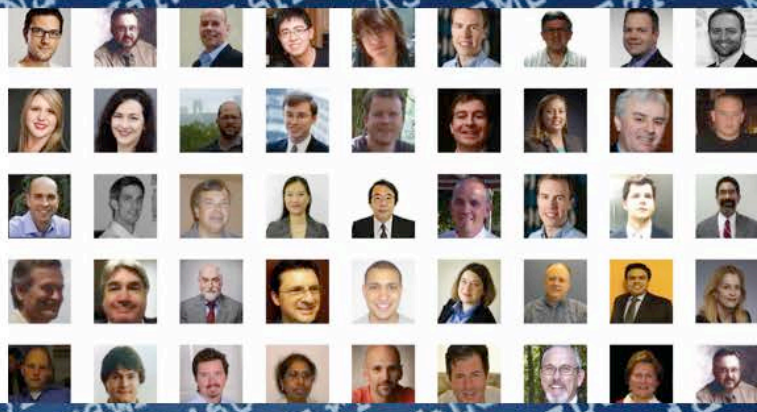
CONFERENCE PROGRAM

LEVEL 2 SPONSOR

utimaco®

THE SECOND

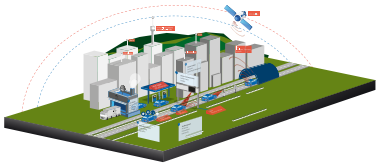
International Cryptographic Module Conference ICMC14



November 19–21, 2014 * Hilton, Washington, D.C.

utimaco®

We keep your cryptographic keys safe



Automotive

Key Generation • PKI Services
Code Signing • Authentication Services
Digital Rights Management

Energy

Meter Manufacture • Key Injection
Key Generation • Birth Certificate
Key Management

hsm.utimaco.com

Welcome

Dear ICMC 2014 Participant,

The ICMC Program Committee personally welcomes you to the Second Annual International Cryptographic Module Conference (ICMC). We are excited to share with you the workshops and presentations from government, academia, product developers, laboratories, consultants and industry leaders. I would like to give you an idea of what to expect in the next three days.

Day one consists of workshops and presentations related to the ISO 19790 and ISO 24759.

Day two starts with Keynote speeches and presentations on three tracks: Certification Programs, General Technology and Advanced Technology. Exhibit area opens this day. At the end of the day, we invite you to join us for a reception.

Day three brings presentations on two tracks: Certification Programs and General Technology. Conference concludes with a closing remarks. Exhibits are open till 15:30.

We hope this conference will enable open discussions, exchange of ideas and provide many opportunities to network.

Thank you for being a part of this exciting conference and sharing your experience and ideas. We are tremendously encouraged by your participation and feedback. We will be requesting feedback and ideas on how we can continue to keep ICMC interesting and beneficial to all participants.

Our thanks to conference sponsors and exhibitors. We hope you will take some time to visit the booths.

Wishing you a very fruitful week.

Regards,

The ICMC 2014 Program Committee

Table of Contents

Contact Information

Program Committee

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

Nithya Rachamadugu, Director, Cygnacom

Erin Connor, Director, EWA-Canada

Conference Staff

Bill Rutledge, Project Management, 1.212.866.2169, bill.rutledge@icmconference.org

Andrew Baranich, Sales Manager, 1.609.316.6079, andrew@cnxtd.com

Nikki Principe, Operations Manager, 1.571.249.5680, nikki@cnxtd.com

Presented by CMUF

The Cryptographic Module User Forum (CMUF) provides a voice and communications channel between the community of unclassified cryptographic module (CM) and unclassified cryptographic algorithm developers, vendors, test labs and other interested parties, and the various national, international, and multi-lateral organizational committees, schemes, and policy makers. Join the Forum at cmuf.org.

Sponsoring Organizations

Event Sponsors & Exhibitors

LEVEL 2 SPONSOR

OPENING LUNCH SPONSOR

BAG SPONSOR

BADGE SPONSOR

EVENT SPONSOR

Exhibitors

Association & Media Sponsors

Conference Agenda

Pre-Conference Workshop

Wednesday, November 19

Workshop Sessions

Plaza 2-3

9:00 **Explaining the ISO 19790 Standard** *Randall Easter, NIST, Security Testing, Validation, and Management Group*

10:30 **Coffee Break**

10:45 **Explaining the ISO 19790 Standard** *Continued Randall Easter, NIST, Security Testing, Validation, and Management Group*

12:15 **Lunch**

13:15 **Comparing ISO/IEC 19790 and FIPS PUB 140-2** *William Tung, Cryptographic and Security Testing Laboratory's (CSTL) Laboratory Manager, Leidos; Zhiqiang (Richard) Wang, Cryptographic & Security Test Lab (CSTL) Sr. Security Engineer, Leidos*

14:45 **Break**

15:00 **Questions to CMVP (NIST/CSEC) on ISO 19790 Standard, 140-4 or Any Other** *Randall Easter, NIST, Security Testing, Validation, and Management Group; Allen Roginsky, Mathematician, NIST, Carolyn French, Manager, CMVP, CSEC and Sharon Keller, Director, Cryptographic Algorithm Validation Program (CAVP), NIST*

15:45 **Status of the Transition to New Algorithms and Stronger Keys** *Allen Roginsky, Mathematician, NIST*

Thursday Opening Lunch

Sponsored by

ORACLE

Conference Sessions

Thursday, November 20

Plenary Keynote Presentations

Plaza 1-3

8:00 **Registration and Coffee**

9:00 **Welcome & Introduction**

9:15 **Random Thoughts** *Helmut Kurth, Chief Scientist, atsec information security*

9:45 **Is Anybody Listening? Business Issues in Cryptographic Implementations** *Mary Ann Davidson, Chief Security Officer, Oracle Corp.*

10:15 **Break, Exhibits Open**

Track Sessions

Certification Programs Track

Plaza 2

11:00 **Roadmap to testing of new algorithms** *Sharon Keller, Director, Cryptographic Algorithm Validation Program (CAVP), NIST*

11:45 **FIPS 140-Next Is Coming: What Does It Mean and What Are You Going To Do?** *Tony Busciglio, Laboratory Manager, Acumen Security*

12:30 **Lunch in Exhibit Hall** *Lunchtime Meeting of the Cryptographic Module User Forum (CMUF) in Plaza 2*

13:45 **Making Diamonds Out of Coal: CST Labs Are Under Pressure** *Yi Mao, Principal Consultant, atsec*

14:30 **Navigating the Minefield as an Operating System Vendor and FIPS-140 Newbie** *Darren Moffat, Senior Principal Engineer, Solaris; Valerie Fenwick, Software Engineering Manager, Oracle*

15:15 **Break in Exhibit Area**

15:45 **Results of a Research Effort in Response to New Entropy Standards** *Ray Potter, CEO & Co-Founder, SafeLogic*

16:30 **Help! I'm Bricked and Can't Zero My CSPs!** *Tammy Green, Senior Security Architect & Vulnerability Response Director, Blue Coat Systems*

17:15 **Networking Reception in Exhibit Area**

Track Sessions (Cont'd)

Thursday, November 20

General Technology Track

Plaza 3

11:00 **ID Suite B Cryptography and Commercial Solutions for Classified: A Primer** *Jon Green, CTO Aruba Networks Government Solutions*

11:45 **FIPS 140-2 Implementation Guidance 9.10: What is a Software Library and How to Engineer It for Compliance?** *Apostol Vassilev, Cybersecurity Expert, Computer Security Division, NIST, Staff Member, CMVP*

12:30 **Lunch in Exhibit Hall**
Lunchtime Meeting of the Cryptographic Module User Forum (CMUF) in Plaza 2

13:45 **PKCS#11: Breathing New Life Into a Beloved Cryptographic Standard** *Valerie Fenwick, Software Engineering Manager, Oracle*

14:30 **A Study on the Interoperability of Certification for Commercial Cryptographic Module Validation** *Neng Gao, Associate Professor, Institute of Information Engineering, Chinese Academy of Sciences*

15:15 **Networking Break in Exhibit Hall**

15:45 **FIPS 140-2 Compliance of Industry Protocols in 2015 and 2016,** *Edward Morris, Co-Founder, Gossamer Security Solutions*

16:30 **Panel Discussion: ISO/IEC 19790 Editors**

Moderator: *Fiona Pattinson, Director, Strategy & Business Development, atsec,* **Panelists:** *Randall Easter, NIST, Security Testing, Validation, and Management Group; Junichi Kondo, Director, JCMVP, IPA; Jean-Pierre Quémard, Head of Sales Aeronautics & Space, Cassidean; Dr. Gen'ya Sakurai, JCMVP, IPA*

17:15 **Networking Reception in Exhibit Hall**

Advanced Technology Track

Plaza 1

11:00 **Tamper Event Detection on Distributed Devices in Critical Infrastructure** *Jason Reeves, Graduate Student, Dartmouth College*

11:45 **MRS: Tamper-Respondent Meshes** *Moisés Riesgo Suárez, Evaluator, Epoche & Espri*

12:30 **Lunch in Exhibit Hall**
Lunchtime Meeting of the Cryptographic Module User Forum (CMUF) in Plaza 2

13:45 **Cryptographic Side-Channel Analysis on the Primary Side of Switching-Mode Power Supplies** *Sami Saab, Principal Field Applications Engineer, Cryptography Research*

14:30 **SLEAK: A Side-Channel Leakage Evaluator and Analysis Kit** *Dan Walters, Digital/Micro HW Engineer, MITRE*

15:15 **Networking Break in Exhibit Hall**

15:45 **Validating Sub-Chip Modules and Partial Cryptographic Accelerators,** *Carolyn French, Manager, CMVP, CSEC and Randall Easter, NIST, Security Testing, Validation, and Management Group*

16:30 **SE, TEE, HCE: Making Sense of the Security of Cryptography in Your Phone,** *Jasper van Woudenberg, CTO North America, Riscure and Marc Witteman, CTO, Riscure*

17:15 **Networking Reception in Exhibit Hall**

Conference Presentations

Presentations will be available after the conference at www.ICMConference.org

Password: *******

WiFi Access

WiFi service is available to conference registrants in the public areas of the hotel.
User Name: **hilton14**
Password: **plaza14**

Track Sessions

Friday, November 21

Certification Programs Track

Plaza 2

8:30 **Registration and Coffee in Exhibit Hall**

9:00 **Guidelines for Concurrent FIPS 140-2 and ISO/IEC 19790 Validations** *Luis Alfonso Garcia, IT Security Engineer, Epoche & Espri*

9:45 **Shoehorning Software Modules into FIPS 140-2** *Luis Alfonso Garcia, IT Security Engineer, Epoche & Espri*

10:30 **Break in Exhibit Hall**

11:00 **CMVP Programmatic Status** *Michael Cooper, NIST and Carolyn French, Manager, CMVP, CSEC*

11:45 **NIST SP 800-90 Series** *Allen Roginsky, Mathematician, NIST*

12:30 **Lunch in Exhibit Hall**

13:30 **NIST SP 800-131A Transition** *Chris Byrch, Senior Principal Security Analyst, Oracle Security Evaluations*

14:15 **NIAP--Recent Updates** *Janine Pederson, Director, NIAP, NSA/CSS Commercial Solutions Center*

15:00 **Break in Exhibit Hall** (Exhibit Hall Closes at 15:30)

15:30 **Summary & Wrap-Up**

16:15 **Conference Adjourns**

General Technology Track

Plaza 3

8:30 **Registration and Coffee in Exhibit Hall**

9:00 **Heartbleed, Best Practices and Why Are There Still Buffer Overflow Attacks?** *Steve Weingart, Public Sector Certifications, Aruba Networks*

9:45 **Validation of Cryptographic Protocol Implementations** *Juan Gonzalez Nieto, Technical Manager, BAE Systems Applied Intelligence*

10:30 **Break in Exhibit Hall**

11:00 **Entropy–A FIPS and Common Criteria Perspective Including SP 800-90B** *Gary Grainger, AT&E Technical Director, Leidos*

11:45 **Entropy Sources–Recommendations for a Scalable, Repeatable and Comprehensive Evaluation Process** *Sonu Shankar, Software Engineer, Cisco Systems, Alicia Squires, Global Certifications Team – Manager, FIPS/Common Criteria, Cisco Systems, Ashit Vora, Lab Director and Co-Founder, Acumen Security*

12:30 **Lunch in Exhibit Hall**

13:30 **Implementing SM2 Cryptographic Module on Graphics Processing Units** *Jiwu Jing, Professor, Institute of Information Engineering, Chinese Academy of Sciences*

14:15 **Understanding FIPS Requirements for UC APL Listing Eligibility** *Kathleen Moyer, Project Management Engineer, Corsec Security*

15:00 **Break in Exhibit Hall** (Exhibit Hall Closes at 15:30)

15:30 **Summary & Wrap-Up**

16:15 **Conference Adjourns**

Speaker Biographies

Josh Brickman

PMP, Director, Security Evaluations, Oracle

Joshua Brickman, PMP (Project Management Professional), runs Oracle Corporation's Security Evaluations group. At Oracle, Josh and his team are responsible for all Common Criteria, FIPS and other security related certifications. Prior to Oracle, Josh led CA Technologies Federal Certifications Program for over six and a half years. While at CA, he led the successful evaluations of sixteen products through the Common Criteria (in both the U.S. and Canada). Brickman is a Steering Committee member and an original contributor to the Open Group Trusted Technology Provider Standard which is focused on Supply Chain Integrity and Security.

Tony Busciglio

Laboratory Manager, Acumen Security

Tony is Acumen Security's Co-founder and Laboratory Director. Prior to Acumen, Tony was a member of the Cisco certification team guiding product through both FIPS 140 and Common Criteria certifications. Before Cisco, Tony was both a Common Criteria Evaluator and CSTL Manager. With Acumen, Tony leverages his experiences as part of both a certification lab and product vendor to provide to provide the customers with the most effective and efficient product certifications.

Chris Byrch

Senior Principal Security Analyst, Oracle Security Evaluations

Chris recently joined Oracle's Security Assurance Group as a Senior Principal Security Analyst to support Oracle's global security evaluations. Chris has worked exclusively with the FIPS-140 Standard for almost 15 years now - on the Lab side testing cryptographic modules to FIPS 140-1 and FIPS 140-2 compliance, and on the vendor side – providing requirements to development teams to design products to meet FIPS 140-2 compliance. Prior to joining Oracle, Chris held various management positions at SafeNet, CGI, and DOMUS IT Security Laboratory.

Erin Connor

Director, EWA-Canada

Erin is a Director at EWA-Canada with responsibility for EWA-Canada's Information Technology Security Evaluation & Testing Facility, which includes a Cryptographic Module Test Lab testing to FIPS 140-2 and ISO 19790 ("ISO FIPS"); a Common Criteria Test Lab; a Security Content Automation Protocol (SCAP) Test Lab; and a Payment Assurance lab that certifies Point-of-Sale devices, Unattended Payment Terminals and Hardware Security Modules to Payment Card Industry standards.

Michael Cooper

IT Specialist, NIST

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

Mary Ann Davidson

Chief Security Officer, Oracle

Mary Ann Davidson is the Chief Security Officer at Oracle Corporation, responsible for Oracle Software Security Assurance. She represents Oracle on the Board of Directors of the Information Technology Information Sharing and Analysis Center (IT-ISAC), and serves on the international board of the Information Systems Security Association (ISSA). She has been named one of Information Security's top five "Women of Vision," is a Federal 100 award recipient from Federal Computer Week, and was recently named to the ISSA Hall of Fame. She has

served on the Defense Science Board and as a member of the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency. She has testified on cybersecurity to the U.S. House of Representatives (Energy and Commerce Committee; Armed Services Committee; and Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology) and the U.S. Senate Committee on Commerce, Science and Technology.

Randall Easter

NIST, Security Testing, Validation, and Management Group

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.

Valerie Fenwick

Software Engineering Manager, Oracle

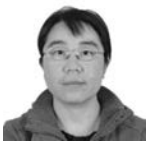
Valerie Anne Fenwick is a Software Engineering Manager at Oracle Corporation with over a decade of experience in computer security. Valerie is currently managing the Solaris Cryptographic Technologies team, of which she was a designer and major contributor. She was the lead for the Solaris Change Request 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. Valerie is co-chair of the OASIS PKCS11 technical committee.

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



Associate Professor, State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China

Neng Gao. is an Associate Professor at the Institute of Information Engineering at Chinese Academy of SciencesChris recently joined Oracle's Security Assurance Group as a Senior Principal Security Analyst to support Oracle's global security evaluations.

Luis Alfonso Garcia

IT Security Engineer, Epoche & Espri

Luis A. García Sánchez, graduated in computer science, has worked in areas related to the information system development, IT products security evaluation under CC standard, ISO-19790 and FIPS 140-2 conformance testing of cryptographic modules. Luis is a senior CC evaluator, ISO-19790 and FIPS 140-2 tester in Epoche and Espri since July 2011, and his main involvement with the security evaluations comes from participating as pen-tester, developing useful tools in order to carry out the

evaluations, such as, script or exploit and helping in the development of the lab AVA_VAN methodology. Luis has been involved in over 15 security evaluations with several assurance levels from EAL1 to EAL4 + AVA_VAN.5 and in the conformance testing process of several cryptographic modules under FIPS and ISO/IEC 19790 validation.

Dave Gerendas

Group Product Manager, McAfee

Dave Gerendas is Group Product Manager for McAfee.

Dr. Gary Grainger

AT&E Technical Director, Leidos

As an evaluator with 15 years of experience, Dr. Grainger analyzes and tests the security properties of commercial products including firewalls, network devices, web applications, operating systems, hypervisors, and public key infrastructure (PKI) systems. Evaluation work involves analysis of security designs along with identifying, learning, and applying security testing tools such as network scanners, traffic sniffers, vulnerability scanners, and cryptographic applications. Dr. Grainger has worked as an evaluator, information technology (IT) security professional, Mathematician, and developer. His IT security experience includes research into using system management mode (SMM) of Intel processors to detect and prevent kernel-level attacks. This work was part of two Small Business Innovation Research (SBIR) awards, for which Dr. Grainger was Principal Investigator. Dr. Grainger earned a Bachelor's in Mathematics from George Mason University and a Ph.D in Mathematics from the University of Arizona.

Jon Green

CTO, Aruba Networks Government Solutions

Jon Green, CISSP, is CTO of Aruba Networks Government Solutions, which ensures that Aruba's commercial solutions meet the high security requirements of government customers worldwide. Jon joined Aruba Networks in 2003 and helped it grow from a small startup to today's position as a leading provider of network mobility solutions. Prior to Aruba, Jon held technical, marketing, and sales positions with Foundry Networks, Atrica, Nortel Networks, and Bay Networks. Jon holds a BS in Information Security from Western Governor's University and is will graduate in 2015 with a MS in Computer Science and Information Security from James Madison University. When not playing with technology, he enjoys flying airplanes, making wine, and cooking competition barbecue.

Tammy Green

Senior Security Architect & Vulnerability Response Director, Blue Coat Systems

Tammy Green is the Senior Security and Certification Architect at Blue Coat Systems. She is responsible for preparing products for government certifications, and leading the engineering teams through the certification process. She is also responsible for product security and vulnerability response. Tammy has more than 15 years of experience in security field. She has a Master's degree in Computer Science from Carnegie Mellon University, and a Bachelor's degree in Computer Engineering from Tulane University.

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.

Jiwu Jing

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

Jiwu Jing is a Professor at the Institute of Information Engineering, Chinese Academy of Sciences.

Sharon Keller

Director, Cryptographic Algorithm Validation Program (CAVP), 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.

Junichi Kondo

Director, JCMVP, IPA

Junichi Kondo is the Director of Japan Cryptographic Module Validation Program. He is responsible for the cryptographic module validation scheme based on ISO/IEC 19790 and also responsible for the hardware CC certification scheme in Japan. He holds the Master degree of Engineering in Electrical Engineering from Kyoto University. He worked for Mitsubishi Electric Corporation for 29 years and developed various hardware products.

Helmut Kurth

Chief Scientist, atsec

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.

David MacFarlane

Senior Director, Security Assurance, Blackberry

David is a founding member of the BlackBerry Security business unit that has made the transparency of BlackBerry security solutions its single biggest differentiator in enterprise and consumer markets. His current mandate is to build confidence in the BlackBerry security ecosystem by reducing the threat of malicious or privacy-infringing applications; automated operations and vulnerability analysis; and obtaining security approvals and certifications of BlackBerry products.

Yi Mao

Principal Consultant, CST Lab Manager, atsec

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.

Cyber Security Requires Forward Thinking

PROPEL YOUR PRODUCT TO THE FEDERAL MARKET

Navigating the cumbersome product validation requirements is a challenge for product vendors. Leidos tackles that challenge, enabling our customers to apply forward thinking to their next generation of products.

The Leidos Accreditation Testing and Evaluation (AT&E) Laboratory is one of the only labs to offer a comprehensive menu of services in the Common Criteria, Cryptography Security and Testing, and FedRAMP arenas. Our exceptional processes for efficiency and reliability empower our customers with an expedited transition of their products into the federal marketspace.

To learn more, email at **ate@leidos.com**
or visit **leidos.com/ate**

leidos

© Leidos. All rights reserved.

Darren Moffat

Senior Principal Engineer, Solaris

Darren is a Senior Principal Engineer in the Solaris Core Technologies 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).

Ed 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.

Kathleen Moyer

Project Management Engineer, Corsec Security

Kathleen Moyer is a Project Management Engineer with Corsec Security and has experience in Corsec's Common Criteria, FIPS, and UC APL business units. Kathleen brings a background in cryptographic module validations, security product certifications, and DoD intelligence systems and a Master's degree in electrical engineering to work in assisting and guiding companies through their enterprise certification efforts.

Juan Gonzalez Nieto

Principal Consultant, BAE Systems Applied Intelligence

Juan is the Technical Manager of the BAE Systems Applied Intelligence's Cryptographic and Security Testing Lab in Canberra (Australia), where he is in charge of ensuring the highest quality in the testing of cryptographic products and related activities. Juan has over fourteen years' experience in ICT security, including research and consultancy services. Juan has a PhD in Cryptography and an extensive track record on applied cryptography and computer security research, having published extensively in these areas.

Fiona Pattinson

Director Strategy & 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.

Janine Pederson

Director, NIAP, NSA/CSS Commercial Solutions Center

Janine Stadter Pedersen is the Director, National Information Assurance Partnership (NIAP) established to evaluate IT product conformance to international standards. The program is a partnership between the public and private sectors and is implemented to help consumers select COTS ICT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace. Janine has served as the Technical Advisor for the Office of Community

Outreach, which included the Committee on National Security Systems (CNSS) Secretariat, worldwide Information Assurance Community Outreach, National IA Policy, the National IA Education and Training programs, and Interagency OPSEC Support Center. Janine was a subject matter expert in developing COTS for SECRET, evolving it into the Commercial Solutions for Classified (CSfC) program. As Chief Validator for NIAP, Janine provided technical and strategic direction for the program, working closely with NIST, NSA, and international partners.

Ray Potter

CEO & Co-Founder, SafeLogic

Ray Potter is the CEO and Founder of SafeLogic. Under Ray's leadership, SafeLogic has developed encryption modules for a variety of platforms and technologies, including mobile, wearables, and Cloud. The co-author of FIPS 140 Demystified: An Introductory Guide for Vendors, Potter has been published in Information Security Magazine, leads the FIPS 140 Open Forum on LinkedIn, and has spoken at the RSA Conference, CTIA MobileCon, (ISC)2 Congress, Wearables DevCon, and the International Cryptographic Module Conference.

Nithya Rachamadugu

Director, Cygnacom

Ms. Rachamadugu leads the Certification laboratories at Cygnacom Solution. She is the Director of CygnaCom's Common Criteria and FIPS 140-2 Government accredited labs and is responsible for all aspects of running the labs. CygnaCom Labs evaluate hardware/software/firmware for conformance to US Govt and International standards (NIST and NIAP, TSE and soon CSEC). She is qualified to perform cryptographic module validation to the FIPS 140-2 standard as well as Common Criteria evaluations. She conducts customer training classes and pre-assessment work-shops in the US and abroad. Ms. Rachamadugu regularly presents CC and FIPS relevant topics at international conferences.

Jason Reeves

Graduate Student, Dartmouth College

Jason Reeves is a PhD student and a member of the Trust Lab at Dartmouth College. He has been involved with the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) project since 2010, and his research includes designing intrusion and tamper detection systems for embedded devices within the smart grid. Prior to Dartmouth, he spent several years working as a programmer in the healthcare industry.

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.

Sami Saab

Principal Field Applications Engineer, Cryptography Research

Sami Saab has a B. Eng. and M.A.Sc. from the University of Victoria, with a background in digital filter design and signal processing. Before joining Cryptography Research in 2012, Sami worked in the telecom, IC, defense and embedded processing industries, working on sensor processing and controls problems. At CRI, Sami supports the DPA Workstation used by customers validating their countermeasure designs. Sami also performs analysis on various devices to ascertain inherent vulnerabilities to side-channel attacks.

Dr Gen'ya Sakurai
JCMVP, IPA

Sonu Shankar
Software Engineer, Cisco

Sonu Shankar joined Cisco's Threat Response, Intelligence and Development group in December 2011, working in the Global Certifications Team responsible for FIPS 140, Common Criteria as well as foreign government security evaluations. He works across a large part of the Cisco product portfolio to identify vulnerabilities, assess associated risk and design scalable solutions to fix them. Prior to his current position, Sonu was an early member in the Cisco TrustSec development team working on features in the area of MACSec, Role-Based Access Control and 802.1x authentication. Prior to joining Cisco in 2008, he was a Research Assistant at the Wireless Communication Laboratory at Texas A&M University where he worked on lower layer attack analysis in sensor networks.

Miles Smid
Cyber Security Consultant

Miles Smid provides computer security consulting services to government and industry. He specializes in cryptography, key management, and computer security standards development and implementation.

Alicia Squires
Global Certifications Team, Manager, FIPS/Common Criteria, Cisco

Alicia leads a team of engineers that keep Cisco's suite of products certified for FIPS and Common Criteria. Elected Chair of the Common Criteria Users Forum, which provides a voice and communications channel amongst the Common Criteria community including the vendors, consultants, testing laboratories, Common Criteria organizational committees, national schemes, policy makers, and other interested parties.

Marcus Streets
Director High Security Products, Good Technology

Marcus joined nCipher in 1997 shortly after the company was founded and worked on the FIPS 140-1 certification of its nShield product range achieving level 2 and level 3 certification the following year. For the next 15 years he managed the FIPS and Common Criteria programs at nCipher and its partners Neoscale and Brightstream and was also a key member of the product design team. He remained at nCipher after the takeover by Thales, but in 2012 left to join Good Technology as Director of High Security products. He has been involved in several cryptographic standards, he was one of the authors of the OASIS KMIP standard and is currently editor of the Global Platform TEE Trusted User Interface specification.

Moisés Riesgo Suarez
Evaluator, Epoche & Espri

Moisés Riesgo Suárez is an Electronic Engineer specialized in electronics and automation technology. He has worked in the analysis of hardware systems, IT products security evaluation under CC standard and FIPS 140-2 conformance testing of cryptographic modules. Moisés is a junior CC evaluator and FIPS 140-2 tester in Epoche and Espri, and his main involvement with the security evaluations comes from participating as junior pen-tester and exploit developer in CC security evaluations. He has been involved in security evaluations with several assurance levels from EAL1 to EAL4 + AVA_VAN.5 and has been especially involved in FIPS 140-2 hardware testing.

William Tung

Cryptographic and Security Testing Laboratory's (CSTL) Laboratory Manager, Leidos

Mr. William Tung works for the Accredited Testing and Evaluation (AT&E) division of Leidos as the Cryptographic and Security Testing Laboratory's (CSTL) Laboratory Manager, primarily responsible for FIPS 140-2 validations, FIPS 201/GSA testing, SCAP validation and TWIC testing. He has 10 years of computer security testing experience along with C&A activities. He earned his Bachelor's Degree in Computer Engineering from the University of Maryland, College Park.

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, 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.

Ashit Vora

Lab Director and Co-Founder Acumen Security

Ashit is the Co-founder and Laboratory Director of Acumen Security. Acumen provides consulting and evaluation services in the security certitications arena with offices in US and India. Before co-founding Acumen, Ashit led the FIPS and CC certification team at Cisco Systems, Inc. Ashit was responsible for enabling and protecting $2 billion in annual revenue. While at Cisco, Ashit instrumented changes to increase efficiency and certify more intelligently. Ashit's experience spans the gamut of IA and IA enabled products such as Routers, Switches, Firewalls, Data Center products, smart cards, and software applications. Ashit's areas of expertise include FIPS 140-2, Common Criteria, International crypto certification requirements, cryptography, and networking. He holds a Masters of Science degree from the University of Southern California (USC) and a Bachelors in Telecommunications Engineering from the University of Mumbai (India).

Dan Walters

Digital/Micro HW Engineer at MITRE

Dan Walters is a Lead Digital/Micro HW Engineer at MITRE in Electronic Systems Development. Dan has worked in the area of embedded systems and security since arriving at MITRE in 2006. He helped to develop MITRE's Secure Electronics Lab, which has advanced capabilities for researching implementation security issues such as side-channel leakage, fault induction, and trusted hardware. He is currently the principle investigator on a research project for developing tools to evaluate cryptographic software against implementation attacks.

Zhiqiang (Richard) Wang

Cryptographic & Security Test Lab (CSTL) Technical Director

Mr. Wang has been performing FIPS 140-2 and FIPS 201 product testing and evaluations for 8 years. Mr. Wang has tested various network Routers, Switches,

Software Modules and Wireless Controllers and Access Points. He continues to perform validation testing of FIPS 140-2 and 201 products while acting as a lead and oversight technical tester on active CSTL testing projects. Mr. Wang has performed testing on algorithm implementations to obtain required algorithm certificates from the Cryptographic Algorithm Validation Program (CAVP) for modules that are undergoing FIPS 140-2 testing. Mr. Wang earned his Bachelor's degree in Mechanical Engineering from Tianjin University in China and a Master's degree in Electrical Engineering from University of Nevada, Reno (UNR).

Steve Weingart

Public Sector Certifications, Aruba Networks

Steve Weingart, Manager of Public Sector Certifications at Aruba Networks, coordinates validation/certification/listing of Aruba's products under FIPS 140-2 and other standards. He received his BSEE in 1978 and has been working in security and cryptography since the early 1980s. While at IBM's T. J. Watson Research Center he joined the NIST working group that wrote FIPS 140-1 and was the lead hardware engineer on the first FIPS 140-1 level 4 module, the IBM 4758. Steve has remained in the security and security standards field as a developer of cryptographic products, physical security subsystems and as a security standards consultant, test engineer, laboratory manager and coordinator.

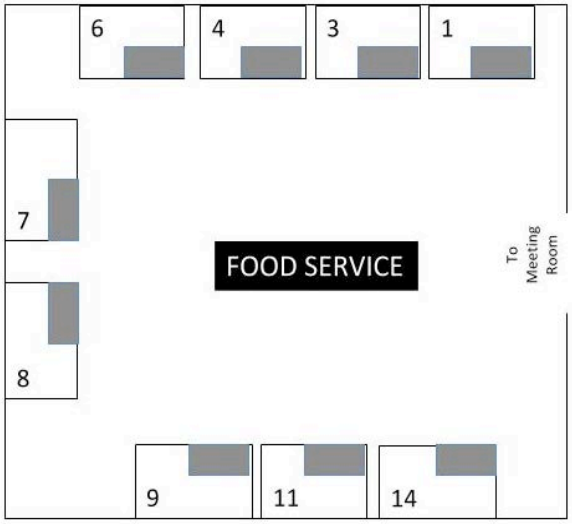
Marc Witteman

Founder, Riscure

Marc Witteman has a long track record in the security industry. He has been involved with a variety of security projects for over two decades and worked on applications in mobile communications, payment industry, identification, and pay television. Recent work includes secure programming and fault injection. He has authored several articles on smart card and embedded device security issues. Further, he has extensive experience as a trainer, lecturing security topics for audiences ranging from novices to experts. In 2001 he founded Riscure, a security lab based in the Netherlands, which is now a leading security research center, and side channel test tool vendor. Today he is the Chief Technology Officer of Riscure Security Lab.

Exhibitors & Sponsors

Exhibit Floor Plan



Booth	Exhibitor
1	Cryptographic Module User Forum
3	Cryptography Research
4	Oracle
6	WolfSSL
7	Ultra Electronics, 3eTI
8	Secure-IC
9	atsec information security
11	Riscure
14	Utimaco

Booth 9

atsec information security

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.

Association Sponsor

Common Criteria User Forum

www.ccusersforum.org

The Common Criteria User Forum mission is to provide a voice and communications channel amongst the CC community including the vendors, consultants, testing laboratories, Common Criteria organizational committees, national schemes, policy makers, and other interested parties.

Association Sponsor, Booth 1

Cryptographic Module User Forum

www.cmuf.org

The Cryptographic Module User Forum (CMUF) provides a voice and communications channel between the community of unclassified cryptographic module (CM) and unclassified cryptographic algorithm developers, vendors, test labs and other interested parties, and the various national, international, and multi-lateral organizational

committees, schemes, and policy makers. Join the Forum at cmuf.org.

Booth 3

Cryptography Research

425 Market Street, 11th Floor
San Francisco, CA 94105
www.cryptography.com

With more than 7 billion security products made under a license to our technologies each year, Cryptography Research, Inc. is the world's leading semiconductor security R&D and licensing company. Our specialty is solving complex data security problems, with a focus on helping industries eliminate fraud, piracy, counterfeiting, and other forms of abuse. Security systems designed by Cryptography Research engineers protect hundreds of billions of dollars of commerce annually. Cryptography Research develops and licenses innovative technologies in areas including tamper resistance, content protection, network security, and financial services. In addition, we perform security evaluations and provide specialized applied engineering services. Cryptography Research's clients include many of the world's leading technology and media delivery companies. The company was founded in 1995 by internationally renowned cryptographer Paul Kocher. Security systems designed by Cryptography Research engineers protect hundreds of billions of dollars of commerce annually for the government, wireless, telecommunications, financial, digital television, entertainment, consumer electronics, and Internet industries.

Media Sponsor

Global Security Magazine

www.GlobalSecurityMag.com

Global Security Magazine 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: ww.globalsecuritymag.com & www.globalsecuritymag.fr and in newsletters.

Media Sponsor

InfoSecurity Magazine

www.infosecurity-magazine.com

Infosecurity Magazine has almost ten years of experience providing knowledge and insight into the information security industry. Its multiple award winning editorial content provides compelling features both online and in print that focus on hot topics and trends, in-depth news analysis and opinion columns from industry experts. Infosecurity Magazine also provides free educational content, endorsed by all major industry accreditation bodies and is therefore considered a key learning resource for industry professionals.

Event Sponsor

Leidos

6841 Benjamin Franklin Drive
Columbia, MD 21046
www.leidos.com

CloudShield Technologies, a wholly owned subsidiary of Leidos, has been a leading innovator in cybersecurity for a decade. It delivers proven protection against the latest threats and exploits on a scalable, open solutions platform to governments and tier-one telecoms worldwide.

Opening Lunch Sponsor, Booth 4

Oracle

500 Oracle Parkway
Redwood City, CA 94065
www.oracle.com

Oracle engineers hardware and software to work together in the cloud and in your data center. With more than 400,000 customers—including 100 of the Fortune 100—in more than 145 countries around the globe, Oracle is the only vendor able to offer a complete technology stack in which every layer is engineered to work together as a single system. Oracle's industry-leading cloud-based and on-premises solutions give customers complete deployment flexibility and unmatched benefits including advanced security, high availability, scalability, energy efficiency, powerful performance, and low total cost of ownership. For more

information about Oracle (NYSE:ORCL), visit oracle.com.

Booth 11

Riscure

Delftechpark 49, 2628 XJ Delft,
Netherlands
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, Ste. 200
Palo Alto, CA 94301
www.SafeLogic.com

SafeLogic provides innovative encryption products for applications in mobile, server, appliance, wearable, and other constrained environments. Our flagship product, CryptoComply, provides drop-in FIPS 140-2 compliance with a common API across platforms, while our RapidCert process has revolutionized the way that certificates are earned. You needed SafeLogic six months ago.

Booth 8

Secure-IC

80 Avenue Des Buttes De Coesmes
Rennes France 35000
secure-ic.com

Based in France, Singapore and Silicon Valley, Secure-IC develops trusted computing security technologies for embedded systems to protect them from malevolent attacks and cyber threats. Secure-IC works 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. We prevent the hack of any secure element, reverse engineering of any embedded system, theft of intellectual property and are a partner for maximizing digital trust. http://secure-ic.com

Booth 7

Ultra Electronics, 3eTI

9713 Key West Avenue, Suite 500
Rockville, MD 20850
www.ultra-3eti.com

Ultra Electronics, 3eTI is a leading cyber-technology company with products and systems that secure critical infrastructure and improve operational efficiency. 3eTI helps connect and protect operations through military-grade machine-to-machine (M2M) security, secure wireless networks and sensor network applications, leveraging new and legacy systems while complying with highest government and industry standards such as FIPS 140-2 and IEC 62443 / ISA99. (www.ultra-3eti.com)

Level 2 Sponsor, Booth 14

Utimaco

3790 El Camino Real
Palo Alto, CA 94306
www.utimaco.com

Utimaco is a leading manufacturer of hardware based security solutions that provide the root of trust to keep cryptographic keys safe, secure critical digital infrastructures and protect high value data assets. Only Utimaco delivers a general-purpose hardware security module (HSM) as a customizable platform to easily integrate into existing software solutions, embed business logic and build secure applications. With German precision engineering, tamperproof Utimaco HSM offers scalable performance with the highest level of physical security and self-defense for hostile environments. Tens of thousands of enterprise and infrastructure companies rely on Utimaco to guard IP against internal and external threats and protect hundreds of millions of consumers globally. By building business applications on Utimaco's hardware root of trust, customers achieve regulatory compliance and the security confidence to focus on their core business.

Badge/Lanyard Sponsor, Booth 6

WolfSSL

10016 Edmonds Way, Suite C-300
Edmonds, WA 98020
www.yassl.com

WolfSSL, founded in 2004, is an open source Internet security company with products including the CyaSSL embedded SSL library, wolfCrypt crypto engine, SSL Inspection, and the yaSSL Embedded Web Server. WolfSSL employs the dual licensing model, offering products under both the GPLv2 as well as a standard commercial license. WolfSSL's products are designed to offer optimal embedded performance, rapid integration into existing applications and platforms, the ability to leverage a wide range of hardware crypto solutions, and support for the most current standards. All products are designed for ease-of-use with clean APIs, and are backed by a dedicated and responsive support and development team.

Your Conference Badge is a Digital Business Card

Badge/Lanyard Sponsor

Use any smart phone or pad QR code scanning app to retrieve complete contact information

Many free QR code scanning apps are available. The following app is highly rated in many app stores:

ScanLife by ScanBuy Inc. on Android, iOS, BlackBerry, Nokia Ovi, Windows Phone

We make no representations or warranties regarding the functionality or performance of any third party software

Conference Registrants @11/11/14

Maria Teresa Aarao, Innovation Director, Certisign Certificadora Digital
Admir Abdurahmanovic, VP Business Development, PrimeKey Solutions AB
Dawn Adams, Lab Manager, EWA-CANADA
Andrei Alexandru, Information Security Engineer, Penumbra Security, Inc.
Daniel Ambrosich, Principal Software Engineer, Oracle
Irina Avram, CSTL and FRAL Director, Leidos
Mary Baish, DOD
Maureen Barry, Lab Manager, Computer Sciences Canada
Chris Bean, DOD
Joanna Bell, Operations Manager, SafeLogic
Martin Bergling, Technical Manager, FMV/CSEC
Eric Betts, Security Certifications Manager, VMware
John Boggie, Manager Security Evaluation & Certification, NXP Semiconductors
Marc Boire, Lab Manager, CGI
Fritz Bollmann, Common Criteria certification, Federal Office for Information Security (BSI)
Dieter Bong, Product Manager, Utimaco IS GmbH
Josh Brickman, Oracle
Glenn Brunette, Senior Director, Cybersecurity, Oracle Public Sector
Eric Bryant, DEPARTMENT OF DEFENSE
Chris Brych, Senior Principal Security Analyst, Oracle Security Evaluations
Robert Burns, CSO, Thales e-Security
Tony Busciglio, Laboratory Manager, Acumen Security
Tom Caddy, CEO, Penumbra Security, Inc.
Peter Catherwood, Security Engineer, Thales UK
HeeBong Choi, Principal Researcher, The Attached Institute of ETRI
Giuseppe Cimmino, Sr. Analyst, Protiviti
Erin Connor, Director, EWA-CANADA
Chris Constantinides, Wind River
Michael Cooper, IT Specialist, NIST
Graham Costa, Security Certifications Manager, Safenet-inc
Jason Cox, Intel Corporation
David Cuccia, Engineer, US Department of Defense
Jason Cunningham, Program Manager, Computer Sciences Canada
Don Davidson, Chief Outreach, Science & Standards, US Department of Defense (DoD-CIO)
Mary Ann Davidson, Chief Security Officer, Oracle
Jatin Deshpande, Sr. Technical Account Manager, Giesecke & Devrient America Inc
Kelvin Desplanque, TME - Government Certification CoGS - Canada, Cisco Systems, Inc.
James Donndelinger, Aerospace
Randall Easter, Director, CMVP, NIST
Scott Ellett, Principal Software Engineer, Oracle
Kenneth Elliott III, Principal Engineering Specialist - IA, The Aerospace Corporation
Presley Ellsworth, Senior Firmware Developer, Sonavation, Inc.
Frederick Fakename, Faketitle, Fake Technology Partners
Valerie Fenwick, Software Engineering Manager, Oracle
Justin Fisher, CST Technical Director, Booz Allen Hamilton
Kevin Fowler, DELL
Jim Fox, NIST
Carolyn French, ITS Engineer, CSE
Gene Frost, Senior Integration Engineer, Utimaco Inc.
Linda Gallops, Principal Security Analyst, Oracle
Neng Gao, Assistant Professor,Ph.D., State Key Laboratory of Information Security, Inst
Luis Alfonso Garcia, IT Security Engineer, Epoche & Espri
Doug Gardner, Chief Technologiest, Sypris
Mrityunjay Gautam, Manager, Security Engineering, Citrix Systems
Tim Gaylor, Chief Security Architect, Citrix
Douglas Gebert, Hewlett-Packard Company
Shawn Geddis, Product Security Certifications Lead, Apple, Inc.
Dave Gerendas, MCAFEE
Nick Goble, Certifications Program Manager, Blue Coat
Nick Goble, CGI
Amarendra Godbole, Usual Suspect, Symantec Corporation
Gilbert Goodwill, Senior Principal Engineer, DPA Software & Training, Cryptography Research
Alan Gornall, Principal Consultant, Rycombe Consulting
Christophe Goyet, Technical Marketing Director, Oberthur Technologies
Gary Grainger, AT&E Technical Director, Leidos
Jon Green, CTO, Aruba Networks
Tammy Green, Senior Security Architect & Vulnerability Response, Blue Coat
Timothy Hall, NIST
Mark Hanson, Principal Program Manager, Product Certifications, McAfee. Part of Intel Security.
Stefan Harringer, IT Security, ÌDsterreichische Staatsdruckerei GmbH
Maarit Hietalahti, Senior Specialist, National Cyber Security Centre Finland
Brian Hwang, Security Certification Manager, BlackBerry
Ronny Janse, Program manager, Swedish civil contingencies agency
Jiwu Jing, tate Key Laboratory of Information Security, Insti
Darryl Johnson, Lead Security Engineer, Corsec Security, Inc.
James Kassebaum, USG
Masatoshi Kawashima, Security Evaluator, Information Technology Security Center
Matthew Keller, Vice President, Corsec Security, Inc.
Sharon Keller, Director, Cryptographic Algorithm Validation Prog., NIST
Stephen King, Lab Manager, Coact, Inc
Neha Kochar, Senior Software Engineer, F5 Networks
Junichi Kondo, Director, JCMVP, IPA
Helmut Kurth, Chief Scientist, atsec Information Security Corporation
Sam Lam, DOD
Don Laursen, Product Manager, F5 Networks, Inc
Dkj Ldjkf, adfads, adf
Vincent Le Roy, Engineer, Senior Staff, QUALCOMM
Suzanne Leicht, Mathematician, National Security Agency
Di Li, atsec
Yung-Li Liu, Telecom Technology Center
Iben Lunding, IT Security Adviser, CFCS
David MacFarlane, BlackBerry
Laurie Mack, Director Security & Certifications, Safenet
Lawrence Mao, Sr. Manager, Product Development, F5 Networks
Yi Mao, Principal Consultant, CST Lab Manager, atsec Information Security Corporation
Chris Marks, Brocade
Alexander Mazuruc, Senior Software Developer, WinMagic Inc
David McGregor, Device Evaluation Manager, UL
Scott McKinnon, Senior Product Manager, Juniper Networks
Michael Mehlberg, Senior Director of Business Development, Cryptography Research
Mark Minnoch, Account Manager, WolfSSL
Kenneth Modeste, Principal Engineer, UL LLC
Darren Moffat, Senior Principal Engineer, Solaris
Ed Morris, Co-Founder, Gossamer Security Solutions
Kathleen Moyer, Project Management Engineer, Corsec Security
Stephan Mueller, Principal Consultant, atsec Information Security Corporation
Werner Ness, Giesecke & Devrient
Vannie Van Nguyen, Security Certifications Lead Engineer, Junipeer Networks
Juan Gonzalez Nieto, Principal Consultant, BAE Systems Applied Intelligence
Martin Oczko, Product Manager, PrimeKey
Gesa Ott, Head of cryptographic analysis, Utimaco IS GmbH
Steve Pate, Chief Architect, HyTrust
Fiona Pattinson, Director Strategy & Business Development, atsec Information Security Corporation
Janine Pederson, Director, NIAP, NSA/CSS Commercial Solutions Center
William Penny, Principal Consultant, IBM
Bob Pittman, Federal Certification Program Manager - HP Network, Hewlett-Packard
Ray Potter, CEO & Co-Founder, SafeLogic
Eysha Shirrine Powers, System z Cryptography, IBM
Nikki Principe, Operations Manager, CNXTD events
Brad Proffitt, International Business Director åÐ ISG Lab Services, Infosec Global
Jean-Pierre Quemard, VP Security and Technology, Airbus Defense & Space
Nithya Rachamadugu, Director, Cygnacom
Arunprasad Ramiya Mothilal, TE Development Director, Imation Corporation
Steve Ratcliffe, TME, Cisco Systems
Jason Reeves, Graduate Student, Dartmouth College
Jose Rivera, Regional Sales Director, Utimaco
Richard Roane, Chief Engineer - INFOSEC, L-3 Communications, Linkabit
Diana Robinson, Government Certifications Progam Manager, Blue Coat
Langley Rock, Senior Security Analyst, SafeNet Inc.
Allen Roginsky, Mathematician, NIST
Ellard Roush, System Architect, Vormetric, Inc
William Rutledge, Managing Director, International Cryptographic Module Conference
Sami Saab, Principal Field Applications Engineer, Cryptography Research
Dr. Gen'Ya Sakurai, JCMVP, IPA
Gideon Samid, Professor, Case Western Reserve University
Gideon Samid, Professor, BitMint, LLC
Rory Saunders, Sr. Security Analyst, COACT, Inc.
Stephen Savard, ITS Engineer, CSE
Mike Scanlin, Information Assurance Program Manager, NetApp, Inc.
Steven Schmalz, Security Solution Architect, RSA The Security Division of EMC
Jerrod Schultz, Senior Security Engineer, Corsec Security, Inc.
Sonu Shankar, Software Engineer, Cisco
Ron Sims II, Federal Government
Miles Smid, Cyber Security Consultant
Bill Smith, Manager, Security Engineering, Citrix Systems, Inc
Jonathan Smith, Crypto Module Tester, CygnaCom Solutions
Sean Smith, Dartmouth College
Daniel Southern, Systems Security, Oracle Corporation
Desiree Spann, AEGISOLVE
Travis Spann, AEGISOLVE
Alicia Squires, Global Certifications Team, Manager, Cisco
Randy Steck, Symbiotic Systems Research
Michael StJohns, Security Architect, NthPermutation Security
Marcus Streets, Director High Security Products, Good Technology
MoisÎ©s Riesgo Suarez, Evaluator, Epoche & Espri
William Supernor, CTO, KoolSpan
Harshad Thakar, Engineer, Seagate
Ryan Thomas, FIPS 140-2 Program Manager, CGI
Beverly Trapnell, NIST
M Hassan Triqui, CEO, Secure-IC
Tsun-Te Tsui, TUV Nord Asia Pacific
William Tung, Cryptographic and Security Testing Laboratory Mgr, Leidos
Jasper Van Woudenberg, CTO North America, Riscure
Apostol Vassilev, Cybersecurity Expert, Computer Security Division, NIST
Ashit Vora, Lab Director and Co-FounderAcumen Security, Acumen Security
John Ross Wallrabenstein, Senior Research Scientist, Sypris Electronics
Dan Walters, MITRE
Richard Wang, Cryptographic & Security Test Lab Engineer, Leidos
Patrick Warley, Head of R&D, Integral Memory Plc
Rod Weaver, Business Director, WolfSSL
Steve Weingart, Public Sector Certifications, Aruba Networks
Gijs Willemse, INSIDE Secure B.V.
Marc Witteman, Founder, Riscure
Clinton WInebrenner, Tech Lead, Cisco Systems, Inc.
Kwok Wong, Crypto Module Tester, CygnaCom Solutions
Lu Xiao, Security Assurance Lead, Qualcomm Technologies, Inc.
Tatsuya Yanagisawa, Senior Security Engineer, ECSEC Laboratory Inc.
Jenn Ya Yang, Telecom Technology Center
Yu Chih Yang, Telecom Technology Center
Li Zhang, atsec China

wolfSSL FIPS 140-2 support

wolfSSL will soon have FIPS 140-2 level one validation for the wolfCrypt crypto engine! We are completing the lab testing process and our application will reach NIST for final review in December 2014.

Our FIPS certification will support a broad range of wolfSSL customers, specifically those who sell to the US government.

wolfSSL is on the NIST FIPS 140 process list, which is located at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf

wolfSSL provides SSL/TLS and cryptography solutions with an emphasis on speed, portability, features, and standards compliance. We cater to diverse user base in the cloud, on appliances, and in government and military applications. We are happy to help our customers and community in any way we can. Our products are Open Source, which provides our users with access to all of our underlying code and documentation.

Why does a security company that focuses on SSL/TLS and cryptography choose a wolf over any number of possible logo designs? The wolf was chosen to be part of the wolfSSL logo for several reasons: wolves like to live in free and open environments, they communicate and hunt in packs (like open source developers hunt bugs), and they are both lean and fast.

All of wolfSSL's products are 100% made in the USA and have been since the company's birth in 2004. wolfSSL is based in Bozeman, MT, Seattle, WA, and Portland, OR. All product support provided by wolfSSL is from native English-speaking engineers.

SSL/TLS Library

For Military and Government Applications, Devices, IoT, and the Cloud

Providing secure communication for Military, Government, IoT, smart grid, connected home, automobiles, routers, applications, games, IP,

CyaSSL CyaSSL is a C-language-based SSL/TLS that sports a small size, speed, and excellent portability. CyaSSL supports industry standards up to the current TLS 1.2 and DTLS 1.2 levels, is up to 20 times smaller than OpenSSL, offers a simple API, an OpenSSL compatibility layer, OCSP and CRL, and several progressive ciphers, including the emerging ChaCha 20 and Poly 1305.

Crypto Engines

The wolfCrypt embedded cryptography engine is a lightweight cryptography library targeted for embedded, RTOS, and resource constrained environments primarily because of its small size, speed, and portability. wolfCrypt supports the most popular algorithms and ciphers as well as progressive ones such as HC-128, RABBIT, NTRU, and SHA 3. wolfCrypt is **stable**, **production-ready**, and backed by an **excellent support team**.

Java Wrapper

For Java applications that wish to leverage the industry-leading CyaSSL SSL/TLS implementation for secure communication, our JNI wrapper provides an interface to give those applications support for the current SSL/TLS standards up to TLS 1.2 and DTLS 1.2. **TLS 1.3 support is in Alpha.**

wolfSSL Inc.
Bozeman, MT
info@wolfSSL.com
wolfSSL.com

Public Sector Leaders

- ✓ 20 of the 20 Top Global Governments
- ✓ 15 of the 15 Federal Cabinet Departments
- ✓ 50 of the 50 States
- ✓ 20 of the 20 Top Counties
- ✓ 20 of the 20 Top Cities

Get Better Results

ORACLE®

oracle.com/government
or call 1.800.633.0584

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates.