CONFERENCE PROGRAM

THE THIRD

International Cryptographic Module Conference ICMC15

PLATINUM SPONSOR

SILVER SPONSOR

SILVER SPONSOR

November 4-6, 2015 ■ Hilton, Washington, D.C.

Customer Voices

"...With the help of atsec's CST Lab, Watchdata received a FIPS 140-2 Security Level 3 validation certificate (#2397) for the Watchkey ProX USB Token. We applaud the professional ability of atsec's team. They have proven once again that they are able to work successfully with customers around the world for their certification needs."

Sincerely,
Thomas Wang Xuelin
Watchdata Technologies Pte Ltd

"...We are grateful for atsec's assistance in preparing the hardware-based cryptographic module in the Qualcomm® Snapdragon™ 805 processor to pass FIPS 140-2 security certification.
Passing FIPS 140-2 certification helps qualify our customers to work with government departments and regulated industries and to better address enterprise needs."

Sincerely,
Antonio Challita
Qualcomm Technologies, Inc.

"...We have been working together with atsec on Common Criteria, FIPS 140-2, and DISA STIG certifications for many years. atsec's professionalism, knowledge, and steady effort helps make our products more secure for all our customers."

Sincerly,
Thomas Biege
SUSE

"...In the process of working towards the certificate, we experienced atsec as a reliable team with personal attention that manages changes adequately and is committed to perform. It was a pleasure to work with the team from atsec."

Best regards,
Gijs Willemse,
Bob Oerlemans
INSIDESecure

"...We have been working with atsec for many years undergoing Common Criteria and FIPS evaluations. Having just completed our latest FIPS evaluation I would like to once again thank atsec for their professional approach to helping us achieve our goals. As always, the core team has demonstrated great care and attention to detail. They have been a pleasure to work with."

Sincerely
Alex Hennekam
IBM Security Systems

"...We have worked closely with atsec information security corporation as the evaluation lab for Common Criteria and FIPS-140 certifications of Red Hat Enterprise Linux during the past several years. With the help of atsec, Red Hat has earned a place at the top of the list of the industry's most certified operating systems.
atsec always demonstrates integrity, professionalism, and technical expertise in the security field. They are a pleasure to work with."

Regards,
Steve Grubb
Red Hat, Inc.

"...atsec has always shown professionalism, integrity, and expertise in the field of information security. They have been a pleasure to work with."

Sincerely,
Jorma Levomäki
McAfee

"...atsec information security corporation is the evaluation lab of SecuTech for FIPS-140 certifications.
We are really happy to work with atsec's professional team. The whole validation process runs smoothly and efficiently under the instruction of atsec. We really appreciate the effort, help and kindness of atsec in the past years."

Best regards,
Raymond Chaw
SecuTech

Learn more at our booth in the exhibition hall or visit www.atsec.com

Welcome

Dear ICMC 2015 Participant,

I'd like to personally welcome each of you to the Third Annual International Cryptographic Module Conference (ICMC). Three years ago, when atsec launched the first ICMC, we envisioned that the community needed a common ground to discuss the standards, technologies and processes that influence cryptographic module validation. Three years down the road, the conference has evolved into a self-funded event with many enthusiastic supporters working in the technical community.

We are seeing many changes in commercial cryptography and it's exciting to see the industry embrace them and move forward with a spirit of innovation and discovery. We work in a vibrant field and the ICMC brings together inspired people to ensure we navigate the cutting edge successfully.

I'd like to give you an idea of what you can expect and what we hope to achieve over the next three days. We are excited to share with you the workshops and presentations from government, academia, product developers, laboratories, consultants and industry leaders.

Wednesday, November 4th, consists of five half-day, Pre-Conference Workshops.

Thursday, November 5th, begins with three exciting keynote speeches from industry and government leaders, and continues with presentations on three tracks: Certification Programs, General Technology and Advanced Technology. The exhibit area opens this day right after keynotes. At the end of the day, we invite you to join us for a reception in the exhibits area.

Friday, November 6th, continues presentations on two tracks: Certification Programs and General Technology, and begins presentations on a new track: End User Experience. The conference concludes with a Summary Panel Discussion. The exhibits are open until immediately before the Summary Panel.

We hope this conference will enable open discussions, exchange of ideas and provide many opportunities to network, collaborate and share information. We have attendees and presenters from around the globe and we hope build international relationships as well.

Thank you so much for attending the ICMC and sharing your experience, expertise and ideas. We are tremendously encouraged by your participation and feedback. Throughout the conference, please stay engaged and assist us in shaping the future of the ICMC and the commercial cryptography industry. Our thanks also goes out to the conference sponsors and exhibitors. We hope you will take some time to visit the booths.

My personal respect and thanks to all of you,

Yi Mao, CST Lab Manager
atsec information security corporation

Table of Contents

Contact Information

Program Committee

Erin Connor, Director, EWA-Canada

Ryan Hill, Consultant, atsec information security

Nithya Rachamadugu, Director, CygnaCom

Bill Rutledge, Project Director, ICMC 2015

Marcus Streets, Product Director, High Security Products, Good Technology

Conference Staff

Bill Rutledge, Project Director, 1.212.866.2169, bill.rutledge@ICMConference.org

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

PLATINUM SPONSOR

SILVER SPONSOR

SILVER SPONSOR

BAG SPONSOR

BADGE SPONSOR

OPENING LUNCH SPONSOR

EVENT SPONSOR

EVENT SPONSOR

EVENT SPONSOR

LAB SHOWCASE SPONSOR

LAB SHOWCASE SPONSOR

EXHIBITORS

ASSOCIATION & MEDIA SPONSORS

Conference Agenda

Detailed session descriptions are online at www.ICMConference.org

Pre-Conference Workshops (W) on Nov 4. **Plenary Sessions** (P) on Nov 5, followed by 4 tracks:	**Certification Programs Track** (C) Issues related to the CMVP, government programs and policy	**General Technology Track** (T) Tools and techniques relating to cryptographic modules	**Advanced Technology Track** (A) High-level technology issues, or special-focus subject matter	**User Experience Track** (U) Information of interest to the cryptographic module end-user

Pre-Conference Workshops

Wednesday, November 4

Pre-Conference Workshop Sessions

Regency, Plaza 2 & Plaza 3

9:00 **How Not To Do a FIPS 140 Project** (W01a) Steve Weingart, Manager of Public Sector Certifications, Aruba Networks; Chris Keenan, Evaluator, Gossamer Security Solutions

9:00 **Breaking into Embedded Devices: Side Channel Analysis (**W01b) Jasper Van Woudenberg, CTO North America, Riscure

9:00 **GlobalPlatform—Addressing Unique Security Challenges through Standardization** (W01c) Kevin Gillick, Executive Director, GlobalPlatform; Hank Chavers, Technical Program Manager, GlobalPlatform; Philip Hoyer, Director of Strategic Innovation, HID Global, and Identity Task Force Chair, GlobalPlatform; Alexander Summerer, Technology Consultant, Giesecke & Devrient, and Secure Element Access Control Working Group Chair, GlobalPlatform

12:15 **Lunch in Atrium**

13:15 **Validating a Virtual Module Without Guidance From CMVP** (W02a) Steve Ratcliffe, TME, Cisco

13:15 **Breaking into Embedded Devices: Fault Injection** (W02b) Jasper Van Woudenberg, CTO North America, Riscure

16:30 **Adjourn**

Conference Sessions

Thursday, November 5

Plenary Keynote Presentations — Plaza 1-3

8:00 **Registration and Coffee**

9:00 **Welcome, Introductions** Yi Mao, Principal Consultant, atsec information security

Current Issues in Cryptography Phil Zimmermann, Co-founder, Silent Circle

Cryptography, Moore's Law & Hardware Foundations for Security Paul Kocher, President, Chief Scientist, Crytography Research

Department of Defense Cybersecurity Marianne Bailey, Principal Director, Deputy CIO for Cybersecurity, Department of Defense

10:30 **Break, Exhibits Open**

Thursday Opening Lunch

Sponsored by

ORACLE

Save the Date: May 18-20, 2016 * Shaw Centre * Ottawa, Ontario

THE FOURTH

International Cryptographic Module Conference

ICMC16

In 2016, ICMC will grow into an expanded international venue, with a new late Spring timeframe chosen to avoid conflict with other major industry events.

Conference Sessions

Thursday, November 5

	Certification Programs Track — Plaza 1	General Technology Track — Plaza 2
11:00	**Accreditation, Validation and Recognition based on ISO Standards** (C12) Randall Easter, NIST. *The future in International Standards for cryptographic module testing and how to participate in their development. Let's also talk about a new International scheme for cryptographic module testing.*	**Effective Cryptography—Or: What's Wrong With All These Crypto APIs?** (G12) Thorsten Groetker, CTO, Utimaco. *We'll talk about implementing cryptographic algorithms in software, while overcoming the shortcomings of the likes of PKCS#11 and JCE*
11:45	**The Next Steps Toward A Scalable International Cryptographic Evaluation Process** (C13) Clint Winebrenner, Technical Lead, Product Certifications Security & Trust Organization, Cisco. *We'll propose how we can work together influence an internationally acceptable cryptographic algorithm validation process.*	**The Next Steps Toward A Scalable International Cryptographic Evaluation Process** (C13) Clint Winebrenner, Technical Lead, Product Certifications Security & Trust Organization, Cisco. *We'll propose how we can work together influence an internationally acceptable cryptographic algorithm validation process.*
12:30	**Lunch in Exhibit Area, Sponsored by Oracle** *Cryptographic Module User Forum (CMUF) Meeting: Twinbrook Room*	
13:45	**Legacy Random Number Generators (RNGs)** (C14) Zhiqiang (Richard) Wang, CSTL Lab Technical Director, Leidos; William Tung, Senior Security Evaluation Analyst, Gemalto. *Many legacy RNGs won't be permitted in FIPS mode after 2015. We'll talk about how to prepare for this change.*	**The What, Why, and How of Tokenization** (G14) Peter Helderman, Principal Consultant, UL. *Tokenization: from complementing cryptography to being a part of cryptographic operations.*
14:30	**Proposed Changes for a Long-Overdue Revision of FIPS 140-2** (C15) Francisco Corella, Founder & CTO, Pomcor; Karen Lewison, CEO, Pomcor. *ISO 19790:2012 has been suggested as a candidate to succeed FIPS 140-2, but it only makes incremental changes. We propose three substantial changes that should be incorporated into a revised standard.*	**SP 800-131A Transitions and Related Implementation Guidance** (G15) Allen Roginsky, Mathematician, NIST; Apostol Vassilev, Cybersecurity Expert, Computer Security Division, NIST. *We'll review the status of the cryptographic algorithms and key sizes that are subject to the NIST transition and will announce the future transition steps.*
15:15	**Break in Exhibit Area**	
15:45	**Adding to the Approved List of Algorithms** (C16) Kelvin Desplanque, TME—Government Certification CoGS—Canada, Cisco Systems. *Occasionally someone in the vendor community will find a method for extending either the efficiency or security of a new mode of a particular algorithm on the FIPS Approved List. This presentation will describe the journey that follows.*	**SP800-90B: Analysis of Linux /dev/random** (G16) Stephan Mueller, Principal Consultant and Evaluator, atsec information security. *We will present test approaches that allows /dev/random with the entropy pools and the events feeding into these pools to be observed at runtime.*
16:30	**CMVP Programmatic Status (CMVP)** (C17) Carolyn French, ITS Engineer, CSE; Michael Cooper, IT Specialist, NIST; Apostol Vassilev, Cybersecurity Expert, Computer Security Division, NIST. *This presentation will discuss the status of the CMVP, including some of the challenges, successes, and directions for development.*	**Enough Entropy? Justify It!** (G17) Yi Mao, Principal Consultant, atsec information security. *This presentation will review various mathematical definitions of Entropy, and present some examples of how the entropy assessment can be performed on commonly used seed sources.*
17:15	**Networking Reception in Exhibit Area**	

Advanced Technology Track — **Plaza 3**

11:00 **Quantum Computing and Its Impact** (A12) David Cornwell, Lead Engineer, Booz Allen Hamilton. *You'll learn about which FIPS 140 algorithms are "quantum safe" and which ones are not.*

11:45 **Extending Derived Credential Use to Support S/MIME Even with Medium-Hardware Protected Credentials** (A13) Issam Andoni, Chief Technology Architect/Owner, Zeva Inc. *We'll review a solution that allows mobile device users to securely read encrypted email by extending the use of derived credentials rather than smart card credentials.*

12:30 **Lunch in Exhibit Area, Sponsored by Oracle**

13:45 **A Look into Hard Drive Firmware Hacking** (A14) Khai Van, Security Tester, Gossamer Security Solutions. *This presentation will dissect a firmware hack, examine the procedure, and review the implications on consumers. We will also explore possible future safeguards against these attacks as this story progresses.*

14:30 **Improved Approaches to Online Health Testing in SP800-90 RNGs** (A15) David Johnston, Hardware Security Architect, Intel. *This presentation will address the current suite of standards for the validation of cryptographic algorithms and modules and those that are in development.*

15:15 **Break in Exhibit Area**

15:45 **Test Vector Leakage Assessment (TVLA) for Side Channel Analysis in Conformance Testing Scenario** (A16a) Gilbert Goodwill, Sr. Principal Engineer, Cryptography Research. (A16b) Steve Weymann, Security Engineer, InfoGard Laboratories. *Two presentations provide an update on side channel testing, and a look at its practicality in conformance testing scenarios.*

16:30 **CMVP Programmatic Status (CMVP)** (C17) Carolyn French, ITS Engineer, CSE; Michael Cooper, IT Specialist, NIST; Apostol Vassilev, Cybersecurity Expert, Computer Security Division, NIST. *This presentation will discuss the status of the CMVP, including some of the challenges, successes, and directions for development.*

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

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.

Network Name: **Hilton Conference**

User Name: **hilton14**

Password: **plaza14**

Join the Conversation on Twitter

#CryptoModConf

Conference Sessions

Friday, November 6

	Certification Programs Track — Plaza 1	General Technology Track — Plaza 2
9:00	**CSfC Program and its FIPS 140-2 Requirements** (C21) Matt Keller, VP, Corsec Security. *We'll explain how FIPS 140-2 validation and adherence to Suite B will impact a vendor's ability to be listed on the CSfC Components List.*	**Repetition Count Test** (G21) Jason Tseng, Project Control Analyst, Leidos; Michael Powers, Security Assurance Engineer, Leidos. *We'll discuss the new proposed Repetition Count Test (RCT), its benefits for vendors, as well as the FIPS 140-2 requirements behind a CRNGT for NIST Special Publication 800-90A Deterministic Random Bit Generators (DRBGs).*
9:45	**What is Suite-B Cryptography and How Does it Relate to Government Certifications?** (C22) Anthony Busciglio, Co-Founder, Laboratory Manager, Acumen Security. *This presentation will provide a high-level introduction to Suite-B, and discusses how it applies to commonly certified cryptographic protocols.*	**Roadmap to Testing of New Algorithms (CAVP)** (G22) Sharon Keller, Computer Scientist, NIST; Apostol Vassilev, Cybersecurity Expert, Computer Security Division, NIST. *This presentation will discuss the evolution of the CAVP with the testing of newly adopted approved cryptographic algorithms.*
10:30	**Break in Exhibit Area**	
11:00	**Introduction on the Commercial Cryptography Scheme in China** (C23) Di Li, atsec information security. *We've heard a lot about CMVP and FIPS 140-2, this time let's see what is happening in China and what we can do to join the game.*	**Entropy Estimation by Example** (G23) David Cornwell, Lead Engineer, Booz Allen Hamilton. *We will review the fundamentals of entropy estimation, statistical tests of SP 800-90, and the NIST entropy tool. We will provide specific examples of the entropy estimation of data streams and keys.*
11:45	**FIPS 140 Quo Vadis?** (C24) Apostol Vassilev, Cybersecurity Expert, Computer Security Division, NIST. *It takes a village—industry, labs, CMVP, government agencies—to respond well to the incredibly fast evolving challenges in cybersecurity and cryptography.*	**Importance of Open Source to the Cryptographic Module Community** (G24) Chris Brych, Senior Principal Security Analyst, Oracle. *After almost 10 years, the time is coming that OpenSSL distributions will not contain any FIPS support. We'll look at the history of the OpenSSL project, why OpenSSL FIPS support is important, and discuss concerns in the near future.*
12:30	**Lunch in Exhibit Area**	
13:30	**Cryptographic Validation Requirements and the Common Criteria (ISO/IEC 15408)** (C25) Kirill Sinitski, Common Criteria Evaluator & Quality Coordinator, CygnaCom. *For anyone who is interested in the Common Criteria this presentation may lessen the pain of meeting requirements.*	**Challenges in Generating Keys for Asymmetric-Key Algorithms** (G25) Allen Roginsky, Mathematician, NIST. *We will review the approved methods for key generation for RSA and other asymmetric-key algorithms, the risks, the attacks, the implementation and testing issues.*
14:15	**NIST & NIAP Working Together** (C26) Janine Pedersen, Director, National Information Assurance Partnership (NIAP); Michael Cooper, IT Specialist, NIST. *NIST and NIAP are collaborating to streamline evaluations—leveraging commonalities to gain efficiencies. This presentation will discuss progress to date and plans for the future.*	**What is My Operational Environment?** (G26) Swapneela Unkule, atsec information security. *Attendees will understanding operational environment for algorithm vs module validation.*
15:00	**Break in Exhibit Area** (Exhibits Close at 15:30)	

End User Experience Track — Plaza 3

9:00 **Commonly Accepted Keys and CSPs Initiative** (U21) *Ryan Thomas, FIPS 140-2 Program Manager, CGI Global Labs. This presentation will focus on an initial list of Industry Protocols such as TLS, SSH, SNMP and IPsec, RADIUS, Key Derivation Protocols such as 802.11i, and algorithms such as Diffie-Hellman, EC Diffie-Hellman and SP 800-90A DRBG.*

9:45 **FIPS is FIPS, Real World is Real World and Never the Twain Shall Meet?** (U22) Ashit Vora, Co-Founder and Laboratory Director, Acumen Security. *This presentation will cover the evolution of FIPS 140-2, discuss some egregious requirements that may be irrelevant or harmful to modern crypto systems, and provide recommendations on remediation.*

10:30 **Break in Exhibit Area**

11:00 **Collateral Damage—Vendor and Customer Impact of Frequent Policy Changes** (U23) Joshua Brickman, Director, Security Evaluations, Oracle; Glenn Brunette, Senior Director and Chief Technologist, Cybersecurity, Oracle. *This talk will demonstrate examples highlighting how continuous changes to policies can have a major impact on a product's lifecycle from*

11:45 **Learning From Each Other and Our Mistakes** (U24) Terrie Diaz, Product Certification Engineer, Cisco Systems; Edward Morris, Co-Founder, Gossamer Security Solutions. *We will examine how FIPS 140-2 and Common Criteria certification schemes intersect, support one another, are (to a degree) synergistic, and could remain so.*

12:30 **Lunch in Exhibit Area**

13:30 **FIPS140-Testing: You Want My What?** (U25) Valerie Fenwick, Software Engineering Manager, Oracle; Hai-May Chao, Principal Software Engineer, Solaris Security Technologies Group, Oracle. *Algorithm testing and IGs—what your customers don't know won't hurt them?*

14:15 **Validating Encryption: The Bottleneck in Security Innovation** (U26) Ray Potter, CEO, SafeLogic; Walter Paley, Director of Marketing, SafeLogic. *True or False: Validating encryption allows the US Federal government to deploy the best, most cutting-edge technology in a secure way?*

15:00 **Break in Exhibit Area** (Exhibits Close at 15:30)

Summary Panel Discussion — Plaza 1

15:30 **Impact of Draft CMVP Policy Changes on Industry (P27)** Moderator: Marcus Streets, Product Director High Security Products, Good Technology Panelists: Douglas Gebert, Enterprise Architect, HP Enterprise; Michael Cooper, IT Specialist, NIST; Tammy Green, Senior Principal Security Architect, Blue Coat Systems; Laurie Mack, Director Security & Certifications, Gemalto.

Recently, NIST requested public comment on a proposal to use the ISO/IEC 19790:2014 Security Requirements for Cryptographic Modules standard as the U.S. Federal Standard for cryptographic algorithm and cryptographic module testing, conformance, and validation activities, replacing the standards currently specified by FIPS 140-2. With the period for public comment ending just prior to ICMC15, there will be much to discuss about this proposed shift. These industry experts will explore the issue in a moderated discussion with plenty of opportunity for audience Q&A. Don't miss it.

16:15 **Conference Adjourns**

Speakers

Speaker biographies are online at www.ICMConference.org

Issam Andoni

Chief Technology Architect/Owner, Zeva Inc.

A13

Marianne Bailey

Principal Director, Deputy CIO for Cybersecurity, Department of Defense

P11c

Joshua Brickman

Director, Security Evaluations, Oracle

U23

Glenn Brunette

Senior Director & Chief Cybersecurity Technologist, Oracle

U23

Tony Busciglio

Co-founder & Laboratory Director, Acumen Security

C22

Chris Byrch

Senior Principal Security Analyst, Oracle

G24

Hai-May Chao

Principal Software Engineer, Solaris Security Technologies Group, Oracle

U25

Hank Chavers

Technical Program Manager, Global Platform

W01c

Erin Connor

Director, EWA-Canada

Program Committee

Michael Cooper

IT Specialist, NIST

C17, C26

Francisco Corella

Founder & CTO, Pomcor

C15

David Cornwell

Lead Engineer, Booz Allen Hamilton

G23

Kelvin Desplanque

Security Certification Engineer, Cisco Systems Limited

C16

Terrie Diaz

Product Certification Engineer, Cisco Systems

U24

Randall Easter
Computer Security Division, STVM, NIST

C12

Valerie Fenwick
Software Engineering Manager, Oracle

U25

Carolyn French
Manager, Cryptographic Module Validation Program

C17

Douglas Gebert
Enterprise Architect, HP Enterprise

P27

Shawn Geddis
Security & Certifications Engineer, Apple Inc.

Moderator

Kevin Gillick
Executive Director, GlobalPlatform

W01c

Gabriel Goller
R&D Specialist Cryptology, Giesecke & Devrient GmbH

A17

Gilbert Goodwill
Senior Principal Engineer, Cryptography Research

A16a

Tammy Green
Senior Principal Security Architect, Blue Coat Systems

P27

Thorsten Groetker
CTO, Utimaco

G12

Peter Helderman
Principal Consultant, UL

G14

David Johnston
Hardware Security Architect, Intel Corporation

A15

Chris Keenan
Gossamer Security Solutions

W01a

Matt Keller
Vice President, Corsec

C21

Sharon Keller
Computer Scientist, NIST

G22

Paul Kocher
President and Chief Scientist, Cryptography Research

P11b

Karen Lewison
CEO, Pomcor
C15

Di Li
Senior Consultant, atsec China
C23

Laurie Mack
Director Security & Certifications, Gemalto
P27

Yi Mao
Lab Director, atsec information security
G17

Edward Morris
Co-Founder, Gossamer Security Solutions
G13

Stephan Mueller
Principal Consultant and Evaluator, atsec information security
G16

Walter Paley
Director of Marketing, SafeLogic
U26

Janine Pederson
Director, National Information Assurance Partnership (NIAP)
C26

Ray Potter
CEO & Founder, SafeLogic
U26

Michael Powers
Security Assurance Engineer, Leidos
G21

Nithya Rachamadugu
Director, Cygnacom
Program Committee

Steve Ratcliffe
TME, Cisco Systems
W02a

Allen Roginsky
Mathematician, NIST
G15, G25

Kirill Sinitski
Common Criteria Evaluator, CygnaCom CCCEL Canada
C25

Jonathan Smith
Senior FIPS Engineer, CygnaCom Solutions
Moderator

Marcus Streets
Director High Security Products, Good Technology
Program Committee, P27

Alexander Summerer

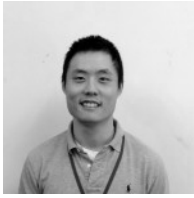
Technology Consultant, Giesecke & Devrient; Chair, GlobalPlatform Secure Element Access Control Working Group

W01c

Ryan Thomas

FIPS 140-2 Program Manager, CGI Global IT Security Labs-Canada

U21



Jason Tseng

Leidos CSTL Lab Manager

G21

William Tung

Senior Security & Certifications Analyst, Gemalto

Moderator

Swapneela Unkule

Senior Consultant, atsec information security

G26

Khai Van

Security Tester, Gossamer Security Solutions

A14

Jasper Van Woudenberg

CTO North America, Riscure

W01b

Apostol Vassilev

Technical Director, Cryptographic Module Validation Program, NIST

G15, C24

Ashit Vora

Co-Founder & Lab Director, Acumen Security

U22

Zhiqiang (Richard) Wang

CSTL Lab Technical Director, Leidos

C14

Steve Weingart

Manager of Public Sector Certifications, Aruba Networks

W01a

Steve Weymann

Security Engineer, InfoGuard

A16b

Clint Winebrenner

Technical Lead, Product Certifications Security & Trust Organization, Cisco

C13

Phil Zimmermann

Co-founder of Silent Circle

P11a

COACT

Your FIPS Expert

www.COACT.com

Sponsors & Exhibitors

Event Sponsor

Acumen Security

18504 Office Park Dr,
Montgomery Village, MD 20886
www.acumensecurity.net

Acumen Security is your one stop shop to certify your products and get into the hands of your government customers ASAP. We aim to not only certify your products, but also do so in the easiest, fastest and cheapest way possible while maintaining the integrity of the certification efforts. That means not cutting corners but working smartly. It means being able to understand your worldview so that we can adapt to your needs. It means being available when you need us. Most of all it means being a partner in your certification journey rather than running parallel.

Acumen Security

Your One Stop Shop For Product Certification

FIPS 140 | Common Criteria | SCAP| Secure Supply Chain

Mail: info@acumensecurity.net
Phone: +1 (703) 375-9820
Web: www.acumensecurity.net
Twitter: @acumensec

Event Sponsor

AEGISOLVE

415 Fairchild Drive,
Mountain View, CA 94043
www.aegisolve.com

AEGISOLVE Cyber Security Laboratories accelerates your time to market with proven security analysis and testing processes. Headquartered in Silicon Valley, California, AEGISOLVE is an accredited industry leader, providing FIPS 140-2 validations for nearly a decade.

ÆGISOLVE

Silver Sponsor, Booth 10

Allegro Software Development

www.allegrosoft.com/icmc2015

Secure Software for the Internet of Things – Allegro Software is a leading provider of embedded Internet software toolkits to product developers worldwide. Field proven in 200,000,000+ devices, our solutions enable manufacturers of hardware, software and digital products in the Military, Energy, Healthcare, Enterprise and Consumer markets to create connected secure devices using TLS, Suite B, FIPS 140-2 capabilities and more. Stop by our booth at ICMC 2015 (Booth #10)

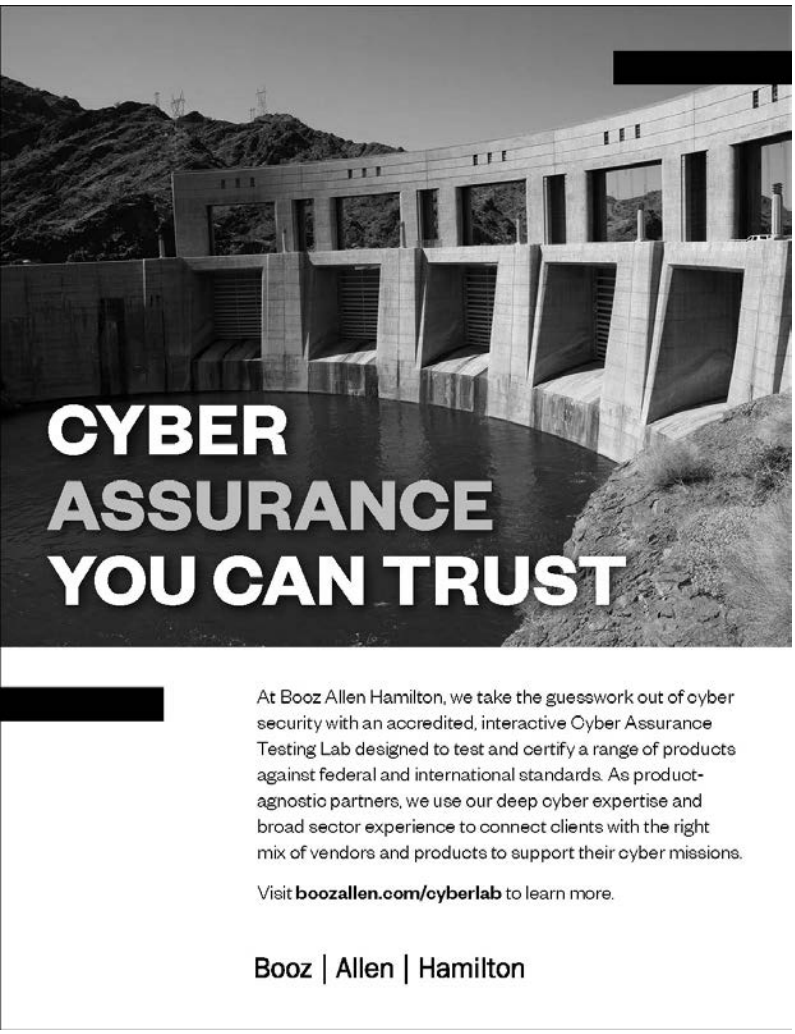
Platinum Sponsor, Booth 9

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



Event Sponsor

Booz Allen Hamilton

308 Sentinel Drive,
Annapolis, MD 20701

www.boozallen.com

Booz Allen Hamilton has been at the forefront of strategy and technology for more than 100 years. Today, the firm provides management and technology consulting and engineering services to leading Fortune 500 corporations, governments, and not-for-profits around the globe. Booz Allen partners with public and private sector clients to solve their most difficult challenges through a combination of consulting, analytics, mission operations, technology, systems delivery, cyber security, engineering, and innovation expertise. With international headquarters in McLean, Virginia, the firm employs more than 22,500 people globally and had revenue of $5.27 billion for the 12 months ended March 31, 2015. To learn more, visit www.boozallen.com. (NYSE: BAH)

Booth 6

COACT

9140 Guilford Road,
Columbia, MD 21046

www.coact.com

COACT is the leading provider of Information assurance and Network security services to both commercial and federal agencies. With over 25 years of industry experience, COACT provides Common Criteria, Fedramp, SCAP, and FIPS 140-2 certifications and has completed nearly 33 % of all SCAP certifications. Distinguished for having been one of the first companies to receive their FedRAMP accreditation, COACT has an unparalleled lab and network testing facility powered by practical experience. As a Service Disabled Veteran Owned Small Business, COACT proudly partners with numerous veteran hiring programs and prides itself in offering its customers multiple compliance certification options.

Association Sponsor

Common Criteria User Forum

www.ccusersforum.org

The Common Criteria Users Forum's mission is to provide a voice and communications channel amongst the CC community. The CCUF promotes the CC and provides an open forum for various CC topics to be discussed without favoring anyone group and supports international Technical Communities and technical working groups in a number of ways. The CCUF is independent of any government or certification body and membership is open to all interested in the CC.

Association Sponsor

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.

Lab Showcase Sponsor

CygnaCom Solutions

7925 Jones Branch Dr, Ste 5400, McLean, VA 22102

www.cygnacom.com

CygnaCom offers a full range of security testing services enabling our clients to certify products to the standards required by many Government and regulatory bodies. Our staff of highly qualified professionals will guide your team through evaluations, validations, certifications, and assessments to ensure on time and within budget procurement eligibility and listing.

Media Sponsor

The Ethical Hacker Network

www.ethicalhacker.net

The Ethical Hacker Network (EH-Net) is a free online magazine for security professionals. We are here not only to help the good guys learn what the bad guys know in order to help secure your own systems, but we also strive to help those desiring to enter, advance and maintain their careers in the many aspects of ethical hacking from network & webapp penetration testing to forensics, incident response to reverse engineering, project management to social engineering… If you want to hack for a living, we'll help you get there.

Lab Showcase Sponsor

EWA - Canada

1223 Michael Street

Suite 200, Ottawa, Ontario, Canada, K1J7T2

www.ewa-canada.com

EWA-Canada was incorporated and has been in operation since June 1988. We are recognized as Canada's premiere provider of information and communications technology (ICT) security and assurance services and a global centre of excellence in security engineering and test and evaluation innovation. Our solutions are based on the vast expertise of our personnel, a structured system engineering approach, and vendor-neutral selection and implementation of appropriate technologies. Our commitment is to provide excellence to our clients. EWA-Canada provides experienced, qualified resources, and company expertise in all facets of security program development and assessments, product test, evaluation and certification, security architecture design and development, identification token and credential issuance, security incident response, computer forensics and training. EWA-Canada offers our clients proven, end-to-end solutions (technology, people and processes) to assess, plan, and protect the security of their ICT infrastructure and enterprise.

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.

Association Sponsor

GlobalPlatform

www.Globalplatform.org

GlobalPlatform is a cross industry, non-profit association which identifies, develops and publishes specifications that promote the secure and interoperable deployment and management of multiple applications on secure chip technology. Its proven technical specifications, which focus on the secure element (SE), trusted execution environment (TEE) and system messaging, provide the tools that are regarded as the international industry standard for building a trusted end-to-end solution which serves multiple actors and supports several business models.

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.

Media Sponsor

Information Security Community on LinkedIn

www.linkedin.com/groups/38412

Join the Information Security Community on LinkedIn – the largest community of infosec professionals in the industry. Let's build a network that connects people, opportunities, and ideas. If you are involved in purchasing, selling, designing, deploying… or using information security solutions – this group is for you. Covered topics include compliance, encryption, anti-virus, malware, cloud security, data protection, hacking, network security, virtualization, and more.

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 3

Rambus Cryptography Research

1050 Enterprise Way, Suite 700,
Sunnyvale, CA 94089
www.Rambus.com

The Rambus Cryptography Research division specializes in embedded security solutions to combat the worldwide threat to data integrity. Our innovative technologies span areas including tamper resistance, content protection, network security, media and

payment and transaction services. Nearly nine billion security products are made annually with our security technology, and systems designed by our scientists and engineers protect billions of dollars in revenue every year. Additional information is available at rambus.com/security.

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

Association Sponsor

Trusted Computing Group

3855 SW 153rd Drive, Beaverton, Oregon 97003

www.trustedcomputinggroup.org

The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. Learn more about the TCG organization and technologies at www.TrustedComputingGroup.org.

Silver 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.

wolfCrypt FIPS

wolfSSL now has wofCrypt with FIPS 140-2 validation (Certificate #2425).

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

You have the option of rebranding the wolfCrypt module and NIST will issue a FIPS 140-2 certificate in your company's name.

The wolfSSL team has the FIPS expertise you need. Talk to us about it. We can save you time and money.

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, mobile phones, the cloud, and more.

wolfSSL wolfSSL 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 ChaCha20 and Poly1305.

wolfCrypt

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**.

wolfCrypt FIPS

wolfCrypt FIPS provides customers with a FIPS 140-2 validated (Certificate #2425) cryptography library. The wolfSSL team can add new operating environments and algorithms as needed in addition to accelerating FIPS projects by providing validated cryptography and testing services to our customers.

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

Badge Sponsor, Booth 7

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.

Booth 12

Zeva

11710 Plaza America Drive
Suite 2000, Reston, VA 20190

www.zevainc.com

Zeva is a technology-driven company delivering software solutions and expert consulting to commercial and government markets. Our principals have over 20 years experience building solutions for Microsoft technology, and optimizing the Microsoft software investments of our customers. We serve as a trusted Microsoft Architecture Advisor to more than half of our commercial and government clients, and we are proud to have earned a 100% customer satisfaction rating.

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

LEVERAGE FIPS VALIDATED CRYPTOGRAPHY TO MEET YOUR TIME TO MARKET NEEDS

IOT and Cloud based applications require developers to employ a "defense in depth" strategy using multiple layers of security services. Protecting sensitive consumer data, detecting and preventing a system compromise, and defending against unauthorized duplication and theft are all among the their top concerns.

With the inherent threats that come with connectivity, manufacturers are putting pressure on developers to deploy strong security, authentication, and encryption technologies to mitigate and reduce the risk of potential vulnerabilities in their designs.

Implementing Allegro's strong encryption technology and optimized device management and control platform helps developers build security and trust into their applications that provide persistent protection for sensitive data.

To learn more at ICMC 2015 visit Booth #10 and explore how Allegro's FIPS validated solutions deliver time to market and reduce risk for your specific application.

www.allegrosoft.com/ICMC2015

Allegro

Utimaco IS GmbH

Germanusstraße 4
D - 52080 Aachen
Germany

phone +49. 241. 16 96 - 200
fax +49. 241. 16 96 - 199

Utimaco Inc.

3790 El Camino Real
Palo Alto, CA 94306
United States of America

phone +1 650 485 4920
fax +1 650 485 4921

utimaco®

We keep your cryptographic keys safe

CryptoServer CSe-Serie

- Up to 1500 elliptic curve signatures per second
- Certified in accordance with FIPS 140-2-Level 4 for physical security
- Tamper responsive sensor foil technology
- Open internal programming interfaces
- PCIe or Network attached

Maximum security at the highest performance level.

SecurityServer

The multi purpose HSM

CryptoServer SDK

The Software Developement Kit

TimeStamp Server

Tramperproof Timestamp

Deutschland HSM

For secure ID solution

CryptoServer Se-Serie

- FIPS 140-2-Level 3
- Tamper resistant technology
- TRUE Random Number Generator AIS31
- Optimized for common security requirements
- HSM Software Simulator for rapid POC

Unrivalled level of reliability and quality in HSMs