST Ltd., a multinational company focusing on secure software architecture, applied cryptography and mobile storage technologies. Dr. Ronchi holds a Ph.D. in Applied Physics and has conducted academic and applied industrial research for 20+ years. Prior to his current occupation, he worked for leading global corporations, such as AT&T, Cisco Systems and the Telecom Italia Group.

Security Management, CISO Inside *A practical approach to application security metrics*

In this presentation we describe a practical approach to application security metrics based on the application's complexity and the observed residual activity of attack vectors, rather than on the analysis of low-level vulnerabilities. In this context, different vulnerabilities can activate the same attack vector, which is defined as an elemental constituent necessary to enable at least one step of the attack procedure.

David Ruana

Product Manager Safelayer Secure Communications S.A. Spain

David Ruana graduated in 1997 in computer engineering from the Universitat Politecnica de Catalunya, Barcelona. In July 1997, he began his professional career at SET Projects dedicated to safety in electronic commerce. In 1999 SET Projects became the nucleus of a new company Safelayer Secure Communications, focused on PKI and digital signature solutions, where has worked until now. After holding the position of Project Manager for 10 years, currently holds the role of Product Manager.

Trust Services, eID and Cloud Security *Achieving the eIDAS vision through the mobile, social and cloud triad*

The Identity Services (eIDAS) proposal aims to "strengthen EU single market by boosting TRUST and CONVENIENCE in secure and seamless cross-border electronic transactions". Although the proposal is technology-neutral, in this paper, we put forward that the mobile, social and cloud triad of technology can quickly boost the deployment of applications and, therefore, may accelerate the achievement of the eIDAS vision.

Stephan Sekula

Security Analyst Compass Security Deutschland GmbH Germany

Stephan Sekula, IT-Security Analyst, Compass Security Deutschland GmbH, Berlin
In his position as IT-Security Analyst he assesses (industrial) IT systems on a daily basis. Since October 2013 he has been actively involved with the HoneyTrain Project, an ICS honeypot based on real life components that has been designed to aid researches from universities and industry alike to gain new insights into the ever changing attack methods used by hackers attacking industrial IT today.

Cybersecurity, Cybercrime, Critical Infrastructures | *Live hacking Industrial Control Systems (ICS) – attack scenarios on critical infrastructure systems*

Hacker attacks and cyber espionage have become a permanent threat for today's industrial IT systems. Specialized malware and Trojans are being developed to extract information from industrial control systems and to sabotage production plants. Apart from highly complex cyber weapons, the highest risk for companies and their production sites lies in vulnerabilities that are already well known from other IT systems. The plethora of attack vectors establishes a whole new threat landscape as the influence of IT on production and control systems increases with ever higher network integration.
This talk explains and demonstrates attack methods used by cyber criminals who target industrial control systems and critical infrastructures. These demos are based on real incidents and case studies.

Cybersecurity, Cybercrime, Critical Infrastructures | *Live hacking Industrial Control Systems (ICS) – attack scenarios on critical infrastructure systems*

Hacker attacks and cyber espionage have become a permanent threat for today's industrial IT systems. Specialized malware and Trojans are being developed to extract information from industrial control systems and to sabotage production plants. Apart from highly complex cyber weapons, the highest risk for companies and their production sites lies in vulnerabilities that are already well known from other IT systems. The plethora of attack vectors establishes a whole new threat landscape as the influence of IT on production and control systems increases with ever higher network integration.
This talk explains and demonstrates attack methods used by cyber criminals who target industrial control systems and critical infrastructures. These demos are based on real incidents and case studies.

Marc Sel

Director | PwC | Belgium

I'm working for PricewaterhouseCoopers 'Advisory Services' in Belgium as a Director, specialised in IT Performance Improvement. I joined the firm in january 1989 as a Consultant. Over time, I specialised in the field of security, both from the technical and from the organisational/management perspective. I performed specialised in-depth reviews, assisted clients with the selection of solutions, and performed implementations. Areas I worked in include authorisations and access control, network security, PKI, smartcards, as well as information security organisation and policies, standards and guidelines.
Prior to PwC I was with Esso, where I worked for two years as a Systems Programmer on IBM mainframes, and two years as a Technical Analyst in the Breda Headquarters. I moved to Esso after a stay of approximately 4 years with Bell Telephone Manufacturing Company, where I developed and delivered training courses on all aspects of digital telephony. Initially after my first graduation I joined Texas Instruments as Internal Sales Engineer in their Brussels semiconductor department for 18 months.

I was born in Antwerp, Belgium. I obtained degrees from Technicum North Antwerp (Antwerp, Belgium - 1980), Brussels Free University (VUB, Brussels, Belgium, 1984) and Royal Holloway University Of London, UK, 2002. See also the graduation list.I hold CISA (1993), CISM (2004) and CGEIT (2008) certifications from ISACA. Since 2006 I'm also accredited "Lead Auditor" for ISO/IEC 27001 assignments.
- see also: www.marcsel.eu

Trust Services, eID and Cloud Security | *Using the semantic web to generate trust indicators*

This presentation describes how Semantic Web technology such as RDF and SPARQL can define and compute Trust indicators related to Trust Service Providers (TSPs) using independent public domain information. Such Trust Indicators can complement the purely cryptographic trust evaluations that are common today. These Trust Indicators are set in the context of the new Regulation of the European Commission on electronic identification and trust services for electronic transactions in the internal market (COM 2012 238), approved by the European Parliament in April, 2014.

Marcel Selhorst

Software Architect | Bundesdruckerei GmbH | Germany

Dipl.-Ing. Marcel Selhorst is a security expert in the fields of Trusted Computing, qualified electronic signatures and electronic identification. After successfully graduating in IT-Security at the Ruhr-University Bochum, he worked for different IT-security companies as a software architect and project manager. Due to his background in cryptography, he developed secure microkernel-based operating systems aided by Trusted Computing technology.
Today, Marcel works at the Bundesdruckerei GmbH as the technical project manager for qualified electronic signatures with the German ID card aswell as a team manager for eID-solutions.

Trust Services, eID and Cloud Security | *Security versus usability – user-friendly qualified signatures based on German ID cards*

This talk will present the German ID cards along with their electronic applications. The pilot phase of the signature application will be introduced along with the valuable feedback received during the first year. Finally, a live demonstration will show the process of loading a qualified signature certificate to the ID card concluded by the actually online-signing of documents.

James Sellwood

Lead Consultant Mobile Security | Consult Hyperion | UK

James Sellwood is a Senior Consultant at Consult Hyperion where his work focuses on the security of new and existing payment systems. Information Security has long been a passion for him with previous roles involving applying this knowledge to both software development and network management. In his last role, James managed the development of software now distributed in large volumes of credit cards. With his eye for detail and significant experience of development and security James has established a reputation for being able to critically test software and to unmask often missed functional and security flaws. James has numerous industrial certifications, a BSc in Combined Science and is completing an MSc in Information Security.

Trust Services, eID and Cloud Security | *Authentication is the key to mobile payments*

Authentication is a key element of any payment service. The consumer payments landscape is changing with new approaches to NFC and many disruptors bringing new payments services to market. How is authentication being performed in these services? What can we learn?

Jon Shamah

Chair | EEMA | UK

Jon Shamah is a graduate of Southampton University, specialising in Aeronautics & Astronautics.
A Chartered Information Technology Professional, and a recognised international Identity Management Subject Matter Expert, he specialises in maximising the technology and operational value chain of very large scale eID programmes. He focusses on the business exploitation of eID, Public Key Infrastructures, authentication and other IAM, especially in critical national infrastructures and national programmes.
Jon was the recipient of the 2009 EEMA Fellowship Award for Services to European e-identity, and is currently the Vice-Chairman of EEMA. Jon is a frequent public speaker on issues surrounding eID and sits on the organising and programme committees of ISSE.
For over four years, Jon consulted to the Nordic Financial Organisation NETS on eID issues, and currently contributes to European Programs such as SSEDIC, TDL, STORK2.0, CloudforEurope and FutureID. In additon, Jon is co-chairman of ITU-T,SG17,Joint Coordination for IDM.

Panel Session eID | *eID - new Strategies: EU-Regulation - the FIDO Example*

Rekha Shenoy

Vice President, Marketing & Corporate Development | Tripwire, Inc. | India

Rekha Shenoy, Tripwire's Vice President of Marketing and Corporate Development, joined Tripwire in 2007, bringing with her an extensive background leading product management teams to deliver maximum customer value. Prior to Tripwire, Rekha held leadership positions in corporate development and product management at BMC Software, Inc., where she was responsible for driving strategic decisions around new technologies and championing the 'Agile Development' methodology to meet product delivery goals. Rekha holds an MBA in Marketing and Finance from Rice University, and received a BS in Computer Science and Engineering from the University Visvesvaraya College of Engineering in Bangalore, India

Security Management, CISO Inside *Connecting security to the business – speaking the CEO language*

One of the biggest challenges facing heads of information security is the ability to effectively communicate the value of their team's efforts across the organisation, especially to the C-Suite, Board of Directors and other non-technical executives. This session will focus on providing practical advice on how to speak the CEO language using concepts CEOs already understand, establish measurable and persistent indicators of security confidence, and expose metrics that drive meaningful action, decision or discussion in the organisation. Session attendees will also learn the characteristics that make successful security metrics and how to constantly adapt them to ensure innovation and improvement.

Michael Sparenberg

Project Manager Internet Key Figures | Institute for Internet Security - if(is) | Germany

Michael Sparenberg is a data scientist and project manager at the Institute for Internet Security, Gelsenkirchen University. His professional expertise covers recent topics in the domain of network and data security, like big data analytics and malware research. He is an active member of multinational collaboration groups and projects funded by the European Commission, aimed at the protection of critical infrastructures and secure information handling. Before joining the research community, he gained more than 20 years of experience running a consulting company, providing services for data recovery and digital forensics. Michael was born in Dusseldorf, Germany. He studied at the universities of Bochum and Dortmund and holds a master degree in economics and sociology.

Cybersecurity, Cybercrime, Critical Infrastructures *Schengen routing or Schengen encryption?*

Following recent discussions about Europe's digital sovereignty, we will introduce our scientific approach to simulate the effects of routing regulation policies that limit data traffic within the Schengen area to autonomous systems located in the respective countries (covered by the Schengen act).
This controversial concept was proposed by several stakeholders as a countermeasure to the ongoing violation of European data protection policies by well-known governmental and non-governmental parties.
The objective of this presentation is to analyze the current landscape of European Internet interconnections and to compare the fitness for purpose of technical concepts (including AS-level end point encryption), which aim to improve security by protecting integrity and privacy - and thus trustworthiness of communication based on Internet services.

Giuseppe Strina

Consultant, Trainer | itb in DHI e. V. | Germany

PD Dr.-Ing. Giuseppe Strina M. A. , 1985-1990 development engineer (hardware and software development), 1990-1993 Research Fellow at the Association of German Engineers (VDI), 1991-1995 Research assistant at RWTH Aachen; 1995 - 2004 Managing Director of a private research and consulting institute at agiplan GmbH, Mülheim an der Ruhr, Germany; since 2004 freelance organizational consultant, trainer and lecturer, since 2006 Associated Professor at RWTH Aachen, since 2007 working as scientific adviser and researcher for the itb, Karlsruhe; here currently lead manager of the BMWi-funded project "ISiK - IT security in crafts" (see www.it-sicherheit-handwer.de, in German)

Security Management, CISO Inside *IT security in crafts - experiences and measures*

Many studies confirm the fact: the smaller a company the higher the need to close existing IT-security gaps. Therefore the German Federal Ministry of Economics supports a project within the German Crafts Association to train crafts consultants to become "IT-security ambassadors". In future these ambassadors will act as contact persons as well as organizers of local information events for all IT security issues. The presentation will show experiences and measures around this exemplary project.

Christoph Thiel

Professor | University of Applied Sciences Bielefeld | Germany

1995 PhD in computer science, 1995-2002 Principal IT-Security Consultant, 2002-2004 Head of the department Security Management of the Fraunhofer Institute for Software and Systems Engineering in Berlin, 2004-2014 Professor at the University of Applied Sciences Düsseldorf, Since 2014 Professor at the University of Applied Sciences
Bielefeld: Chair of Safety and Security of Software Systems

Cybersecurity, Cybercrime, Critical Infrastructures — *The need of European white knights for the TLS/SSL certificate system*

There are many reasons to be concerned about internet security: For example, we have to worry that formerly trusted security solutions are manipulated by (friendly or hostile) government institutions. We have to discover that classical local security concepts have limits in a globally networked world, and we have to learn that in many (if not most) cases cryptographic protocols are implemented in a poor or wrong way.
Since a strong and secure SSL/TSL ecosystem is still held as an important building block of a secure internet, there are numerous efforts to overcome the security concerns stated above. These new approaches include supporting the development of secure (reference) implementations as well as the expansion of the SSL/TSL ecosystems by Certificate Transparency, Certificate Authority Authorization, or Certificate Pinning, and many more. Not surprisingly, these approaches are mainly driven by companies or organisations with a strong U.S. background.
In this presentation, we will discuss these approaches from a European perspective. We derive that from a European perspective, these approaches will only restore trust in the SSL/TSL ecosystem, if on the one hand, they are covered by the European standardization efforts and on the other hand major European companies or organisations without U.S. background will explicitly construct and operate corresponding solutions.

Privacy, Data Protection, Human Factors — *Enforcing data privacy in the age of google glass*

While in many cases wearable devices (involving the incorporation of computers/electronics into clothing and accessories) using all kind of different sensors may enhance our live, there is one big downside: the many privacy issues that spring out of the widespread use of wearable technology. Here we discuss new approaches to formulate and enforce appropriate data privacy policies. We propose simple technologies that could easily be used by any person to indicate his/her requirements to capturing devices and we describe components of wearable devices, which should guarantee the compliance against the situation-based requirements.

Franky Thrasher

Information Security Manager | Electrabel | Belgium

Franky Thrasher is the Information Security Manager for Electrabel Generation. He is responsible for information security in industrial control systems for all the companies conventional renewable and nuclear power plants.
He holds a Master of Science in computer security from the University of Liverpool.

BYOD and Mobile Security — *End User Session: BYOD implementation pitfalls*

Panel Session Critical Infrastructures — *Industrial control system security what are the issues at hand?*

Erik R. van Zuuren

Board Member EEMA Director Deloitte Belgium

Erik's experience/expertize includes a wide strategic- and tactical-level experience/expertize in eGovernment/eBusiness, Enterprise (Security) Architectures, Service Oriented Architectures, Governance, Risk, Compliance, Service Management, Information Security (Management),…

Erik's experiences/engagements include activities at governments and related agencies (Chancelery of the Prime Minister, the Ministry of Foreign Affairs, the Federal ICT Department (Fedict), the Cross Roads Bank for Social Security, the eGov & ICT agency of the Flemish Gov, DG Connect, DG Employment, DG RTD, EC-ISA, etc.) and a diverse spectrum of private industry organisations (incl. ING, KBC, Electrabel Suez, Infrabel, Euroclear, ...).

Erik's achievements includes being one of the fathers/authors of the blueprint for the Belgian Personal Identity Card Project (BelPIC) and being one of the fathers of key egov-supporting services at the Flemish government (wide range of (trust-)services wrt e-identification / e-authentication / authorisation / e-signing / stamping /...).

Currently focussing on eGov-supporting services, trusted/trustworhty online and cloud services, trusted eco-systems, governance of eco-systems, challenges of large scale pilots/eco-systems, electronic/mobile/federated identities, esignature/eseals/etc, ... See also: http://be.linkedin.com/in/evanzuuren

Peter Versmissen

Director – Technology Consulting PwC Belgium

Peter started his professional career at PricewaterhouseCoopers and initially assisted in IS audit work at various multinational corporations. Later on Peter redirected his career towards IT Security projects. In projects Peter typically takes the role of aligning business expectations with IT (Security) concepts. Peter acts as a trusted advisor towards IT professionals and management in further maturing their practice. This type of advice can range from maturity assessments and reviews, to policy definition, and even to business transformation projects.
Peter's main areas of expertise are: IT security (procedural and governance aspects, Identity and Access Management, ISO 27001, cyber security), (organisational) change management and quality assurance on large transformation projects. The latter typically requires a diverse skillset as a professional who masters both IT and business typical knowhow. Peter has gained this experience in the various projects he has been responsible for in the past.
Within PwC Europe, Peter acts as the Belgian representative and driver for all cyber security initiatives and services.
Peter holds a master degree in Business Administration with a specialisation in Information Technology. Peter is also certified in ITIL v3, Prince2, Togaf and is also accredited "Lead Auditor" for ISO/IEC 27001 assignments and CISA certified.

Security Management, CISO Inside Enterprise-wide information security

PwC has access to sensitive client data where confidentiality has become an important factor. Additionally, the type of services provided by PwC and the other Big-4 companies (e.g. audit opinions, tax advice, etc.) leads to a situation where image and trustworthiness are very important and hence potentially interesting in a cyber security context. Based on this situation I would like to present how PwC approaches security, both as vision (governance) and as organisation. I would like address specific measures that we as organisation implement on global and/or local scale to guarantee the required security level. These technical security measures are only relevant if they fit into and are supported by a profound framework. The alignment of vision, supporting framework and topical security solutions (preventive and reactive) result in the expected security guarantee in line with the demands and expectations of ourselves as professional organisation and of our clients.

Eberhard von Faber

Security Strategy and Executive Consulting | T-Systems | Germany

Eberhard von Faber works for T-Systems. He has more than 20 years industrial experience in the field of information security. In his sideline job he is professor for IT Security at Brandenburg University of Applied Science. He started his career as developer for security products. Then he moved to debis Systemhaus where he worked in various fields of security engineering and consulting. He set up, developed and headed the Security Evaluation Facility and was active as evaluator till 2003. Herr von Faber is now working for T-Systems where he held different positions. He formed and shaped the structure of the security offering portfolio, developed innovative solutions and worked on the go-to-market. He is an internationally recognized security expert with more than 100 public talks and publications. Nowadays his workspace is Security Strategy and Executive Consulting. His special subjects are security strategy, enterprise security management, identity and access management, as well as IT security solutions and components. His current special interests are security aspects in outsourcing models including cloud computing, measuring security and assurance models as well as enterprise security architectures.

Security Management, CISO Inside *In-house standardization of security measures: necessity, benefits and real-world obstructions*

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. This report also focuses on real-world obstacles which need to be considered and surmounted in order to secure ICT services in an efficient and flexible way.

Murdoch Watney

Professor of Law | University of Johannesburg | South Africa

Murdoch Watney is professor in the Department of Public Law at the University of Johannesburg, South Africa where she teaches criminal law. She worked as a prosecutor and is an admitted advocate of the High Court of South Africa. She contributed to three textbooks and has published extensively nationally and internationally in law journals on the law of criminal procedure, criminal law, law of evidence and cyber law. She has delivered a number of papers at national and international conferences.

Cybersecurity, Cybercrime, Critical Infrastructures *Restricting excessive state-on-state cyber espionage under international law: a quest of futility?*

States have criticised other states of employing excessive state-on-state cyber espionage. The presentation focuses on establishing whether espionage falls within the ambit of the present international law and if not, which legal solutions – if any - may be considered to ensure that nations do not employ excessive espionage against other nations?

Steffen Wendzel

Head of Secure Building Automation | Fraunhofer FKIE | Germany

Steffen Wendzel leads the building automation security research team at Fraunhofer FKIE, Bonn, Germany, where he also focusses on network covert channel research. He received his PhD in computer science in 2013 and wrote four books. His website is http://www.wendzel.de

Cybersecurity, Cybercrime, Critical Infrastructures

Hidden and uncontrolled: the emergence of network steganography

Classic malware communications take advantage of traffic encryption means but recent developments highlight a trend towards the application of network steganography, i.e. the hidden transfer of malicious data.
The talk discusses network steganography, including its potential and trends, and provides an outlook on future malware.