The First

International Cryptographic Module Conference

September 24-26, 2013
Gaithersburg, Maryland

Level 4 Sponsor

Welcomes you to the first

International Cryptographic Module Conference

Some of our service offerings:

FIPS 140-2

atsec offers these cryptographic module testing services:

- Consultation on FIPS 140-2 requirements
- Assessment of test readiness for cryptographic modules
- Support for the production of the Security Policy, Finite State Model and user documentation
- Conformance testing of cryptographic modules, resulting in a certificate issued by the National Institute of Standards and Technology (NIST) and Communications Security Establishment of Canada (CSEC) Cryptographic Module Validation Program (CMVP)

Cryptographic Algorithm Validation

SCAP Validation

NIST Personal Identity Verification Program Testing

Transportation Worker Identification Credential (TWIC) Reader Testing

Hardware Testing

Come and visit us at our booth (#9)!

Find out more on our website:

www.atsec.com

Welcome to the first ICMC!

I am very excited to welcome you to the first International Cryptographic Module Conference. I am also very happy with the response from the technical community to this conference – both in regards to the excellent papers we received and the general interest that this event garnered world-wide.

We have a full agenda for this conference and I would like to invite you to take a look at the presentations and workshops, as well as the opportunities to mingle and meet your peers.

This conference is put on by the technical community for the technical community and it is my hope that the ICMC will grow in the years to come. I would like to thank all contributors, speakers and the program committee for their hard work.

And please take note of the session, “The Next ICMC: Moving Forward, Wrap Up and Summary” on Thursday afternoon where we will discuss the future of the ICMC.

We hope to see you in 2014!

Fiona Pattison, Program Chair
atsec information security

Table of Contents

Contact Information

Event staff is here to assist you.

Bill Rutledge, Project Manager, bill.rutledge@icmc-2013.org, +1 212-866-2169

Carolyn Carniaux, Sales Manager, carolyn@cnxtd.com, +1 609-316-6079

Nikki Principe, Operations Manager, nikki@cnxtd.com, +1 571-249-5680

Program Chair

Fiona Pattinson, atsec information security

Program Committee

Wolfgang Killmann, T-Systems

Junichi Kondo, Director JCMVP, IPA

Helmut Kurth, Chief Scientist, atsec information security

Matt Landrock, Director, Cryptomathic

Dr. Claire Loiseaux, President, Trusted Labs

Prof. Chris Mitchell, Royal Holloway, University of London

Prof. Jean-Jacques Quisquater, UCL

Prof. Sean W. Smith, Dartmouth College

Randall Easter, NIST

About ICMC

ICMC was created by and for the information security industry to fill an important void in the market and establish a place for the community to come together this year. Under the leadership of a Program Committee of industry leaders, ICMC will bring together experts from around the world to confer on the topic of cryptographic modules with emphasis on their secure design, implementation, assurance, and use, referencing both new and established standards such as FIPS 140-2 and ISO/IEC 19790. The event was conceived and founded by atsec information security, a leading accreditation and testing laboratory, working closely with NIST. Operations are managed by Cnxtd (“Connected”) Event Media Services, an event management company with extensive experience in the information security market.

Sponsoring Organizations

Event Sponsors & Exhibitors

Association & Media Sponsors


Conference Agenda

#CryptoModConf

Pre-Conference Workshops

Tuesday, September 24

Workshop Sessions

Walker Ballroom

8:00 **Registration and Coffee**

8:30 **Introduction to FIPS 140-2** *Steve Weingart, Cryptographic & Security Testing Laboratory Manager, atsec information security*

10:30 **Coffee Break**

11:15 **Introduction to FIPS 140-2** (Cont'd)

12:45 **Lunch**

14:00 **Physical Security for FIPS 140-2** *Steve Weingart, Cryptographic and Security Testing Laboratory Manager, atsec information security*

15:30 **Coffee Break**

16:15 **Physical Security for FIPS 140-2** (Cont'd)

17:45 **Adjourn**

Workshop Sessions

Whetstone Ballroom

8:00 **Registration and Coffee**

8:45 **Introduction to Side-Channel Analysis and Testing** *Gary Kenworthy, Gilbert Goodwill, Cryptography Research*

10:30 **Coffee Break**

11:15 **Introduction to Side-Channel Analysis and Testing** (Cont'd)

12:45 **Lunch**

14:00 **The Cryptographic Module and Beyond for Data Protection in a Mobile World** *Eugene Liderman, Sriram Krishnan, Good Technology*

15:30 **Coffee Break**

16:15 **The Cryptographic Module and Beyond for Data Protection in a Mobile World** (Cont'd)

17:45 **Adjourn**

Conference Sessions

Wednesday, September 25

Plenary Keynote Presentations

Walker/Whetstone Ballroom

8:00 **Registration and Coffee**

9:00 **Welcome and Plenary Session:**

Charles H. Romine, Director, Information Technology Laboratory, NIST

Dr Bertrand du Castel, Schlumberger Fellow and Java Card Pioneer

9:45 **CAVP/CMVP Status—What's Next?** *Sharon Keller, NIST; Carolyn French, CSEC; Randall Easter, NIST*

10:30 **Break in Exhibit Hall**

Wednesday Lunch
Sponsored By
eNOVA®

Certification Programs Track

Walker Ballroom

Moderator: *Fiona Pattinson, Director Strategy and Business Development, atsec information security*

11:15 **High Impact CMVP and FIPS 140-2 Implementation Guidance** *Kim Schaffer, Apostol Vassilev, Jim Fox, NIST*

12:00 **The Current Status of CMVP in Japan** *Junichi Kondo, Director JCMVP, at IPA* **The Current Status of CMVP in Korea** *Yongdae Kim, Researcher, ETRI* **Commercial Cryptography in Europe** *Helmut Kurth, Chief Scientist, atsec information security*

12:45 **Lunch**

Technical Track

Whetstone Ballroom

Moderators: *Dr. Claire Loiseaux, President, Trusted Labs; Dr. Yi Mao, Principal Consultant, atsec information security*

11:15 **Physical Security Protection Based on Non-deterministic Configuration of Integrated Microelectronic Security Features** *Silvio Dragone, IBM Research-Zurich*

12:00 **Non-Invasive Attack Testing: Feedback on Relevant Methods** *Sylvain Guilley, TELECOM-ParisTech; Robert Nguyen, Laurent Sauvage, Secure-IC*

12:45 **Lunch**

Certification Programs Track (Cont'd)

Walker Ballroom

14:00 **Panel: How Can the Validation Queue for the CMVP be Improved** Moderator: *Fiona Pattinson, Director of Strategy and Business Development, atsec information security* Panelists*: Michael Cooper, NIST; Steve Weymann, Infogard; James McLaughlin, Gemalto*

14:45 **Building a Certification Program: Techniques That (Might) Work** *Tammy Green, Security Architect and Vulnerability Response Director, Blue Coat Systems*

15:30 **Break in Exhibit Hall**

16:15 **Understanding the FIPS Government Crypto Regulations for 2014** *Edward Morris, Co-founder, Gossamer Security Solutions*

17:00 **FIPS and FUD** *Ray Potter, CEO, SafeLogic*

17:45 **Adjourn**

Technical Track (Cont'd)

Whetstone Ballroom

14:00 **Test Vector Leakage Assessment (TVLA) Methodology in Practice** *Jeremy Cooper, Gilbert Goodwill, Joshua Jaffe, Gary Kenworthy, Pankaj Rohatgi, Cryptography Research*

14:45 **Electro Magnetic Fault Injection in Practice** *Rajesh Velegalati, Jasper Van Woudenberg, Riscure*

15:30 **Coffee Break**

16:15 **Security Mechanisms, Services, Protocols and Architecture for Secure Mobile Applications,** *Sead Muftic, Professor in Computer Networks Security, SETECS*

17:00 **Session TBA**

17:45 **Adjourn**

NB: These speakers were unable to attend, but their paper will be published as part of the proceedings: **Double DPA Attacks that Can Eliminate Power Hiding Effectively**, *Shunxian Gao, Jianfeng Liu, Feiyu Wang, Zhe Wang, CEC Huada Electronic Design*

Conference Sessions

Thursday, September 26

Certification Programs Track

Walker Ballroom

8:00 **Registration and Coffee**

9:00 **A Study on the Certify Interoperability of Commercial Cryptographic Module Validation** *Neng Gao, Jiwu Jing, Limin Liu, Yuewu Wang, State Key Laboratory of Information Engineering, Chinese Academy of Science, Beijing, China*

9:45 **The Upcoming Transition to New Algorithms and Key Sizes** *Allen Roginsky, Kim Schaffer, NIST*

10:30 **Break**

11:15 **Approved vs. Non-Approved: Decoding the Language** *Yi Mao, atsec information security*

12:00 **Pattern Based FIPS 140-2 Cryptographic Module Validation** *Steve Weymann, Mark Minnoch, InfoGard Laboratories*

12:45 **Lunch**

14:00 **Securing the Supply Chain for COTS ICT Products** *Sally Long, Open Group Trusted Technology Forum*

14:45 **Implementation and Assessment on Cryptography for Payment Solutions** *Yan Liu, atsec information security*

15:30 **Break**

16:15 **The Next ICMC: Moving Forward. Wrap Up and Summary** Session Leader: *Fiona Pattinson, Director Strategy and Business Development, atsec information security*

17:00 **Adjourn**

Technical Track

Whetstone Ballroom

8:00 **Registration and Coffee**

9:00 **Entropy: Order From Disorder** *Tim Hall, Apostol Vassilev, NIST*

9:45 **SP800-90 – Reviewing the Standard,** *Stephan Mueller, Principal Consultant and Evaluator atsec information security*

10:30 **Break**

11:15 **Software in Silicon: Crypto-Capable Processors** *Wajdi Feghali, Intel; Valerie Fenwick, Darren Moffat, Oracle Solaris Security; David Weaver, Oracle SPARC Hardware*

12:00 **Key Management Overview** *Allen Roginsky, Kim Shaffer, NIST*

12:45 **Lunch**

14:00 **Implementing SM2 Cryptographic Module on Graphics Processing Units** *Neng Gao, Jiwu Jing, Jingqiang Lin, Wuqing Pan, Yuewu Wang, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China*

14:45 **Panel: Everything You Always Wanted to Know About Labs (But Were Afraid to Ask….)** Moderator: *Fiona Pattinson, Director Strategy and Business Development, atsec information security*

15:30 **Break**

Papers and presentations are available for download at the conference web site.
www.icmc-2013.org Password: sep24#edge

Speaker Biographies

Michael Cooper, IT Specialist, NIST

Michael Cooper is an IT Specialist at the National Institute of Standards and Technology Computer Security Division.

Dr. Bertrand du Castel, Schlumberger Fellow and Java Card Pioneer

Dr. Bertrand du Castel is a French-American author and scientist who pioneered the Java Card, the most sold computer in the world, with over 7 billion units worldwide. A graduate of Ecole Polytechnique with a 1977 PhD from the University of Paris in Theoretical Computer Science, he was a Post-Doctoral Fellow at the IBM France Research Center before hiring with Schlumberger in France in 1978. He emigrated to the United States in 1983 where he has lived in Austin, Texas since becoming an American citizen in 1994. He became head of research for Axalto in 1996, and Chairman of the Technical Committee for the Java Card Forum in 1997. He was named a Schlumberger fellow in 2002 and in 2005 he was presented with the Visionary Award from Card Technology Magazine for his work on the Java Card. In 2005 Dr. du Castel joined with Timothy M. Jurgensen to write Computer Theology: Intelligent Design of the World Wide Web, which uses theological principles to study the role of religion in computer networks, and reciprocally studies religion in the light of well-established computer concepts such as trust.

Silvio Dragone, IBM Research Division, Zürich Research Center

Mr. Dragone received a MSc in Electrical Engineering from the Swiss Federal Institute of Technology (ETH) Zurich in 2002. Mr. Dragone joined the Communication Systems department in IBM Research, Switzerland in 2002 to work on network processors. Since 2007 he works on embedded security and cryptographic coprocessors.

Randall Easter, Director, CMVP, NIST

Mr. Easter assumed the role of Director of the NIST Cryptographic Module Validation Program (CMVP) in 2003. Mr. Easter graduated in 1978 from the Pennsylvania State University with a Bachelor's degree in Electrical Engineering. Prior to joining NIST, Mr. Easter worked for the IBM Corporation in Poughkeepsie, NY for 23-years as Senior Engineer for cryptographic hardware development. He is the author of CMVP and FIPS 140-2 documents and standards; four published ISO standards and three ISO draft standards; and was awarded twelve filed US patents.

Wadji Feghali, Intel

Wajdi Feghali in an architect working in the Intel Data Center and Connected Systems Group. Wajdi works in the area of cryptography, compression, data integrity and data de-duplication. Wajdi is leading hardware and software solutions focusing on performance across all Intel products. Wajdi is responsible for the architecture and implementation of fixed function hardware accelerators as well as instruction set extensions for Intel Core and Intel Atom based processors.

Valerie Fenwick, Manager, Software Development, Oracle Solaris Security

Valerie Anne Fenwick is a Software Engineering Manager at Oracle Corporation with over a decade of experience in computer security. Valerie is currently managing the Solaris Cryptographic Technologies team, of which she was a designer and major contributor. She was the lead for the Solaris Change Request Team, responsible for making decisions as to what code changes are incorporated into the Operating System and Networking consolidation, and one of the sponsors for the Open Solaris project. She was a leader in redefining the software bugtracking strategy and processes used across Sun Systems today, and continuing that transition as we migrate to Oracle's tools. Previously Valerie was the technical lead for the release of Solaris 10 1/06 and was responsible for NAT implementation as well as other

network security features of the SunScreen firewall. She is a co-author of Solaris 10 Security Essentials book.

Jim Fox, Computer Scientist, NIST

Jim Fox is a computer scientist working for the National Institute of Standards and Technology (NIST) in the Cryptographic Module Validation Program (CMVP). Jim graduated with a B.Sc. in computer science and started his career straight out of college working at NIST. Jim has worked at NIST for 27 years and in the CMVP for the last 5 years. Jim also has 10 years UNIX system administration experience.

Carolyn French, Manager, CMVP, CSEC

Carolyn French is the manager of the Cryptographic Module Validation Program (CMVP) at the Communications Security Establishment Canada (CSEC), where she has worked as a Security Architecture Engineer since 2006. Prior to joining CSEC, Ms. French worked at Nortel Networks, where she held the position of Senior System Architect in the CTO office of Nortel's Network and Service Management product line. She graduated from the University of Waterloo with a Bachelor of Applied Science in Systems Design Engineering.

Neng Gao, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

Gilbert Goodwill, Senior Principle Engineer, Cryptography Research

Gilbert Goodwill, Senior Principal Engineer, DPA Software and Training Lead at Cryptography Research, develops and maintains side-channel analysis platforms for research and CRI's customers. He has over 15 years' experience with embedded systems and has worked on security components of wireless systems at both hardware and software providers. He has trained extensively on embedded systems, wireless communications and security related issues.

Tammy Green. Security Architect & Vulnerability Response Director, Blue Coat

Tammy reviews products and features for security flaws. Designs and approves vulnerability fixes. Proposes and architects new security features. Leads the vulnerability response effort for Blue Coat Systems using a virtual team from throughout the company. Publishes vulnerability announcements for customers. Designs security processes for use within the company. Certification Technical lead achieve FIPS 140-2 and Common Criteria certifications for key products.

Sylvain Guilley, Scientific Advisor, Secure-IC

Sylvain Guilley is associate professor at TELECOM ParisTech. He has been conducting researches towards defining provably secure architectures for trusted computing for ten years. Many proofs of concept, in secure designs and in implementation of cryptography, have been transfered to the industry, in products (ASIC, FPGA) that have been evaluated at the highest levels.Sylvain authored more than 100 scientific publications and 10 patents. Sylvain graduated from Ecole Polytechnique (X97), TELECOM-ParisTech (ENST 2002), and got a MSc from ENS / Paris 6 University, a PhD from TELECOM-ParisTech (2007) and an HDR from Paris 7 University (2012).

Tim Hall, NIST

Dr. Hall holds a PhD in Electrical Engineering from University of Delaware. After working on modeling and simulation in private industry, he joined the National Institute of Standards and Technology (NIST) in 1999, working on internet telephony, wireless network modeling and program management for the Advanced Technology Program (ATP). In 2006 he joined NIST's computer security division, developing tests for cryptographic algorithms. His latest research topic is entropy sources for cryptographic applications.

Joshua Jaffe, Research Scientist, Cryptography Research

Josh Jaffe is a Cryptosystem Researcher and Engineer at Cryptography Research. His recent research has focused on physical and mathematical analysis of smart card security and related

intellectual property, including differential power analysis and related countermeasures. Josh is a founding employee of Cryptography Research, Inc. He earned a B.A. summa cum laude in Physics and Computer Science at Brandeis University.

Jiwu Jing, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

Sharon Keller, Director, Cryptographic Algorithm Validation Program (CAVP), National Institute of Standards and Technology (NIST)

Ms. Keller has worked as a computer scientist for the U.S. Federal Government since October of 1983. She joined NIST's Computer Security Division in 1988. Ms. Keller is the Director of the NIST Cryptographic Algorithm Validation Program. She has designed and developed cryptographic algorithm validation systems for various cryptographic algorithms. Other duties include managing the Cryptographic Algorithm Validation System tool, validating cryptographic algorithm implementations, and writing cryptographic algorithm validation guidance.

Gary Kenworthy, Senior Principle Engineer – Digital Signal Processing, Cryptography Research

Gary Kenworthy is a Senior Principal Engineer at Cryptography Research. Kenworthy investigates EM and RF vulnerabilities on cryptographic systems, and develops software and systems to support that research. His experience covers many aspects of signal processing, communication, cryptanalysis, adaptive filters, and location finding. Prior to joining Cryptography Research, he served as Chief Technical Officer of Signami, LLC, which provided signal analysis software and hardware, collection systems, and consulting to the Department of Defense. He holds B.S. and M.S. degrees in Electrical Engineering from Brigham Young University.

Yongdae Kim, Ensec

Yongdae, Kim is a researcher in the attached institute of ETRI (Electronics and Telecommunications Research Institute), Korea. In the past, he had conducted a collaborative research (SASEBO Project) with AIST (National Institute of Advanced Industrial Science and Technology) while at Tohoku university. Recently, he developed POTASA (Platform Of Testing and Analysis of Side-channel Attacks) for smart card. His research interests include secure design of cryptographic hardware and software, side-channel attacks and countermeasures, cryptographic module validation program.

Junichi Kondo, Director JCMVP, IPA

Sriram Krishnan, Senior Director, Product Management and Ecosystem, Good Technology

Sriram Krishnan is a Senior Director, Product Management and Ecosystem at Good Technology. With more than a decade of experience in the mobile industry, he has introduced multiple wireless software products and services in the marketplace. Mr. Krishnan is currently responsible for incubating and productizing emerging mobile security technologies, having recently launched Good Trust™, an industry first in mobile identity and access management (IAM). Recently he spoke at the Gartner IAM and Winter Biometrics conferences.

Helmut Kurth, atsec information security

Helmut Kurth has been working in the area of information security for more than 25 years. His professional experience includes the development of the German IT Security Evaluation Criteria in 1989, participation in the development of the European criteria (ITSEC/ITSEM), and contributions to the development of the US Federal Criteria and the Common Criteria. Helmut Kurth has been involved in security evaluations of IT products since 1988 and has evaluation experience ranging from smart cards to mainframe operating systems. He is working as the chief scientist and Common Criteria lab director of atsec

information security in Austin, Texas, USA.

Eugene Liderman, Director of Public Sector, Good Technology

Eugene Liderman has over 14 years experience in the Information Technology field, specifically in Networking, Directory Services, Email, Mobility, and Information Security. Currently Mr. Liderman is the Director of Public Sector Technology where his primary responsibility is to assist customers in navigating the unique mobile security challenges that exist within Federal Civilian and DoD organizations. Mr. Liderman has spoken at numerous public forums. He belongs to AFCEA, ACT/IAC, and the CTIA Cyber Security Working Group.

Jingqiang Lin, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

Limin Liu, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

Yan Liu, Managing Director and Principal Consultant, Atsec Information Security Corporation China

Yan Liu, a Managing Director and Principal Consultant of atsec China, has worked in IT security for more than 15 years. His areas of interest include cryptographic algorithms, protocols and systems, privacy enhancing technology, DRM technologies, as well as information security standards including Common Criteria, FIPS 140, PCI etc. He has practical experiences in design, implementation and evaluation of security systems and in how to choose effective techniques and standards to address security issues.

Claire Loiseaux, President, Trusted Labs

Sally Long, Director, Open Group Trusted Technology Forum

Sally Long has managed collaborative customer-supplier forums for over twenty years. She is currently The Open Group Trusted Technology Forum Director. The forum recently published the Open Trusted Technology Provider Standard - Mitigating Tainted and Counterfeit Products (O-TTPS) and they are piloting an O-TTPS Accreditation Program, with a planned public launch for December 2013. Ms. Long has a Bachelor of Science degree in Electrical Engineering from Northeastern University in Boston, Massachusetts.

Yi Mao, Principal Consultant, atsec Information Security Corporation

Yi Mao, CISSP, holds a Ph.D. in Mathematical Logic (2003) and a Master's degree in Computer Science (2000) from the University of Texas at Austin. As Deputy Lab Director at atsec information security corporation, Dr. Mao both oversees and performs a lead role in the security evaluation and testing of IT products against standards such as FIPS 140-2 and Common Criteria. She frequently gives presentations on information security topics at national and international conferences.

James McLaughlin, Product Manager, Gemalto

James McLaughlin is a member of the corporate Identity and Access group at Gemalto. In his role as Product Manager, James manages several products and initiatives. These include the IDPrime PIV Protiva Personal Identification Verification (PIV) solution providing strong authentication solution based on the FIPS 201 specification for government and enterprises; IDAdmin service delivering a turnkey hosted provisioning and support service to manage IDPrime .NET devices; and Microsoft partner relationship, finding areas of synergies for the benefit of both and their mutual customers. With over 24 years of experience, James has been instrumental in strategic developments at Gemalto that bring effective smart card and PKI-based solutions to the customer.

Mark Minnoch, Account Manager, CISSP, CISA, Infogard

Mark Minnoch is the Cryptographic and Security Testing Laboratory Director and FIPS 140-2 Program Manager for InfoGard. He has over 25 years of experience in high tech industries including programming, commercial systems, networking management, and information security. He has extensive program management experience and has served as the primary liaison to customers and NIST regulators. He has led InfoGard to achieve the most FIPS 140-2 certificates the last three years.

Darren Moffat, Senior Principal Software Engineer, Oracle Solaris Security

Darren is a Senior Principal Engineer in the Solaris Core Technoglogies group. He is one of the architects for Solaris Security, and has a focus on authentication, cryptography and application containment. He was also the architect and lead developer for the encryption functionality in ZFS. He joined Oracle as part of the Sun acquisition, where he had been in the Solaris development organisation for 12 years. Prior to that Darren worked in SunService supported Trusted Solaris and other Solaris security functionality. Prior to Sun Darren worked for the UK Ministry of Defence and is a graduate of the Computing Science department at the University of Glasgow (Scotland).

Edward Morris, Co-Founder, Gossamer Security Solutions

Prior to co-founding Gossamer Security Solutions, Ed Morris co-founded Atlan Laboratories in 2000, building its FIPS 140-2 laboratory into one of the largest. After SAIC acquired Atlan in 2009, Ed stayed on as a Lab Director, eventually assuming management of both SAIC's Common Criteria and FIPS 140-2 Laboratories before leaving in 2012. At Gossamer, Ed leverages his fifteen years experience in cryptography, FIPS, and CC for Gossamer's CC and FIPS customers.

Stephan Mueller, Principal Consultant and Evaluator, atsec information security corporation

Stephan Mueller holds a Master's degree in Business Administration (1999) from the Technical University Dresden, Germany. Stephan Mueller currently works as a principal consultant and evaluator with atsec information security GmbH, Germany. His main responsibilities include evaluation of security aspects of IT products based on industry standards including FIPS 140-2 and Common Criteria. Consultancy services are provided for architecting secure products, especially in the Open Source and Linux realm as well as operating systems in general.

Sead Muftic, Professor in Computer Networks Security, SETECS

Sead Muftic is a Professor in Computer Networks Security at SETECS. He has a MS and a Ph.D degree in Computer Science from The Ohio State University. His research interests include security for cloud computing environments, security for mobile applications and trusted computing infrastructures.

Robert Nguyen, Senior Evaluator, Secure-IC

Wuqing Pan, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

Fiona Pattinson, Director Strategy and Business Development, atsec information security

Fiona Pattinson joined atsec information security corporation in 2004 as quality manager. She also manages the Cryptographic Module Testing Laboratory, the successful accreditation of atsec's Cryptographic Module Testing Laboratory. She contributes in atsec's Common Criteria laboratory as a project manager and evaluator for the US scheme. Fiona earned her Master of Science in computing for commerce and industry from the UK's Open University.

Ray Potter, CEO and Co-Founder, SafeLogic

Ray Potter is the CEO and co-founder of SafeLogic. Previously, Ray founded Apex Assurance Group, led the Security Assurance program at Cisco Systems, and co- authored FIPS 140 Demystified:

An Introductory Guide for Vendors. Based in Palo Alto, Ray has spoken internationally on topics related to risk management, information assurance, and compliance.

Allen Roginsky, Mathematician, NIST

Allen Roginsky works as a Mathematician at the National Institute of Standards and Technology. His present research interest is Cryptography and its applications. Prior to switching to Cryptography, he spent a number of years with IBM Corporation analyzing and improving computer networks' performance. Allen received his Ph.D. in Statistics from the University of North Carolina at Chapel Hill in 1989. He has more than 30 publications and over a dozen US patents.

Pankaj Rohatgi, Director of Engineering, Cryptography Research

Dr. Rohatgi is an Engineering Director at Cryptography Research where he leads technical efforts in the area of side-channel analysis and countermeasures. He has over 20 years of experience working in the security industry, including 14 years at IBM Research. Apart from contributing to the security of products, Dr. Rohatgi is also active in the security research community. He has published over 40 technical papers, holds numerous patents, and has received several awards for his work in the areas of security and side-channel analysis He was the Program co-Chair of the CHES 2008, serves as an associate editor for the JCEN journal, and will serve as the Program co-Chair of the CARDIS 2013 conference.

Charles H. Romine, Director of the Information Technology Laboratory (ITL), NIST

Charles Romine is Director of the Information Technology Laboratory (ITL). ITL is one of six research Laboratories within the National Institute of Standards and Technology (NIST) with an annual budget of $120 million, more than 350 employees, and about 160 guest researchers from industry, universities, and foreign laboratories. Romine oversees a research program designed to promote U.S. innovation and industrial competitiveness by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of information systems, including cybersecurity standards and guidelines for Federal agencies and U.S. industry, supporting these and measurement science at NIST through fundamental and applied research in computer science, mathematics, and statistics. Through its efforts, ITL supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Laurent Sauvage, Co-founder and Scientific Advisor, Secure-IC

Kim Schaffer, CMVP, NIST

Kim Schaffer is an information technology specialist in the Cryptographic Module Validation Program under the Computer Security Division at NIST. Previously, Dr. Schaffer was the Laboratory Director of CEAL at CygnaCom Solutions, a subsidiary of Entrust. Dr. Schaffer has worked for over 30 years in information assurance, communication and computer security, and digital forensics. Kim became a Certified Information Systems Security Professional in 2002, and recently received a Doctor of Science in Information Assurance.

Hongsong Shi, China Information Technology Security Evaluation Center

Hongsong Shi received the Ph.D. degree in computer science from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2010. He was a visiting student in the Department of Computer Science at the University of Calgary, Calgary, CA, between 2007and 2009. He is currently a research fellow in China Information Technology Security Evaluation Center (CNITSEC). His research interests include cryptography, network security, and theoretical computer science. He has published several papers on pseudorandom generators, secure message transmission protocols and network security applications, including IEEE Transactions on Information Theory, Journal of Designs, codes and

cryptography, and ACM AsiaCCS, etc. He was a speaker of the ICCC 2011.

Jasper Van Woudenberg, CTO North America, Riscure

Jasper is Principal Security Analyst and Manager for Riscure North America. At Riscure, Jasper's expertise has grown to include various aspects of hardware security; from design review and logical testing, to side channel analysis and perturbation attacks. He leads Riscure North America's pentesting teams and has a special interest in combining AI with security research.

Apostol Vassilev, Cybersecurity Expert, Computer Security Division, NIST and Staff Member, CMVP

Apostol Vassilev is a cybersecurity expert in the Computer Security Division of NIST and a staff member of the Cryptographic Module Validation Program. He works on module validations and the development of FIPS 140-2 implementation guidance. Dr. Vassilev also conducts research on cybersecurity standards and cryptography. He is an author and inventor with numerous publications and granted patents. Mr. Vassilev holds a Ph.D. in Mathematics from Texas A&M University.

Rajesh Velegalati, Research Intern, Riscure

Rajesh is currently a Research Intern at Riscure North America. He is working toward his Ph.D. in Computer Engineering at George Mason University. He received his M.Sc. degree in Computer Engineering from George Mason University in 2009 and B.E in Electrical Engineering from Andhra University in 2006. His Ph.D. research focuses on Side Channel Analysis and Countermeasures against SCA. His research interests include cryptography, hardware/software applications of cryptography, nanotechnology and computer forensics.

Yuewu Wang, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

David Weaver, Senior Principal Engineer, Oracle SPARC Hardware

David Weaver has been involved with SPARC for 25+ years. He currently oversees the consistency and evolution of Oracle's SPARC instruction set architecture (ISA). He has edited or authored 6 ISA specifications and an IEEE Standard. He holds one computer architecture patent and has three additional patents pending. He holds a BS in Computer Engineering, an MS in Computer Science, and an MBA.

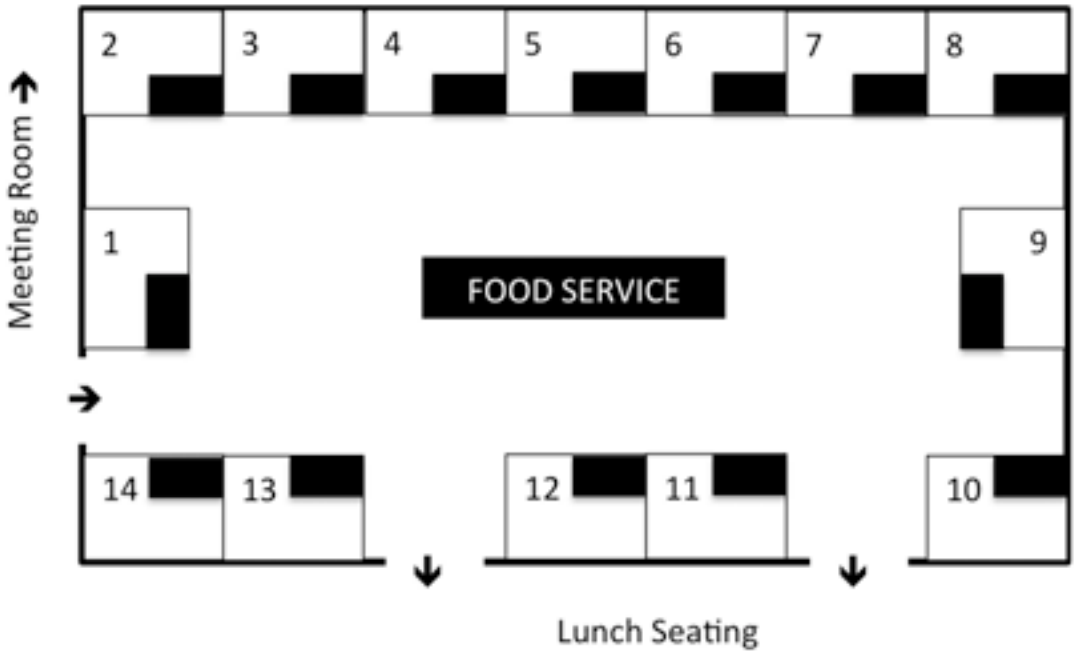
Steve Weingart, Cryptographic and Security Testing Laboratory Manager, atsec Information Security Corporation

Steve Weingart is a Principal Consultant and the Cryptographic and Security Testing Laboratory Manager for atsec information security. Steve began as an electrical engineer with a BSEE from the University of Miami in 1978. He has been working in security and cryptography since the early 1980's. Whjile at IBM's Thomas J. Watson Research Center he joined the NIST working group that wrote the FIPS 140-1 standard and went on to be lead hardware engineer on the first FIPS 140-1 level 4 validated product, the IBM 4758 cryptographic co-processor.

Steve Weymann, Senior Security Engineer, Infogard

Steve is a Senior Security Engineer with extensive experience in information technology security standards and implementation. Steve's eight plus years with InfoGard include FIPS 140-2 cryptographic module validation, FIPS 201 identity component qualification, security risk assessment and support for InfoGard's Business Development establishment of new testing and evaluation services. Steve has a Bachelors in Electrical and Computer Engineering from the University of Arizona and maintains his CISSP certification. His career background includes hardware, software and systems development and management, with expertise in healthcare systems, sonar and defense communications.

Exhibit Floor Plan



1	Plasma Ruggedized Solutions	8	Blue Coat
2	SafeNet	9	atsec information security
3	Cryptography Research	11	Thales
5	ARX	12	ETRI
6	Riscure North America	13	Secure-IC

Exhibitors and Sponsors

Media Partner

ACT Canada

www.actcda.com

ACT Canada is a non-profit association, federally-incorporated in 1989. As an educator, enabler, influencer and advocate for members, ACT Canada is the internationally-recognized authority, trusted knowledge resource and catalyst for change in payments and secure identity. We build bridges and break down barriers to support our members in their quest for competitive advantage in the payments, authentication and identity management space. We are the go-to resource for issuers, acquirers, merchants, regulators, brands, networks, governments, technology providers, integrators, industry associations, security specialists, gateways, processors, integrators, loyalty companies, transit systems, secure identity solution providers and many other stakeholders.

Level 4 Sponsor

atsec Information Security Corporation

9130 Jollyville Road, Suite 260, Austin, TX 78759

www.atsec.com

atsec information security is an independent, privately owned company that focuses on providing laboratory and consulting services for information security. We address commercial and government sectors around the world. Our consultants are expert in a variety of technologies including operating systems, databases, and network devices. Our laboratories specialise in evaluating and testing commercial products, using international standards to help provide assurance to end-users about the products they buy and use. We focus on assisting organizations, large and small, achieve compliance with standards such as Common Criteria, FIPS 140-2, O-TTPS, PCI, ISO/IEC 27001 and FISMA and offer a variety of services that complement that goal.

Booth 5

ARX

855 Folsam Street, Suite 939

San Francisco, CA 94107

www.arx.com

ARX, Inc. is the leading provider of highly secure and efficient cryptographic and key-management security solutions. ARX develops and markets the leading FIPS 140-2 level 3 HSM called PrivateServer™. PrivateServer is a network-attached, high-performance, multi-application, high-capacity HSM that is broadly used in financial and government markets globally. Today PrivateServers operate in the largest distributed networks securing and supporting Billions of transactions under financial applications. Learn more: http://www.arx.com/products/private-server-hsm or Contact: sales@arx.com.

Booth 8

Blue Coat

420 North Mary Avenue, Sunnyvale, CA 94107

www.bluecoat.com

Blue Coat empowers your agency so you can safely and securely deliver Mission Critical Applications, Identify Threats Infiltrating your Network, Accelerate change, Manage Risk, Accelerate Application Performance and Protect Mobile Workers. For more information visit: www.bluecoat.com and join the conversation on our blog site: www.federalblueprint.com.

Booth 3

Cryptography Research, Inc.

425 Market Street, 11th Floor, San Francsico, CA 94105

www.cryptography.com

Cryptography Research, Inc. (CRI), a division of Rambus Inc., is a leader in semiconductor security research and development. Established by internationally renowned cryptographer Paul Kocher, CRI develops and licenses innovative technologies in areas including tamper resistance, content protection, anti-counterfeiting, network security, and financial services. Over six billion security products are made each year under license from CRI. Security systems designed by CRI scientists and engineers protect hundreds of billions of dollars in commerce annually.

Event Sponsor

Cygnacom Solutions

7925 Jones Branch Drive, Suite 5400, McLean, VA 22102

www.cygnacom.com

CygnaCom Solutions Inc. headquartered in McLean, VA, specializes in Public-Key Infrastructure (PKI), Information Assurance and system security engineering. CygnaCom provides risk assessments, security architecture, identity/privilege management and security assurance consulting. CygnaCom is a one-stop provider of comprehensive, U.S. standards-based security testing and evaluation services of IT and cryptographic products. CygnaCom laboratories test Commercial and Government products to verify design, implementation and documentation meet U.S. Government security requirements. We develop Protection Profiles used to evaluate products and solutions. Services include architecture, design, implementation and documentation review. We offer design & development team training plus security design & engineering consulting services.

Booth 7

eNOVA Technology

1st Floor, #11, Research & Development 2nd Road Science Based Industrial Park, Hsin-Chu City, Taiwan, China

www.enovatech.net

Enova builds and provides comprehensive enterprise based security products for Data at Rest (DAR) and Data in Transit (DIT) management and compliance solutions on a global basis. Enova offers the tools to automate and protect data distributed to virtually any SATA and USB enabled storage device, and manages these efforts using simple to understand processes. Using Enova data security products, security teams will become more proactive, while compliance teams can more effectively manage, collaborate and enforce secure accountability. Enova's growing customer base includes leading Governments, Global 2000 organizations in the financial services, healthcare, retail, energy and utility, transportation and manufacturing. For more information, please go to www.enovatech.com or send email to nfo@enovatech.com. You can also contact Mr. Robert Wann at +1 510 825 7900 or email rwann@enovatech.com.

Booth 12

The Attached Institute of ETRI (Electronics and Telecommunications Research

PO Box 1, Yuseong, Daejorn, Korea

www.etri.re.kr

Since its foundation in 1976 with headquarters in Daejeon, ETRI, a non-profit government founded research institute, has been making its immense effort to provide Korea a remarkable growth in the field of ICT industry. ETRI delivers Korea as one of the top ICT nations in the World, by unceasingly developing world's first and best technologies, such as TDX-Exchange, Digital Mobile Telecommunication System (CDMA), etc.

Media Sponsor

FCW

1105 Media, Inc.
8609 Westwood Center Drive, Suite 500
Vienna, VA 22182
www.FCW.com

Celebrating 26 years, FCW, a media brand published by 1105 Government Information Group, provides federal technology executives with the information, insights, and strategies necessary to successfully navigate the complex world of federal business. FCW delivers the "who" and "what" federal executives need to know to get their jobs done effectively and make IT purchasing decisions. www.fcw.com

Media Sponsor

FierceGovernmentIT

ADDRESS
www.fiercegovernmentIT.com

FierceGovernmentIT tracks the latest technological developments in the U.S. government. Federal employees and IT executives rely on our website and free email newsletter for news on cybersecurity, defense IT, network communication systems, open government and other IT advances implemented by government agencies. Our news coverage is not limited to the daily headlines - our editors produce comprehensive features on leading trends and innovators. As part of our community, get insights on cutting-edge technologies through our exclusive webinars and robust whitepaper library. Join thousands of your peers by signing up for to FierceGovernmentIT today!

Media Sponsor

Global Security Magazine

SIMP, 17, av. Marcelin Berthelot, 92320
Châtillon, France
www.globalsecuritymag.fr

Global Security Mag is a quarterly magazine & website in French & English targeting on IT Security. Global Security Magazine is a Logical & Physical IT Security Magazine circulated to 5,000 decision makers, typically CSO. We have daily online information in English & French at: www.globalsecuritymag.com & www.globalsecuritymag.fr and in newsletters. On the 18 Marc 2014, we have organised the 6th annual GS DAYS, the francophone Security days is a conference in French on Ethical hacking, www.gsdays.fr. For more information, please email : ipsimp@free.fr or marc.jacob@globalsecuritymag.com

Media Sponsor

The Green Sheet, Inc.

1160 N. Sutton Ave., Suite 200, Santa Rosa, CA 94501
www.greensheet.com

Dedicated to the education and success of the ISO and MLS, *The Green Sheet* is a semi-monthly resource replete with timely, bias-free coverage of the evolving payments industry. It has more than 25,000 readers who depend on its regular, special and recurring features for information, education and inspiration.

Media Sponsor

Healthcare IT News

ADDRESS
www.healthcareITnews.com

Healthcare IT News offers healthcare IT executives timely, pertinent news every month. Jesse H. Neal Award Winning coverage includes new technologies, IT strategies and tactics, statutory and regulatory issues, as well as provider and vendor updates. Published in partnership with HIMSS, Healthcare IT News is the industry's only newspaper, reaching more than 54,000 subscribers, including IT management, C-suite and general management, and clinical executives at hospitals and IDNs, group practices, ambulatory care facilities, home healthcare organizations, as well as healthcare payers, consultants and vendors.

Media Sponsor

HomelandSecurityToday.US

www.HSToday.US

Homeland Security Today, the leading monthly magazine on homeland security, looks beyond other media to reveal and analyze what is going on behind the scenes. From top national decisionmakers to first responders, Homeland Security Today covers the entire homeland security community. Its global network of correspondents delivers original insight and analysis through its magazine, website, and daily e-newsletters. Homeland Security Today is proud recipient of multiple awards from the American Society of Business Publication Editors. Register for your complimentary subscription at www.HSToday.us.

Media Sponsor

NASCIO

201 East Main St, Suite 1405, Lexington, KY 40507
www.NASCIO.org

NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy. Founded in 1969, the National Association of State Chief Information Officers (NASCIO) is a nonprofit, 501(c)3 association representing state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia. The primary state members are senior officials from state government who have executive-level and statewide responsibility for information technology leadership. State officials who are involved in agency level information technology management may participate as associate members. Representatives from federal, municipal, international government and non-profit organizations may also participate as members. Private-sector firms join as corporate members and participate in the Corporate Leadership Council.

Media Sponsor

OASIS

ADDRESS

www.oasis-open.org

OASIS is a non-profit consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for security, Cloud computing, SOA, Web services, the Smart Grid, electronic publishing, emergency management, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology. The consortium has more than 5,000 participants representing over 600 organizations and individual members in more than 65 countries.

Booth 1

Plasma Ruggedized Solutions

2284 Ringwood Avenue, Suite A, San Jose, CA 92649

www.plasmarugged.com

Plasma Ruggedized Solutions is a leading service provider of custom engineering solutions and we offer conformal coating, potting/encapsulation, underfill services using a variety of materials and plasma ionized gas and cleaning pre-treatments designed to help achieve better adhesion between materials and substrates allowing for a more robust application. With FIPS compliance certification becoming increasingly important throughout the industry, Plasma Ruggedized Solutions offers a number of processes to give your products full FIPS compliance, we offer expert assistance from the design and engineering stage through the completion of FIPS certification.

Booth 6

Riscure North America

71 Steven Street, #400, San Francsico, CA 94105

www.riscure.com

Riscure is an international and independent security test laboratory founded in 2001 by Marc Witteman, with labs in the USA and in The Netherlands. Riscure is an

accredited lab for EMVco security testing, DPA lock testing and various Pay TV schemes. Riscure specializes in evaluating and testing the security of embedded devices that are designed to operate securely in any environment and under all circumstances. Besides offering these services, Riscure develops and maintains security test tools for organizations and companies that want to perform in-house security testing, such as side channel analysis or fault injection.

Conference Bag Sponsor

SafeLogic

530 Lytton Avenue, Palo Alto, CA 94301

www.safelogic.com

SafeLogic provides the most comprehensive set of software and services to minimize time and complexity of achieving FIPS 140 validation. SafeLogic was spun out from Apex Assurance Group, which has provided FIPS 140 consulting services to top companies for over eight years. Leveraging that experience, SafeLogic has built cryptographic modules that are easy to integrate, reduce time to compliance, have consistent APIs across multiple environments, and meet strict compliance requirements (including FIPS 140-2 and Suite B). SafeLogic is privately held and is headquartered in Palo Alto, CA.

Booth 2

Safenet Inc.

4690 Milennium Drive, Belbamp, MD 21017

www.safenet-inc.com

SafeNet is one of the largest data security companies in the world, and is trusted to provide data protection solutions to the most sensitive data for market-leading organizations around the globe. Our data protection solutions ensure high value information is secure throughout its' lifecycle, providing data security from the data center to the cloud.

Media Sponsor

Secure Identity Alliance

8 Rue Bayard,75008 Paris,France

www.secureidentityalliance.org

The Secure Identity Alliance is committed to helping public bodies across the world deliver eGovernment services to citizens through the widespread adoption of secure eDocument technologies. Addressing issues of data security, citizen privacy, identity and authentication, the Alliance offers leadership and advisory services to allow governments, agencies and other public bodies to realize the opportunities, and reduce the risks, of today's shift to digital service provision. From identifying best practice and uncovering new technologies through to standardization and certification, the Secure Identity Alliance brings together stakeholders from across the industry to inject meaningful debate and to accelerate adoption of the secure access and authentication solutions that will drive eGovernment forward, both now and in the future.

Booth 13

Secure-IC

1012 Crestview Drive, Milbsae, CA 94030

http://secure-ic.com

Secure-IC develops trusted computing security technologies for embedded systems to protect them from malevolent attacks and cyber threats. Working with top scientists in the field, we are thought leaders in the cyber security domain with best-of-breed technologies that assess the vulnerability of any embedded system and IP-cores that protect hardware products from state-of-the-art attacks.

Media Sponsor

Smart Insights

9-13 rue Bel Air, 13006 Marseille, France

www.smartinsights.net

Smart Insights is the best information source on the Secure Transactions industry. Smart Insights Weekly is a newsletter covering the smart card industry, its businesses, its technologies, its markets as well as its technology suppliers. Smart Insights covers all the major trends in the industry, it encompasses worldwide business, standardization bodies ... Smart Insights Reports are research reports providing key facts and figures as well as strategic insights about a technology, an area or a major issue in the secure transaction industry. Smart Insights Reports bring business modeling, forecasting and competitive analysis. Smart Insights: facts . intelligence . now . More information at www.smartinsights.net

Media Sponsor

Smart Payment Association

PO Box 800729, D-81607 Munich,Germany

www.smartpaymentassociation.com

The Smart Payment Association (SPA) addresses the challenges of the evolving payment ecosystem, offering leadership and expert guidance to help its members and their financial institution customers realize the opportunities of smart, secure and personalized payment systems & services both now and for the future. The SPA works in partnership with global standards bodies, its own vendor community, and an expanding ecosystem of established and emerging brands offering an ever-growing portfolio of advisory and support services including the market's most accurate barometer of payment trends based on actual manufacturer sales data and an eye-growing library of expert technical resources and thought leadership collaterals.

Booth 11

Thales e-Security

900 S. Pine Island Road, Suite 710, Plantation, FL 33324

www.thales-esecurity.com

Thales e-Security is a leading global provider of data protection solutions with more than 40 years of experience securing the world's most sensitive information. Thales customers —businesses, governments and technology vendors with a broad range of challenges—use our products and services to improve the security of applications that rely on encryption and digital signatures. By protecting the confidentiality, integrity, and availability of sensitive information that flows through today's traditional, virtualized and cloud-based infrastructures, Thales helps organizations reduce risk, demonstrate compliance, enhance agility and pursue strategic goals with greater confidence. Thales solutions not only deliver high levels of assurance, backed by independent certifications, but also offer significant advantages in ease of deployment and ongoing management.

Media Sponsor

Trusted Computing Group

3855 SW 153rd Drive, Beaverton, Oregon 97006

www.trustedcomputinggroup.org

Trusted Computing Group develops, defines and promotes open, vendor-neutral, global industry standards based on a hardware root of trust, for interoperable trusted computing platforms. Billions of endpoints use TCG standards to ensure system integrity, protect networks and secure data. For more information, see www.trustedcomputinggroup.org and on Twitter and LinkedIn.

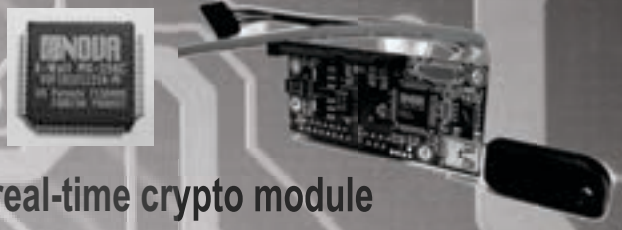
Conference Registrants (as of September 16)

Admir Abdurahmanovic, VP, PrimeKey Solutions AB
Arnold Abromeit, Lab Manager, TUV Informationstechnik GmbH
Dawn Adams, Lab Manager, EWA-Canada
Ojo Ishola Akintelure, ONDO STATE MINISTRY OF HEALTH
Michael Albert, IT Security Engineer, CSEC
Daniel Ambrosich, Principle Systems Engineer, Security Lead, Oracle
Jason Beloro, Security Lead, Oracle
Randy Bowman, SafeNet, SafeNet
Greg Boyd, I/T Specialist, IBM
Jennifer Brady, ICSA Labs
Chris Brych, Manager, Security Certifications, SafeNet, Inc.
Robert Burns, Security Principal, Thales e-Security
Richard Carter, Software Engineer, Cambium Networks
Peter Catherwood, Security Engineer, Thales e Security Ltd
Sooyoung Chae, Principal Member of Engineering Staff, NSRI
Hai-May Chao, Principal Software Engineer, Oracle
Myeong Choi, Sr. Product Manager, Giesecke & Devrient America Inc
Linda Ciabatoni, Consultant, Good Technology
Erin Connor, Director, EWA-Canada
David Cornwell, Technical Director, SAIC
Tom DaMario, Project Engineer, UL LLC
Elke Demulder, Crytography Research
Jatin Deshpande, Sr. Technical Account Manager, Giesecke & Devrient America Inc
Martin Downs, Penumbra Security, Inc.
Silvio Dragone, IBM Research - Zurich
Bertrand Du Castel, Schlumberger Fellow, Schlumberger
Randall Easter, Director, CMVP, NIST
Scott Ellett, Principal Software Engineer, Oracle
Andreas Fabis, atsec Information Security Corporation
Wajdi Feghali, Intel
Valerie Fenwick, Manager, Software Development, Oracle Solaris Security
John Ferris, President, Ferris&Associates, Inc.
Jim Fox, NIST
Carolyn French, IT Security Engineer, CSEC
Neng Gao, Associate Professor,Ph.D., Institute of Information Engineering,CAS
Shunxian Gao, CEC Huada Eletronic Design Co., Ltd.
Mike Gardiner, SafeNet, SafeNet
Shawn Geddis, Enterprise Security Consulting Engineer, Apple Inc.
Nicholas Goble, CGI Global Labs
Juan Gonzalez Nieto, FIPS 140-2 Technical Manager, BAE Systems Detica
Gilbert Goodwill, Senior Principle Engineer, DPA Software and Traini, Cryptography Research
Alan Gornall, Principal Consultant, Rycombe Consulting
Christophe Goyet, Technical Marketing Director, Oberthur Technologies
Jon Green, Aruba Networks
Sylvain Guilley, Secure-IC
Tim Hall, NIST
James Hallman, Design Manager, Atmel Corp
Mark Hanson, Sr. Program Manager, McAfee, Inc.
Randall Hart, Senior Research Scientist, Battelle Memorial Institute
Maarit Hietalahti, Senior Specialist, Audits and Accreditation, Finnish Communications Regulatory Authority FICORA
Wes Higaki, COO, SafeLogic
Sungmin Hong, Senior Engineer, Samsung
Elizabeth Hsu, Director, TUViT Informationstechnik GmbH
Soojin Huh, Professor, University of Ulsan
Marc Ireland, FIPS Program Manager, InfoGard Laboratories, Inc.
Moran Jacuel, Software Engineer, ARX
Joshua Jaffe, Cryptography Research
Jiwu Jing, Professor,Ph.D.,Chief Engineer, Institute of Information Engineering,CAS
Darryl Johnson, Lead Security Engineer, Corsec Security, Inc.
David Kaplan, Security Architect, AMD
Yasuhiko Kawai, Security Evaluator, Information Technology Security Center
Henrique Kawakami, CTO, Kryptus Information Security
Matthew Keller, VP, Corsec Security Inc.
Sharon Keller, NIST
Gary Kenworthy, Senior Principal Engineer - Digital Signal Process, Crytography Research
Wolfgang Killmann, T-Systems
SungDuk Kim, koscom
Yongdae Kim, The Attached Institute of ETRI
Junichi Kondo, Director, JCMVP, IPA
Rohit Kothari, Senior Engineer, Samsung Telecommunications America
Shriram Krishnan, Senior Director, Product Management and Ecosystem, Good Technology
Helmut Kurth, Chief Scientist, atsec Information Security Corporation
Matt Landrock, Director, Cryptomathic
Salvatore Le Pietra, CEO, atsec Information Security Corporation
Eugene Liderman, Director of Public Sector, Good Technology
Chia-Hung Lin, Director, Telecom Technology Center
Jingqiang Lin, State Key Laboratory of Information Security, Inst
Jian Liu, State Key Laboratory of Information Security, Inst
Jianfeng Liu, CEC Huada Eletronic Design Co., Ltd.
Limin Liu, State Key Laboratory of Information Security, Inst

Yan Liu, Principal Consultant, atsec Information Security Corporation
Claire Loiseaux, President, Trusted Labs
Sally Long, Director, Open Group Trusted Technology Forum
Yi Mao, Principal Consultant, atsec Information Security Corporation
John Marchioni, VP Business Development, ARX
Alexander Mazuruc, Senior Software Developer, WinMagic Inc.
Mike Mccarl, Specialist, ICSA Labs
Matthew McGehee, Lab Manager, COACT, Inc.
David McGregor, Device Evaluation Manager, UL Transaction Security
James McLaughlin, Product Manager, Gemalto
Michael Mehlberg, Vice President of Sales and Product Management, Microsemi
Chris Mitchell, Professor, Royal Holloway
Ken Modeste, Principal Engineer, UL LLC
Darren Moffat, Senior Principal Software Engineer, Oracle Solaris Security
Edward Morris, Co-Founder, Gossamer Security Solutions, Inc.
John Morris, President, Corsec
Philip Moylan, Director, Business Development Cyber Soultions, ViaSat, Inc.
Robert Nguyen, Secure-IC
Martin Oczko, Product Manager, PrimeKey Labs
Bob Oerlemans, Director of R&D Embedded HW, INSIDE Secure
Micahel Osborne, Innovation Services RSM, IBM Research - Zurich
Trisha Paine, SafeNet
Wuqing Pan, State Key Laboratory of Information Security, Inst
Sangwoo Park, The Attached Institute of ETRI
Fiona Pattinson, Director of Strategy & Business Development, atsec Information Security Corporation
Brian Pleffner, Lab Manager, CSC
Ray Potter, CEO and Co-founder, SafeLogic
Jean-Jacques Quisquater, Professor at UCL and Designer of Secure Smart Card, UCL Crypto Group
Emily Ratliff, Security Architect, AMD
Jason Reeves, Dartmouth College
Anthony Rink, VP of Sales, Rocstor Inc.
Allen Roginsky, NIST
Pankaj Rohatgi, Director of Engineering, Cryptography Research
William Rutledge, Director, Cnxtd inc.
Wewew S, ewer
Gen'Ya Sakurai, Information-technology Promotion Agency, Japan
Rory Saunders, Sr. Security Analyst, Coact, Inc
Laurent Sauvage, Secure-IC
Kim Schaffer, CMVP, NIST
Steven Schmalz, Security Solution Architect, RSA The Security Division if EMC
Hongsong Shi, CNITSEC
Trupti Shiralkar, Deputy Cryptographic Security Testing Lab Manager, atsec Information Security Corporation
Stan Skowronek, Bloomberg
Bill Smith, Manager, Security Engineering, Citrix
Jonathan Smith, CygnaCom Solutions
Sean Smith, Dartmouth College
David Sodeinde, SENIOR FIELD ENGINEER, WECO SYSTEMS INTERNATIONAL
Desiree Spann, AEGISOLVE
Travis Spann, AEGISOLVE
Bart Stevens, Director of Product Management, INSIDE Secure
William Supernor, CTO, KoolSpan, Inc.
Sander Temme, Sales Engineer, Thales e-Security
Hwee Li Thio, DSO National Laboratories
Mark Thomas, Systems Engineering Manager, Cambium Networks
Ryan Thomas, FIPS 140-2 Program Manager, CGI Global Labs
Tsun-Te Tsui, Telecom Technology Center
William Tung, CSTL Lab Manager, SAIC
Marcel Van Loon, Security Architect, INSIDE Secure
Jasper Van Woudenberg, CTO North America, Riscure
Paula VanDenberg, Technical Sales Manager, Plasma Ruggedized Solutions
Godfrey Vassallo, CTO, Sicore Technologies Inc.
Apostol Vassilev, NIST
Rajesh Velegalati, Research Intern, Riscure
Kyle Villano, Noblis
Tamas Visegrady, IBM Research - Zurich
Ashit Vora, Manager, Security Assurance, Cisco Systems, Inc.
Feiyu Wang, CEC Huada Eletronic Design Co., Ltd.
Yuewu Wang, Assistant Professor,Ph.D., Institute of Information Engineering,CAS
Zhe Wang, CEC Huada Eletronic Design Co., Ltd.
Robert Wann, President & CEO, Enova Technology Corporation
Patrick Warley, Global Head of R&D, Integral Memory
Ken Warren, Business Manager, Cryptography Research
David Weaver, Senior Principal Engineer, Oracle SPARC Hardware
Steve Weingart, Cryptographic and Security Testing Laboratory Mgr, atsec Information Security Corporation
David Wen, Chief Scientist, ECM Inc
Steve Weymann, Security Engineer, Infogard
Michael Woodring, Principal Hardware Engineer, SafeNet
Tatsuya Yanagisawa, Senior Security Engineer, ECSEC Laboratory Inc.
Ching Yu Henry Yip, DSO National Laboratories
Chris Zimman, Bloomberg

Protect Your Data; Safeguard Your Privacy®

X-Wall® MX



SATA-to-SATA FIPS 140-2 certified real-time crypto module

- FIPS 140-2 certifications – 1471 and 1472
- Generic host and device SATA interface – equipped with standard SATA interfaces operated on any SATA 1.0a/2.0/3.0 disk drive/SSD at a sustained 120MB/sec throughput.
- Low Power Consumption –advanced semiconductor technology that offers lower power consumption for power sensitive applications.
- Drive repurposing made easy – simply yank the key to avoid expensive drive erasing procedures as the encrypted content will be illegible.
- Keys Rotation – allows the drive to be encrypted with either the first or the 2nd Key interchangeably without taking the physical drive off line.

X-Wall® DX

USB to USB crypto processor with AES 256-bit hardware encryption

- NIST/CSE certified AES ECB & CBC 256-bit hardware engines
- Features 2-factor authentication and write protect
- Capable of encrypting full disk, any number of connected USB storage devices
- Capable of encrypting selective files/folders of any OS detectable storage drives, including boot drive, external drive such as USB or 1394, network attached storage and virtual drives such as Dropbox, SkyDrive and GoogleDrive.
- Compatible with USB1.1/2.0/3.0 interfaces
- Simple to use GUI of Windows and Macintosh; requires no software and/or driver download and installation

eNIGMA

USB pass-through dongle with AES 256-bit hardware encryption

eNIGMA 2

USB Hardware Crypto Module Securing Cloud Storage

eNOVA®

Enova Technology Corporation
1st Floor, #11, Research & Development 2 Road, Science
-based Industrial Park, Hsin-Chu City Taiwan 300, Republic of China
TEL: +886 (3) 577-2767 FAX: +886 (3) 577-2770 www.enovatech.com