YRP Yokosuka Research Park

Telecom Summit

5rd YRP Symposium on Cooperation between Industry, Academia and Government in Mobile Telecommunications 2003

Advance Program

| Program(English) | Program(Japanese)

'Secure Communications & Transactions - World Class Information Security Research, Technology and Services in the South East of England'

'Welcome and opening remarks'

Mr Neil Impiazzi, Head of International Business, SEEDA - (www.seeda.co.uk) 5 mins

'Information Security at Royal Holloway, University of London: Partnerships with Industry'

Prof. Fred Piper, Head of Information Security Group, Royal Hollloway, University of London (www.isg.rhul.ac.uk) 30 mins

'Research and Development at Vodafone - organization, scope and overview of work in security and smart cards'

Professor Michael Walker, Group R&D Director, Vodafone - 30 mins

'Flexible Cryptography'

Mr Richard Mallett, Managing Director, Thales E-Security Asia Pacific
(http://security.thalesgroup.com). 10 mins

'Domain Based Security: insight into future architectures'

Ms Natsuko Sato, Business Development Manager, QinetiQ
(www.qinetiq.com/services/information.html) 10 mins

'Next Generation PKI'

Mr Omar Farooq, Chief Operating Officer, Ascertia (www.ascertia.com) 10 mins

'The Benefits of Biometrics for Information Security'

Mr Martyn Gates, Marketing Director, OmniPerception (www.omniperception.com) 10 mins

'Secure Payments and Security Evaluation'

Dr Keith Martin, Information Security Group, Royal Holloway, University of London (www.isg.rhul.ac.uk) 10 mins

5-10 min Q&A
Closing remarks by Neil Impiazzi

Biography

Neil Impiazzi joined the South East of England Development Agency (SEEDA) in May 1999 from Invest UK, the UK Government's national inward investment agency. With eight years inward investment experience, Neil has worked extensively with a host of leading international companies from Japan, Korea, Taiwan, China and Australia to manage and deliver their inward investment projects in Europe.

Neil is also responsible for delivering SEEDA's 'Global Regions Initiative' in the Asia Pacific region. To support international business, academia and knowledge transfer, SEEDA has developed this initiative to encourage and facilitate links with other Global Regions with similar expectations and growth. These links are expected to enable the sharing and transfer of new technologies, to increase the knowledge-based networks between like-minded organisations, business and universities, whilst bringing a wide range of benefits to all participating regions including two-way trade and investment. In Japan, SEEDA is currently developing its Global Regions partnership with the Kanagawa Prefecture.

Professor Fred Piper (BSc PhD(London) CEng CMath FIEE ARCS DIC FIMA) has been a Professor of Mathematics at the University of London since 1975 and has worked in security since 1979. In 1985 he formed a company, Codes & Ciphers Ltd., which offers consultancy advice in all aspects of information security. He has acted as a consultant to over 50 companies including a number of financial institutions and major industrial companies in the UK, Europe and USA. The consultancy work has been varied and has included algorithm design and analysis, work on EFTPOS and ATM networks, data systems, security audits, risk analysis and the formulation of security policies. He has lectured world-wide on information security, both academically and commercially, has published a number of cryptographic papers, and is joint author of Cipher Systems (1982), one of the first books to be published on the subject of protection of communications, Secure Speech Communications (1985) and Cryptography: A very short introduction (2002). He was a member of ITSAG, the DTI's Information Technology Advisory Group from 1989 - 1991. From 1992 to 1995 he was a member of ITSSQC, the advisory committee to DTI on IT Standards, Security and Quality. He is currently a member of the Foresight Crime Prevention Panel: IT, Electronics and Communications Task Force, a member of the DTI Management of Information for Fraud Control, Security and Privacy Link Programme, and a member of the Scientific Council of the Smith Institute. He is a member of the Board of Trustees for Bletchley Park. In 2002 he was awarded an IMA gold medal for "services to mathematics" and received an honorary CISSP for "leadership in Information Security".

Professor Michael Walker (BSc PhD (London) Dr.rer.nat.(habil) (Tubinger) Cmath FIMA) Vodafone Group Director of Research and Development. Professor Walker is the Vodafone Professor of Telecommunications at Royal Holloway. He is responsible for the security of the Vodafone networks and services and for heading all of the company's research activities. His work includes the new third generation (3G) mobile systems and mobile e-commerce. Prior to joining Vodafone he was Head of Mathematics at Racal Research Ltd. He has led a number of UK and EU collaborative projects on security for mobile communications, and he has designed cryptographic algorithms and security systems for mobile communications systems, satellite systems, EFTPOS, ATM and military tactical radio. He has also acted as a security consultant to a number of financial institutions. Before joining Racal he was a lecturer at the University of Tubingen, where his research interests included geometry, groups, combinatorics and coding theory. He is Chairman of 3GPP SA3, the group responsible for the security features of 3G, and Chairman of ETSI SMG 10 which is responsible for security of GSM. Formally he was Chairman of the ETSI DECT security expert group, Chairman of ETSI TC Security, member of ETSI SAGE and member of BSI IST/33. He has been BSI Principal Technical Expert to ISO/IEC JTC1/SC27.

Richard Mallett (a first Degree from Nottingham University UK and a Post Graduate Degree in Accounting from Sydney University).has been working in the I.T. and Security industry for almost 20 years and is currently working for Thales e-Security (Asia Pacific) Ltd. Educated and raised in the UK, he has spent his entire career in the Asia Pacific region.

He initially worked in Australia for 10 years working for a US multinational I.T company and then moved to Hong Kong in 1992 to work for Fujitsu Hong Kong Ltd. responsible for managing and growing Fujitsu's telecom software and services division for Greater China.

Still based in Hong Kong, he is now the Managing Director of Thales e-Security Asia Pacific. He is responsible for all business activities involving EMV chip cards, PKI technology and Network Security throughout the Asia Pacific region. He was instrumental in the introduction of EMV chip cards in Japan, with high-profile Japanese companies such as Dai Nippon Printing, UC Card, DC Card and Mitsui Sumitomo Card adopting Thales' security solutions. If you use a Visa or MasterCard chip card, you are already using Thales security products.

Leveraging the success of Thales security solution for EMV financial chip cards, Mr. Mallett's plan is to expand into the Japanese government network security market. Thales will build on its expertise as a supplier of excellent technology and exploit its business model of partnering with strategic system integrators and consultants.

Mr. Mallett has been a Panel Speaker on security issues at The Economist Round Table on E Business as well as at the annual MasterCard Members Conferences.

Natsuko Sato (BSc Computer Science, CEng) is a business Development Manager for Qinetiq in London. Natsuko hold a BSc in Computer Science from University of Bristol. She is responsible for the privatisation of defence technologies into commercial markets in order to maximise the strategic value and operational cost effectiveness of the United Kingdom's defence research capabilities. Qinetiq is a new science and technology powerhouse formed from the major part of the British Government's elite defence research and development organisation. With an unrivalled track record in applied science and technology, it is poised to become a world leading business solutions provider as the leading Science Consultancy company. Previously Natsuko was responsible for pioneering secure knowledge management systems within Shell to share best practices and improve efficiency across the organisation. Natsuko is a Certified Associate of the Institute of Management Consultancy and a member of British Computer Society (Chartered Engineer). She has provided global technology consultancy to multinational companies to maximise their IT investments.

Omar Farooq (BSc in Computer Science, MSc in Information Security) Chief Operating Officer. Omar holds a BSc in Computer Science and an MSc in Information Security, both from Royal Holloway, University of London. Omar has been leading a small, but aggressive sales and marketing effort for Ascertia. Omar has been a freelance consultant in the area of PKI for many years. He has conducted a major study into the practical, liability, regulatory and legislative issues that might arise from the implementation of a network of commercially provided Certification Authorities (CAs) or Trusted Third Parties (TTPs) in support of electronic commerce on a global basis. In a previous role Omar was responsible for defining, implementing and rolling-out of computing services strategy across BaaN. He was at EDS prior to BaaN employed in the Commercial Licensed Evaluation Facility (CLEF) He was responsible for performing security evaluations of products and systems under the UK Government's ITSEC (IT Security Evaluation Criteria) Scheme. Omar also provided consultancy services to GCHQ in the design and implementation specification for CESG's recommended architecture for an HMG Public Key Infrastructure (Cloud Cover).

Martyn Gates has over twenty years of experience in the communications and image-processing industries - including front line broadcast engineering expertise, hardware and software product management, marketing and business development. He has a record of taking innovative products and systems from research concept to established market strength and his role includes leadership of the company's Product Management programme.

He recently joined OmniPerception - a start-up company from the University of Surrey - to lead their "Computing with Vision" strategy: delivering high-performance pattern recognition applications to the world of Face Recognition and Advanced Moving Image Analysis.

Keith Martin (B.Sc. (Glasgow), PhD (London), CMath FIMA) joined the Information Security Group as a lecturer in January 2000. He received his BSc (Hons) in Mathematics from the University of Glasgow in 1988 and a PhD from Royal Holloway in 1991. Between 1992 and 1996 he held a Research Fellowship in the Department of Pure Mathematics at the University of Adelaide, investigating mathematical modeling of cryptographic key distribution problems. In 1996 he joined the COSIC research group of the Katholieke Universiteit Leuven in Belgium where he was primarily involved in an EU ACTS project concerning security for third generation mobile communications. He has also held visiting positions at the University of Wollongong, University of Adelaide and lectured at numerous international institutions. Keith's current research interests include cryptography, mobile security and electronic payment systems. He has served on a number of recent conference program committees and conducts regular refereeing work for international journals. He has provided security consultancy and training for commercial organisations in Australia, Belgium and the U.K. Keith is also interested in e-learning, and is co-developer of the Information Security Group's contribution to The University of London's Virtual Campus Project.

Mini Abstracts

'Information Security at Royal Holloway, University of London: Partnerships with Industry'

Prof. Fred Piper,
Head of Information Security Group, Royal Hollloway, University of London (www.isg.rhul.ac.uk)

Information Security Group,
Royal Holloway, University of London,
Egham,
Surrey TW20 0EX, UK.

The Information Security Group (ISG) is one of the largest academic security groups in the world and is the largest in Europe. The Group regularly hosts international visitors and has close links with leading companies in the area of Information Security. The ISG conducts research in areas such as the design and evaluation of cryptographic algorithms and protocols (where it contributes actively to the international standardisation process), smart cards, electronic commerce, security management, mobile telecommunications security, and the integration of security techniques into specific applications. The presentation will provide an overview of key collaborations with industry in the security sector.

R&D at Vodafone - organisation, scope and overview of work in security and smart cards

Professor Mike Walker
Vodafone Group Director of Research and Development
(www.vodafone.com)

Vodafone Group Plc provides an extensive range of mobile telecommunications services, including voice and data communications, and is the world's largest mobile telecommunications company, with a significant presence in Continental Europe, the United Kingdom, the United States and the Far East through the Company's subsidiary undertakings, associated undertakings and investments. The Group presently operates in 28 countries worldwide.
The benefits Vodafone derive from having close links with the Information Security Group of Royal Holloway, one of the world's most respected centres of excellence in information security wil be highlighted. Vodafone works with a large number of suppliers and benefits from a rage of academic links - for example the Virtual Centre of Excellence in Mobile & Personal Communications (http://www.mobilevce.com) . This presentation will describe how Vodafone works with partners and will describe projects such as the newly established Smart Card Centre at Royal Holloway , jointly sponsored by Vodafone and Giesecke & Devrient GmbH - this project aims to create an international centre of excellence in smart card research and development. The presentation will also describe how Vodafone work with the ISG to design and deliver MSc programmes in Information Security and Secure Commerce.

'Flexible Cryptography'

Mr Richard Mallett,
Managing Director, Thales E-Security Asia Pacific
(http://security.thalesgroup.com).

Thales e-Security has been operating in Asia Pacific for nearly 20 years, with regional Head Office in Hong Kong. The business model is to work with end-users through local partnerships in an OEM, SI or distributor relationship. Thales e-Security is part of the global Thales Group with revenues exceeding US$10b. Thales is a profitable company with long term commitments to the Asia Pacific region, particularly Japan.

Thales, previously known as Racal, is pre-eminent in B2B secure payments, financial chip cards and IP network security. For more than two decades, Thales has been at the forefront of security and payment technology, cooperating and contributing to set the industry standards used for financial transactions and electronic commerce globally.

Thales is daily responsible for making secure the trillions of US$ transmitted around the global payment networks.

"Domain Based Security: insight into future architectures"

Ms Natsuko Sato,
Business Development Manager, QinetiQ
(www.qinetiq.com/services/information.html)

QinetiQ is a new science and technology powerhouse formed from the major part of DERA, the British Government's elite defence research and development organisation. With an unrivalled track record in applied science and technology, it is poised to become a world leading business solutions provider as the leading Science Consultancy company.

DERA's pioneering research and development includes the invention of liquid-crystal displays (LCDs), carbon fibre, the technology for flat-panel speakers, infra-red sensors and microwave radar as well as Chobham armour and shaped charges. QinetiQ has combined and inherited the technology and the expertise from government defence research sites throughout the UK.

Security activities range from Risk Assessment, Security Architecture, and Policy Development through to world-leading Penetration Testing and Vulnerability Analysis. Our Secure Operations Centres in both the UK and the US are protected to unparalleled standards that are recognised as military-strength, and our Research Facility is one of largest and most successful in the world. We have continually developed innovative approaches to security, many of which have become the industry standard.

Every solution we develop is underpinned by our unparalleled intellectual resources but grounded in real life commercial experience.

'Next Generation PKI'

Mr Omar Farooq,
Chief Operating Officer, Ascertia
(www.ascertia.com)

Ascertia is a leading provider of real-time certificate validation solutions, which help to ensure that relying party applications only use valid certificates in their business transactions. In TrustFinderOCSP, Ascertia provides the latest and most sophisticated OCSP (Online Certificate Status Protocol) server on the market.
Ascertia next-generation validation servers include TrustFinderSCVP and TrustFinderXKMS, which allow relying party applications to transfer all PKI processing to these trust servers. This makes PKI application simpler, more cost-effective and easier to deploy.
Ascertia Solutions - Off the shelf PKI enabled solutions meeting the needs of the financial, government, health and consumer markets.
Ascertia's Solutions division is responsible for sourcing and assembling complete turn-key solutions, including infrastructure and application components to meet specific industry and sector needs
Ascertia also offers consultancy and bespoke development services to make applications become PKI-enabled.

'The Benefits of Biometrics for Information Security'

Mr Martyn Gates,
Marketing Director, OmniPerception
(www.omniperception.com)

OmniPerception is an advanced technology company meeting the demanding requirements of customers in the field of Facial Biometrics and advanced applied pattern recognition, with products, system solutions and bespoke software based on proprietary technology

OmniPerception's unique face recognition solutions for access control and personalisation include:

?E a compact high efficiency verification method for implementation on smart cards and resource limited computing platforms - with uniquely flexible scalability and ease of up-date for dynamic client populations.

?E a high performance face identification technique based on Error Correcting Output Coding for demanding personal identity recognition applications - providing unparalleled accuracy and reliability.

'Secure Payments and Security Evaluation'

Dr Keith Martin,
Information Security Group, Royal Holloway, University of London
(www.isg.rhul.ac.uk)

Information Security Group,
Royal Holloway, University of London,
Egham,
Surrey TW20 0EX, UK.

The Information Security Group (ISG) is one of the largest academic security groups in the world and is the largest in Europe. The Group regularly hosts international visitors and has close links with leading companies in the area of Information Security. The ISG conducts research in areas such as the design and evaluation of cryptographic algorithms and protocols (where it contributes actively to the international standardisation process), smart cards, electronic commerce, security management, mobile telecommunications security, and the integration of security techniques into specific applications.

This presentation will provide an overview of key research directions in secure transactions and payment systems and strategic assessment of security protocols. The ISG is involved in a number of European Commission funded research programmes linked to advancing and enabling e-commerce through secure payments. This presentation will describe key projects and highlight future directions for research effort. This presentation will also describe projects such as NESSIE, an EU 5th framework project concerned with the evaluation of cryptographic algorithms. The main objective of the project is to put forward a portfolio of strong cryptographic primitives that has been obtained after an open call and been evaluated using a transparent and open process.