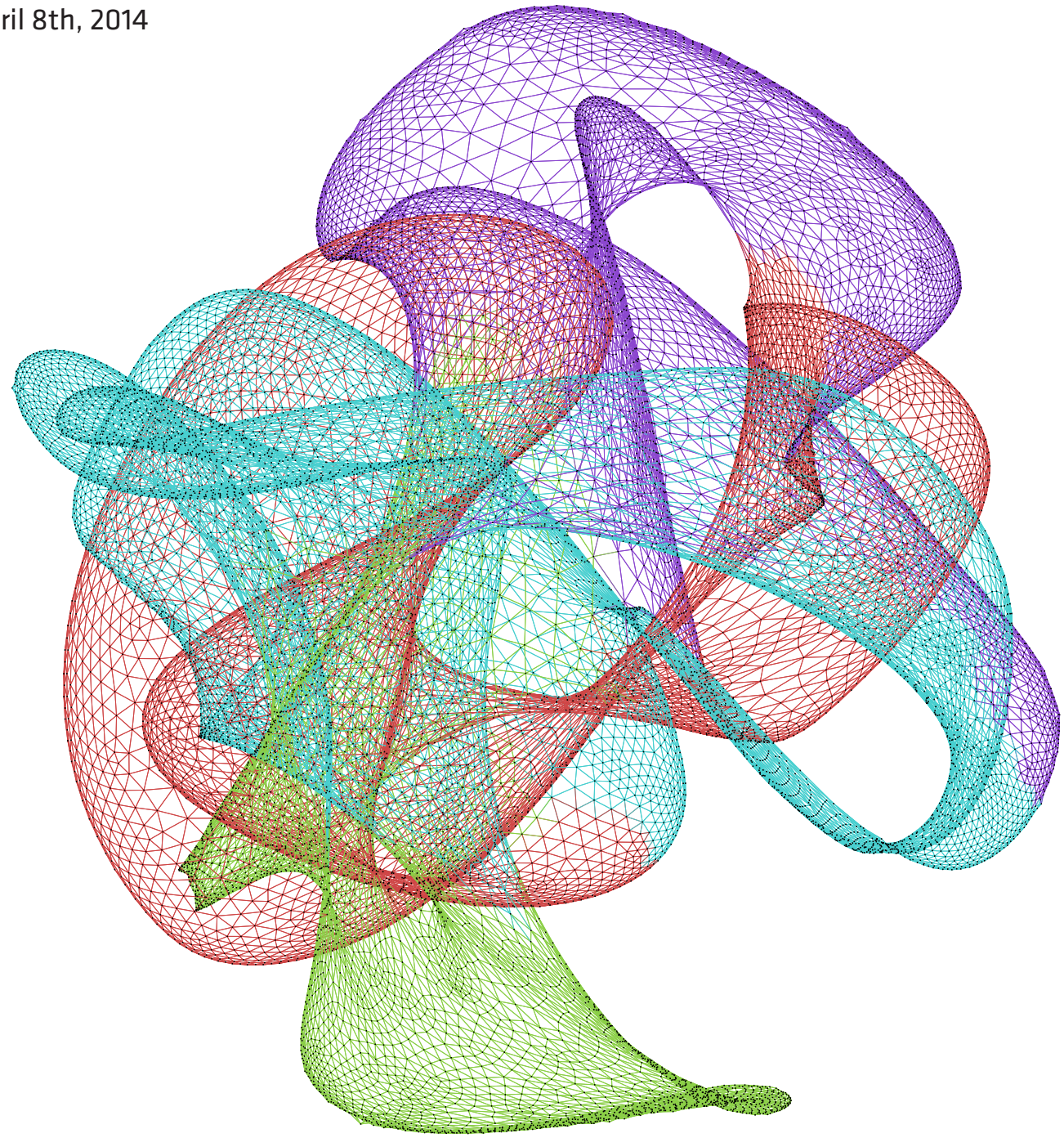
SICS Security Seminar 2014

Securing infrastructures, the Smart GRID and the Things

Nordic Forum, Torshamnsgatan 35, Kista
April 8th, 2014



SWEDISH ICT SICS

PROGRAM

09.00	Introduction Christian Gehrmann (SICS)
09.10	NOTE: New speaker Observations on the Industrial Implementation of an Encrypted Searchable Cloud Database Andreas Schaad (SAP)
10.10	Realizing Trusted Clouds with Trusted Computing and SCAP Mudassar Aslam (SICS)
10.40	Break
11.00	Overview of Security Issues in Public Cloud Platforms Nicolae Paladi (SICS)
11.30	Measurable Security for Sensors - the Driver for Innovation Prof. Josef Noll (Univ. of Oslo & Moviation)
12.15	Lunch
13.15	Internet of Things Security Standardisation Göran Selander (Ericsson)
13.45	Formal Verification of a Tiny Separation Kernel Oliver Schwarz (SICS)
14.15	Smartgrid: Security Challenges - Legacy and Infrastructure Burdens Robert Malmgren (Romab)
14.45	Break
15.00	Assessment of Cyber Security of Enterprise-Wide Architectures Mathias Ekstedt (KTH)
15.30	Smart Grid Security Gunnar Björkman (ABB Germany)
16.15	Conference Wrap-Up, Christian Gehrmann (SICS)

TALKS

Observations on the Industrial Implementation of an Encrypted Searchable Cloud Database
Andreas Schaad, SAP

Abstract
We present an implementation and prototype of a system that supports execution of queries over encrypted data. While this idea is not new, the implementation in a real world large scale in-memory database is still challenging. The three main contributions of the prototype shown are:

a) A significant improvement of functionality by intelligently splitting query execution, i.e. which parts of a query can be performed in the cloud and which on the client.
b) Insights into initial performance measurements on basis of the TPCH benchmark.
c) A domain-specific analysis of three data sets that shows the effects of executing queries over encrypted data and what adjustments are required with respect to the encryption of individual columns.

The observations made when developing the prototype allow to conclude that although searching over outsourced encrypted data is always a tradeoff between functionality, performance and security, it is realistic to assume that working solutions can be provided in the not too distant future to the market.

Bio
Andreas Schaad is a Research Manager in SAP's Product Security Research group. He has been working in IT Security for over 10 years.
His publications are listed in DBLP and Andreas continuously serves the security community as a member of various program committees and as a project reviewer.

Realizing Trusted Clouds with Trusted Computing and SCAP
Mudassar Aslam

Abstract
Lack of user trust is a major obstacle in wide scale commercial, industrial and governmental adoption of many cloud services like Infrastructure-as-a-Service (IaaS). The existing risk management mechanisms such as audit and certification, to increase user trust in IaaS are not robust to deal with the dynamic cloud behaviour; because 1) it is operationally infeasible to audit/assess every cloud platform, 2) infeasible to perform audit frequently and randomly, and as a result 3) the certifications are possibly outdated and hence vulnerable. Using trusted computing and security automation techniques (e.g. SCAP), we propose solutions to solve these issues and to increase user trust in the clouds. Our solutions provide implementation approaches for the newly evolving frameworks for trustworthy clouds such as CSA STAR. The use of existing standards (TCG, SCAP, CSA STAR, etc.) and our prototype implementations validate the feasibility of these solutions for commercial deployment.

Bio
Mudassar Aslam is a researcher at SICS Swedish ICT and also registered as a PhD student in Mälardalen University, Västerås, Sweden. He completed his MS in Information and Communication Systems Security in 2009 from Royal Institute of Technology (KTH), Sweden. His research interests are in the areas of platform security management with the focus on providing transparency services for the public clouds using trusted computing and security automation techniques.

Overview of Security Issues in Public Cloud Platforms
Nicolae Paladi

Abstract
This presentation provides an overview of security risks in public Infrastructure-as-a-Service platforms from the point of view of a cloud provider, followed by several detailed examples of mitigation techniques. The aim of this presentation is to bridge the state-of-the art approaches to infrastructure security used in the industry and the on-going research efforts in this area.

Bio
Nicolae Paladi is a researcher at the Swedish Institute of Computer Science and a PhD student at Lund University. His research interests include distributed systems security, network security and trusted computing.

Measurable Security for Sensors - the Driver for Innovation
Josef Noll

Abstract
The presentation focusses on measurable security as being one of the main drivers of innovation for the Internet of People, Things and Services (IoPTS). Current sensor systems are integrated in silos, and thus only have limited effect on innovation across organisations. Opening up the sensor data to a wider group of users requires (i) security, and (ii) privacy. Security can be addressed through the SHIELD methodology, developed in the European Joint Undertaking Artemis collaborations. Privacy requirements need to be taken into consideration, requiring a framework for an application specific handling of sensor data.

Bio
Josef Noll is professor at the University of Oslo in the area of Wireless Network and Information Security. His work concentrates on areas like mobile-based trust and authentication, personalised and context-aware service provisioning, including sensor systems. He is also CTO in Movation, Norway's open innovation company for mobile services. The company supported more than 40 start-ups in the last two years. He is founding member of the Center for Wireless Innovation, a group consisting of 7 Universities and University colleagues in Norway. Josef Noll was previously Senior Advisor and group leader at Telenor R&I. He was programme manager for the UMTS++ Mobile Broadband Access programme, and project leader of several EU and Eurescom projects. He is reviewer of several EU FP6/FP7 projects, and evaluator of national and EU research programmes.

Internet of Things Security Standardization
Göran Selander

Abstract
The Internet-of-Things (IoT) refers generally to a large set of connected embedded devices which are at an accelerating pace being deployed in many services of the Networked Society. Due to the nature of these services, including critical, unattended infrastructure and usage in the personal sphere, security and privacy protection are critical components. One key ingredient to get interoperable security solutions in place is technical standardisation. The intent of this talk is to show some glimpses from ongoing IoT security related standardisation activities in particular those that that the presenter is involved in (IETF CoRE, ETSI eUICC, GlobalPlatform).

Bio
Göran Selander is a Master Researcher at Ericsson specialising in IoT security. He got his PhD in Mathematics from KTH 1999 and has since then been involved in various security related industry and research projects focusing on authentication and authorisation aspects in mobile and wireless networks, on smart cards, and in embedded devices.

Formal Verification of a Tiny Separation Kernel
Oliver Schwarz

Abstract
Ensuring that no process can access credentials of your online banking or secure communication app is a challenging task - and so is the formal verification of such isolation properties. Besides obvious access methods such as manipulating memory, there are a couple of indirect and hidden ways that need to be covered. The question is how to include them all in the analysis, how to formally express that something has been read and - this is one factor of distinction with our work - what to do when you actually do want an explicit communication channel to exist?

To address the complexity of modern operating systems and provide a solution for IT security's problem child, platform security, SICS Swedish ICT developed a tiny separation kernel (or hypervisor) for embedded systems. KTH Royal Institute of Technology takes care of its formal verification.

In this talk, Oliver Schwarz (who is affiliated with both institutes) will give an overview about both the accomplished verification of a simplified version of that separation kernel and about ongoing efforts to reason on implementations with higher functionality as well.

http://prosper.sics.se/

Bio
Oliver Schwarz is one of the PhD students in the Security Lab at SICS Swedish ICT. As such he is in his last year of studies at the Theoretical Computer Science group of the KTH Royal Institute of Technology in Stockholm. Mainly being active in a collaboration project of these two institutes, he gained experience on security through virtualization in embedded systems and the formal verification of such solutions, mainly by exploitation of theorem provers.
Schwarz holds an MSc (German: Diplom) in Computer Science from Chemnitz University of Technology, Germany.

Smartgrid: Security Challenges - Legacy and Infrastructure Burdens
Robert Malmgren

Abstract
The talk will focus on the challenges that are involved with future and emerging energy systems. In particular we will discuss all the security issues that come with having more interconnections, more dependencies on systems, more external access, and higher levels of automation. We will also discuss the current "hype" in the industry, from governments and others that want to put the stickers "cyber" and "smart" in front of everything and anything. We will look at some overall problems, give several examples from the real world and finally offer some advices on things to avoid and simple quick wins for solid protections as well as remind on forgotten, but important security controls.

Bio
Robert Malmgren has been working as a technical security consultant for the last 20 years. He has been involved in many projects with utility companies, TSO's and government agencies that involve protection of critical infrastructure, industrial control systems as well as the everyday bread-and-butter IT security operations. He has been involved in writing security specifications for new SCADA rollout as well as doing penetration testings, forensic investigations and incident handling.

Assessment of Cyber Security of Enterprise-Wide Architectures
Mathias Ekstedt

Abstract
This talk will advocate the necessity and difficulty to take a holistic approach to cyber security. Most organizations today rely on a complex interconnected ICT infrastructure built from a vast amount of heterogeneous technical components. Due to this complexity there is no single cyber security solution that can secure the architecture, nor any single stakeholder that can overview the full cyber security challenge. The risk of sub-optimizing smart grid cyber security solutions is thus imminent. The talk will discuss security metrics and attack modeling as a potential means for doing system-holistic cyber security assessments.

Bio
Mathias Ekstedt is Associate Professor at the Royal Institute of Technology (KTH) in Stockholm, Sweden. His research interests include systems and enterprise architecture modelling and analyses with respect to information and cyber security, in particular for the domain of power system management. He was technical coordinator of the EU FP7 project VIKING and the manger of the program IT Applications in Power System Operation and Control within the Swedish Centre of Excellence in Electric Power Engineering for many years. He received his MSc and PhD titles from the Royal Institute of Technology in 1999 and 2004 respectively.

Smart Grid Security
Gunnar Björkman

Abstract
Many of society's most critical infrastructures are supervised and controlled by computerized Control Systems, so called SCADA systems (Supervisory Control And Data Acquisition), for example the electrical grid. It is clearly in society's interest to protect these control systems against different types of antagonistic attacks in order to safeguard citizens and property from the impacts from failing or misbehaving infrastructures. One type of attack that has gained considerable interest in the last years is cyber-attacks on SCADA systems. These SCADA systems, which were originally isolated from the outside world, are today more and more often connected to various other networks, even the Internet, and therefore more vulnerable to such attacks.

Today a radical change of the electrical grid is taken place. The introduction of dispersed generation, e.g. solar and wind, requires more automatic control functions on lower voltage levels, more metering and more end customer participation. This is what we call the Smart Grid. This presentation will show some of the new features of Smart Grids based on the experiences gained in the Framework 7 project Grid4EU currently being executed in six demo system in different European countries and being led by six of Europe's biggest Distribution System Operators. Based on the new features in Smart Grids, examples will be given on old and new types of cyber-attacks and possible consequences. Both attacks on low levels, like Denial of Services attacks, and more advanced attacks aimed for the application level will be presented. At the end recommendation for future research activities will be given.

Bio
Gunnar Björkman is employed at ABB in the area of Network Management since 1976 and is since 1995 stationed in Mannheim, Germany. He has held several management positions within R&D and Product Management among them acting as global R&D Manager for ABB's range of Network Control products between the years of 1995 to 1999. Gunnar Björkman has been the Project Coordinator for the, in end 2011, finished EU/FP7 financed security project VIKING. Currently he is coordinating the ABB parts of another FP7 project, Grid4EU, which is focused on the operational aspects of Smart Grids. He is also pursuing a PhD study on SCADA security at Royal Institute of Technology (KTH) in Stockholm. He received is MSc. Electrical Engineering degree from KTH in 1972. Contact him at gunnar.bjoerkman@de.abb.com

NOTES


SWEDISH
ICT
SICS