SICS Security Seminar 2013

Future Trustworthy IT Systems

Ideon Agora, Lund, 11 April 2013

SWEDISH ICT SICS

PROGRAM

8:30	Registration, coffee and sandwich
9:00	Introduction, Christian Gehrmann, SICS
9:10	The Role of Trustworthy Computing to Build Future Secure Internet Architectures, Prof. Adrian Perrig, ETH, Zürich
10:10	How to Secure Infrastructure Clouds with Trusted Computing Technologies, Nicolae Paladi, SICS
10:40	Break
11:00	Trustworthy IT Systems – where is the trust boundary? Prof. Jean-Pierre Seifert, TU-Berlin/Deutsche Telecom Lab
12:00	Lunch (included)
13:00	Mobile Security Evolution, from Fixed Defenses to Defense in Depth, Stefan Andersson, Sony Mobile
13:30	A new Authorization Framework for Internet of Things, Ludwig Seitz, SICS
13:50	The SICS Hypervisor for ARM project, Arash Vahidi, SICS
14:10	Security Issues with the Internet Connected Car, Assoc. Prof. Tomas Olovsson, Chalmers
14:40	Break
15:00	Creating Security for BYOD – Current Approaches, Patrik Ekdahl, Ericsson
15:30	Mobile security in real life, Janne Uusilehto, Nokia
16:30	Conference Wrap-up, Christian Gehrmann, SICS

TALKS

The Role of Trustworthy Computing to Build Future Secure Internet Architectures

Abstract

We have designed the SCION network architecture (SCION is short for: Scalability, Control, and Isolation On Next-Generation Networks). SCION is the first Internet architecture designed to provide route control, failure isolation, and explicit trust information for end-to-end communications. SCION separates ASes into groups of independent routing sub-planes, called trust domains, which then interconnect to form complete routes. Trust domains provide natural isolation of routing failures and human misconfiguration, give endpoints strong control for both inbound and outbound traffic, provide meaningful and enforceable trust, and enable scalable routing updates with high path freshness. As a result, our architecture provides strong resilience and security properties as an intrinsic consequence of good design principles, avoiding piecemeal add-on protocols as security patches.

Attestation is a promising approach for building secure systems. The recent development of a Trusted Platform Module (TPM) by the Trusted Computing Group (TCG) that is starting to be deployed in common laptop and desktop platforms is fuelling research in attestation mechanisms. In this talk, I will briefly present approaches on how to build secure systems with advanced TPM architectures. Unfortunately, the use of Trusted Computing in wide-area networks is challenging, as the TPM does not offer security against local physical attacks.

Despite these issues, I will discuss how Trustworthy Computing mechanisms can be used in future Internet environments. Specifically, I will discuss the use to secure routing, secure fault localization, and how to use trustworthy host-based information in the network.

Bio

Adrian Perrig is a Professor of Computer Science at the Swiss Federal Institute of Technology (ETH) in Zürich. From 2002 to 2012, he was a professor of Electrical and Computer Engineering, Engineering and Public Policy, and Computer Science (courtesy) at Carnegie Mellon University. He served as the technical director for Carnegie Mellon's Cybersecurity Laboratory (CyLab). He earned his Ph.D. degree in Computer Science from Carnegie Mellon University, and spent three years during his Ph.D. degree at the University of California at Berkeley. He received his B.Sc. degree in Computer Engineering from the Swiss Federal Institute of Technology in Lausanne (EPFL). Adrian's research revolves around building secure systems and includes network security, trustworthy computing and security for social networks. More specifically, he is interested in trust establishment, trustworthy code execution in the presence of malware, and how to design secure next-generation networks.

He is a recipient of the NSF CAREER award in 2004, IBM faculty fellowships in 2004 and 2005, the Sloan research fellowship in 2006, the Security 7 award in the category of education by the Information Security Magazine in 2009, and the Benjamin Richard Teare teaching award in 2011.

More information about his research is available on http://www.ece.cmu.edu/~adrian

How to Secure Infrastructure Clouds with Trusted Computing Technologies

Abstract

The steady, abundant and pulsing stream of software vulnerabilities trumpeted in the news draw attention and increase the awareness of the wider public with regard to data security. With no silver bullet for software security available, hardware components such as Trusted Platform Module have been introduced to provide a new layer of protection. Until recently, TPMs have seen a wider success when it comes to data protection (e.g. BitLocker, dm-crypt) or desktop

virtualisation security (Citrix XenClient) on personal computers. However, one of the emerging trends is to use TPM hardware to protect the integrity of computing resources in Infrastructure-as-a-Service environments.

This talk will focus on ideas, techniques and solutions to use TPM hardware in order to ensure resource integrity in IaaS environments.

Bio

Nicolae Paladi is a junior researcher at the Swedish Institute of Computer Science in Stockholm, where he earlier wrote his M.Sc. thesis on trusted computing in IaaS environments. Nicolae's interests are focus on both theoretical and applied aspects of virtualisation and distributed systems security, as well application of new cryptographic approaches to protect data in IaaS environments.

Trustworthy IT Systems – where is the trust boundary?

Abstract

Recent years have witnessed a major demand for trustworthy IT systems, as IT moves into every part of our modern world. Thus, our daily life critically depends on the safety and security of the respective IT systems. While huge efforts are being made all over the world to tackle such issues of our IT landscape another part is getting more and more questions. – the hardware itself.

Due to the globalization of critical hardware manufacturing many parts of our IT systems cannot be seen any longer as coming from a trusted manufacturer. This raises serious concerns on malicious hardware or even hardware Trojans. In this talk we will give a gentle introduction into this problem field, outline central problem settings and present early research results within this new combat field of modern IT security.

Bio

Jean-Pierre Seifert studied computer science and mathematics at Johann-Wolfgang-Goethe-University in Frankfurt/Main. Here he received his Ph.D. in the year 2000 with Prof. Dr. Claus Schnorr, one of the most important theoretician in the field of secure information systems.

Afterwards Seifert gained intensive practical experience working in the research and development departments for hardware Security at Infineon, Munich and Intel, USA. At Intel, USA (2004 – 2006), Prof. Seifert has been responsible for the design and integration of new CPU security instructions for micro processors that are going to be integrated in all Intel micro processors. From 2007 – 2008 he developed for Samsung Electronics the worldwide first commercial secure cell-phone based on the Linux operating system.

Since the end of 2008 Jean-Pierre Seifert has been Professor heading the group "Security in Telecommunications" at TU Berlin. This professorship is related with the management of the identically-named research field at Deutsche Telekom Laboratories, the research and development institute of Deutsche Telekom at TU Berlin at the same time. In 2002 Prof. Seifert has been honoured by Infineon with the award "Inventor of the Year" and has received as well two Intel Achievement Awards in 2005 for his new CPU security instructions for the Intel micro processors.

Mobile Security Evolution, from Fixed Defenses to Defense in Depth

Abstract

This talk will walk you through the mobile security evolution as seen through the eyes of a handset manufacturer. The journey will start back in the days of closed OS devices, describe a situation where the defender had the upper hand and take you through the dramatic shift towards a world dominated by open OS phones and tablets. To handle the new environment the knowledge on how to create appropriate defence mechanisms must be spread across the organ-

ization. The last part of the talk will describe how this is addressed within Sony Mobile Communications both from a technical as well as from a development process perspective.

Bio

Stefan Andersson is a senior specialist in Sony Mobile Communications focusing on product security. He has been active in the security area for more than 15 years working with everything from dedicated security hardware to software security assurance. Mr. Andersson was active in the definition of the UMTS security architecture as a delegate for Ericsson. He has also been involved in the design of the Java MIDP 2.0 security model as well as in the JSR 177 expert group which specified the Security and Trust Services API for J2ME. Working for Sony Ericsson Mr. Andersson was instrumental in the design of all core security features including instances of multiple content protection technologies. He currently occupies dual roles in Sony Mobile Communications where he is both a product manager for the security area as well as member of the software security operations team. Mr. Andersson is currently working on the definition of the next generation SDL to be deployed Sony Mobile Communications.

A new Authorization Framework for Internet of Things

Abstract

This talk presents a framework that allows fine-grained and flexible access control to devices with very limited processing power and memory. We propose a set of security and performance requirements for this setting and derive an authorization framework distributing processing costs between constrained devices and less constrained back-end servers while keeping message exchanges with the constrained devices at a minimum. As a proof of concept we present performance results from a prototype implementing the device part of the framework.

Bio

Ludwig Seitz is a senior researcher at the SICS Security Lab since 2011. His areas of interest are Identity and Access Management, Usable Security, and Privacy Protection. He is currently responsible for a collaborative project with Ericsson Research on Authorization in the Internet of Things. Previously Ludwig worked for the SICS spin-off Axiomatics, where he gathered several years of experience with large-scale, production deployments of identity and access management systems for industrial and governmental customers.

Ludwig holds a M. Sc. in Computer Science from the University of Karlsruhe, Germany and a Ph.D. from INSA Lyon, France.

The SICS Hypervisor for ARM project

Abstract

Virtualisation can be used as a powerful security enabler in computing devices. The Hypervisor project at SICS strives to bring this security to embedded systems, including those past deemed to be incapable of practical virtualisation. Within the SICS ARM Hypervisor project, we have demonstrated how a very small hypervisor can be used to secure an embedded platform with minimal overhead.

Bio

Arash Vahidi is a member of the Security Lab (SEC) at SICS. His main research area is security in embedded systems and virtualisation technologies. He is currently involved in development of the SICS hypervisor for securing embedded systems. In past, Arash worked with design and implementation of cryptographic modules and other types of security hardware.

Arash holds a Ph.D. in formal methods from Chalmers University of Technology in Gothenburg, Sweden.

Security Issues with the Internet Connected Car

Abstract

A modern vehicle consists of 50 to 100 computers, ECUs, which are connected over an internal network. The vehicles will soon be communicating with each other, with road-side objects and be constantly connected to the Internet. In addition, many applications will be offered to drivers by third-party developers, and smaller hand-held devices like Android and iPhones will be seamlessly integrated into the vehicle's network. In this talk, we will see examples of services and what security challenges we face. Security work is quite complex since the internal network is of size of a small company and the vehicle is a safety-critical system with real-time requirements that hardly tolerates any failures.

Bio

Tomas Olovsson is an Associate Professor at the Department of Computer Science and Engineering at Chalmers University of Technology, Sweden, and is involved in both research and education. He received his Ph.D. in Computer Engineering from Chalmers in 1995 which focused on measurement of operational security. He has more than 25 years of experience from the IT industry and has been working actively with computer security since 1990. During 1998-2005 he was the co-founder and Chief Technology Officer of AppGate Network Security where he was responsible for the development of high security products targeting the defence and defence industry.

Creating Security for BYOD - Current Approaches

Abstract

Bring Your Own Device (BYOD) is becoming more and more popular among employees in both enterprise and government. In this talk we will recapitulate the premisses for BYOD and look at how the industry is tackling the need for mobile devices to support strong information separation and management. We will also briefly touch upon the ongoing standardisation efforts in this area.

Bio

Patrik Ekdahl is a Master Researcher at Ericsson in Lund, Sweden. He received his Ph.D. in Information Theory from Lund University in 2003. During the period 2004-2007 he worked for a SME in Lund, developing cryptologic equipment for the Swedish military and high end government institutions. He has been with Ericsson since 2007 where he has been working at the security research department, mainly focusing on mobile device platform security from both a software and hardware perspective. During the last two years he has been involved in different standardisation organisations such as GlobalPlatform and their work on defining a Trusted Execution Environment for mobile devices.

Mobile security in real life

Abstract

This presentation is discussing topics like: Megatrends going on in global mobile security industry. How is the mobile industry thinking about the situation on marketplace and what kind of counter measures mobile industry has taken towards to mobile security? What is the basic nature of mobile security, what are the weak points in mobile security? Can HW security be standardized, why should it be standardized and what are the leading HW security standardization forums offering at the moment, what is available already, what is missing? What are the challenges and possibilities."

Bio

Janne Uusilehto started his career in information technology in 1982, as an independent SW developer and consultant for small businesses. He was an IT support and electronic banking specialist in several Finnish banks. His last position in a bank was with Nordea (then Merita-Nordbanken) as a global cash management specialist, responsible for telecommunication areas of cash management software. Uusilehto was a member of the Merita-Nordbanken Cash Management Services team which initiated Internet sales portals in Finland.

His current position is the Head of Nokia Product Security, globally responsible for the Nokia product security development. His team is the overall owner of product security and product security related education, awareness and process improvement tasks.

Uusilehto is also a member of several Nokia internal security-related management boards, Nokia's main representative to Trusted Computing Group, chairman of the TCG Mobile WG, chairman of the EICTA mobile Security Issue group and Nokia's main representative to the SAFECode forum. Uusilehto is also board officer for Global Platform board of directors.

NOTES