

CONFERENCE PROGRAM



THE FOURTH

International Cryptographic Module Conference

ICMC16

PLATINUM SPONSOR



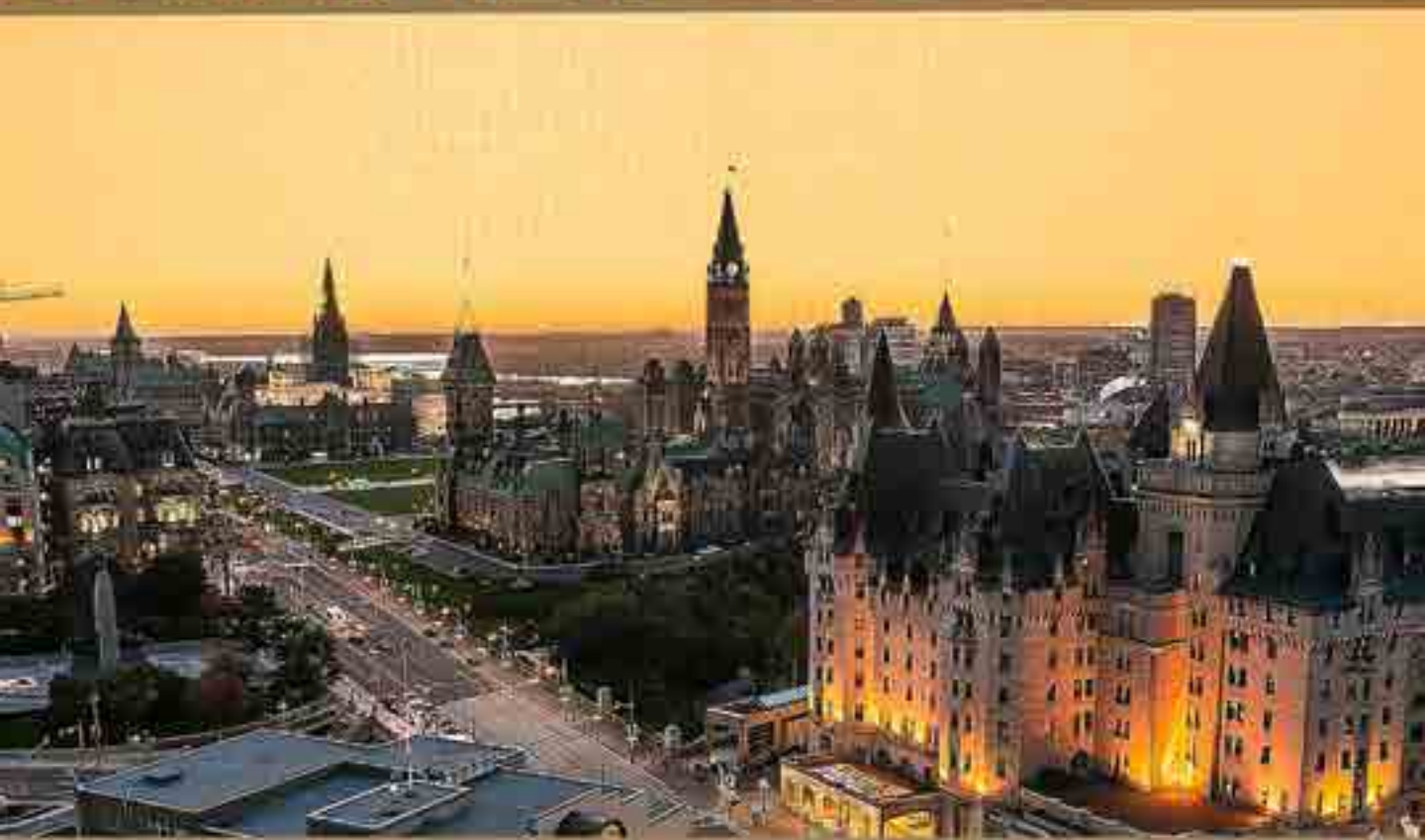
SILVER SPONSOR



SILVER SPONSOR

utimaco

SILVER SPONSOR



May 18-20, 2016 ■ Ottawa, Ontario, Canada

Welcome to the ICMC 2016

FIPS 140-2 can be a dry topic.
atsec information security
invites you to have a little fun...



ICMC 2014

Making Diamonds Out of Coal:
CST Labs Are Under Pressure
vimeo.com/112421140

ICMC 2015

Let It Go (RNG edition)
vimeo.com/144367433



ICMC 2016

Presidential Debate
FIPS 140-2 vs. ISO 19790
Come to Yi Mao's presentation
"Huh, Must be Encrypted?!"
4:10pm, Wed. May 18, Salon 213

Come and talk to us at our booth!

www.atsec.com

Welcome

Dear ICMC 2016 Participant,

Allow me to personally welcome you to the Fourth Annual International Cryptographic Module Conference (ICMC). The launch of the ICMC conference four years ago brought the cryptographic modules community together. Since that time the community has self-organized and collaborated, without any external influence. Its only goals have been to improve the standard, the tools and communication among all parties: the Cryptographic Module Validation Program (CMVP), vendors, laboratories, and consultants.

This year we've seen the CMVP make many positive changes including significantly shortening the review pending queue, streamlining implementation guidance (IG) updates, engaging labs for the working groups, taking input and improving communication.

ICMC is also changing to a new time of year to avoid conflicts with other conferences, and to our first location away from Washington DC to facilitate the international aspect of the conference. ICMC has extended to three full days and six topic tracks to accommodate more international speakers.

Wednesday, May 18th, begins with two exciting keynotes and continues with presentations on two tracks: Certification Programs and General Technology. During the afternoon break three contestants will be tested on FIPS validation trivia in the Cryptographic Module Game Program (CMGP), and the day will end with a Welcome Reception and the opening of the exhibits.

Thursday, May 19th, includes presentations on a new track: End-User Experience. Join us at the end of the day for a Wine & Cheese Reception in the exhibits area and be sure to participate in Dine Around Ottawa to enjoy dinner with your colleagues.

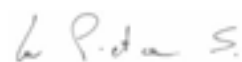
Friday May 20th, introduces new tracks: Common Criteria and Crypto, Advanced Technology, and Industry Vertical/Embedded Crypto. The exhibits close before the afternoon sessions, and the conference concludes with a Summary Panel Discussion, The Value of Certification in Other Industry Verticals.

The conference will enable open discussions, promote exchanges of ideas, and provide many opportunities to network, collaborate and share information. With attendees and presenters from around the globe, the aim is to build and shape an international standard and build strong relationships.

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

My personal respect and thanks to all of you,

Sal La Pietra



President & CEO
atsec information security

Table of Contents

Welcome	1
Sponsors	2
Agenda	3
Speakers	9
Sponsor Profiles	14

Program Committee

Michael Angelo, Micro Focus
Joshua Brickman, Oracle
Erin Connor, EWA-Canada (Chair)
Shawn Geddis, Apple
Tammy Green, Blue Coat Systems
Ryan Hill, atsec information security
Fiona Pattinson, atsec information security (Chair Emeritus)
Nithya Rachamadugu, CygnaCom (Chair)
Marcus Streets (Chair)
Steve Weingart, Aruba, an HP Enterprise Company

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.

Sponsoring Organizations

ICMC would not be possible without the support of these organizations.

Title Sponsors

PLATINUM SPONSOR



SILVER SPONSOR



SILVER SPONSOR



SILVER SPONSOR



Leading Sponsors

WATER SPONSOR



BADGE SPONSOR



LUNCH SPONSOR



BAG SPONSOR



Supporting Sponsors



Exhibitors



Association and Media Sponsors



LinkedIn Group



Conference Agenda

Detailed session descriptions are online at www.ICMConference.org

ICMC will be presented in plenary sessions and six tracks, over the course of three days:	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
Plenary Sessions (P) Industry overview topics are presented at the beginning and end of the conference.	User Experience Track (U) Information of interest to the cryptographic module end-user	Industry Vertical/Embedded Crypto Track (E) The application of embedded encryption in specific industry verticals	Common Criteria and Crypto Track (R) Encryption issues related to NIAP compliant products

Wednesday, May 18

- 9:00 **Welcome and Introduction**, Ryan Hill, Community Outreach Manager, atsec information security; **Cryptographic Module User Forum (CMUF) Overview**, Matt Keller, Vice President, Corsec; **Keynote: Building our Collective Cryptographic Community (P01a)** Scott Jones, Deputy Chief, Communications Security Establishment; **Keynote: Assuring the Faithfulness of Crypto Modules (P01b)** David McGrew, Cisco Fellow, Cisco Systems

10:15 **Networking Break (Rideau Canal Atrium)**

	Certification Programs Track	Salon 215	General Technology Track	Salon 213
10:45	Keynote: Overview of ISO 19790:2012 Revision (C02a) Randall Easter, Computer Security Division, STVM, NIST		Keynote: Modern Crypto Systems and Practical Attacks (G02a) Najwa Aaraj, Senior Vice President, Special Projects, DarkMatter	
11:35	CAVP—Inside the World of Cryptographic Algorithm Validation Testing (C02b) Sharon Keller, Computer Scientist, NIST		What is My Cryptographic Boundary? (G02b) Ying-Chong Hedy Leung, Senior Consultant, atsec information security corporation	
12:00	FIPS Inside (C02c) Carolyn French, Manager, Cryptographic Module Validation Program, Communications Security Establishment		Certification of Quantum Cryptographic Network Security Devices (G02c) Nino Walenta, Principle Research Scientist, Battelle Memorial Institute	
12:35	Lunch (Rideau Canal Atrium)	13:00 Cryptographic Module User Forum (CMUF) Update , Matt Keller, Corsec (Salon 215)		
13:35	Automated Run-time Validation for Cryptographic Modules (C03a) Apostol Vassilev, Technical Director, Research Lead—STVM, Computer Security Division, NIST; David McGrew, Cisco Fellow, Cisco Systems; Barry Fussell, Senior Software Engineer, Cisco Systems		Let's Talk About Physical Security (G03a) Steve Weingart, Manager of Public Sector Certifications, Aruba, an HP Enterprise company	
14:25	Introduction on the Commercial Cryptography Scheme in China (C03b) Di Li, Senior Consultant, atsec information security corporation		Standardized Testing of Public Algorithms (ECC and RSA) Using Test Vector Leakage Assessment (G03b) Gilbert Goodwill, Senior Principal Engineer, Rambus Cryptography Research; Michael Tunstall, Security Engineer, Rambus Cryptography Research Division	
14:50	The Current Status and Entropy Estimation Methodology in Korean CMVP (C03c) Yongjin Yeom, Kookmin University; Sangwoon Jang, Seog Chung Seo, National Security Research Institute		Analysis and Solutions for CAVS Testing Errors (G03c) Yuan Xu, Information Security Consultant, atsec information security corporation	
15:15	Networking Break (Rideau Canal Atrium)	Cryptographic Module Game Program , Nick Goble, Technical Marketing Engineer, Cisco (Salon 215)		
15:45	Germany and the Netherlands—Certification of Secure Cryptographic Modules (C04a) Leo Kool, Group Manager, BrightSight		Secure Access with Open Source Authentication (G04a) Donald Malloy, Chairman, OATH	
16:10	C04a (Continued)		Huh, Must be Encrypted?! (G04b) Yi Mao, Lab Director, atsec information security corp.	
16:35	The Open Trusted Technology Provider™ Standard (C04c) Erin Connor, Director, EWA-Canada		G04b (Continued)	
17:00	Welcome Reception in Exhibits (Exhibits Open, Salon 214)			

Thursday, May 19

Detailed session descriptions are online at www.ICMConference.org

	Certification Programs Track	Salon 215	General Technology Track	Salon 213
9:00	NIST and NIAP Working Together (C11a) Mary Baish, Deputy Director, NIAP; Matthew Scholl, Division Chief, Computer Security Division, NIST		Smartphone Keystores Compared (G11a) William Supernor, CTO, KoolSpan	
9:50	Side Channel Testing Requirements in 19790 (C11b) Randall Easter , Computer Security Division, STVM, NIST		/Dev/Random and your FIPS 140-2 Validation can be Friends (G11b) Valerie Fenwick, Software Engineering Manager, Oracle	
10:15	Testing Fault Injection and Side Channel in FIPS: Vision of a Smart Card Laboratory (C11c) Jose Ruiz Gualda, Common Criteria Leader, David Hernández García, R&D Engineer, Applus		Using /Dev/Urandom the Right Way (G11c) Stephan Mueller, Principal Consultant and Evaluator, atsec information security corp.	
10:40	Networking Break in Exhibits (Salon 214)			
11:10	Creating a Model of the FIPS 140 Testing and Validation Process with a View to Improving the Process (C12a) Kelvin Desplanque, Security Certification Engineer, Cisco Systems		An Overview of OpenSSL (G12a) Tim Hudson, CTO and Technical Director, Cryptsoft Pty Ltd.	
11:35	Objective Security Evaluation: Possibly Feasible, or Feasibly Possible? (C12b) Andrew Jamieson , Security Laboratories Manager, Underwriters Laboratories		Auditing OpenSSL (G12b) Kenneth White, Director & Co-Founder, Open Crypto Audit Project	
12:00	Validation Workflow (C12c) Carol Cantlon, IT Security Specialist, EWA-Canada		LibreSSL Introduction and Overview (G12c) Giovanni Bechis, Owner, System Administrator and Developer, SnB, Developer, OpenBSD	
12:25	Lunch in Exhibit Area, Sponsored by Oracle (Salon 214)			
13:35	Cryptographic Transition Planning Panel Discussion (C13a) Moderator: Ralph Spencer Poore, PCIP, CISSP, CISA, CFE, CHS-III, Director, Emerging Standards, PCI Security Standards Council; Panelists: Dawn Adams, PA and CST Lab Manager, EWA-Canada; Todd Arnold, Senior Technical Staff Member (STSM), IBM Master Inventor, IBM Cryptographic Coprocessor Development; Terence Spies, Chief Technologist, HP Security Voltage, Hewlett-Packard Enterprise, Subcommittee Chair, ANSI X9F1		Multi-Vendor Key Management with KMIP (G13a) Tim Hudson, CTO and Technical Director, Cryptsoft Pty ltd	
14:25	Modifying an Existing Commercial Product for Cryptographic Module Evaluation (C13b) Alan Gornall, Principal Consultant, Rycombe Consulting		Entropy: Finding Random Bits for OpenSSL (G13b) Denis Gauthier, Senior Software Development Manager, Oracle	
14:50	GlobalPlatform: Facilitating the Certification of Multi-Applications (C13c) Hank Chavers, Technical Program Manager, GlobalPlatform		Improving Module's Performance When Executing the Power-up Tests (G13c) Allen Roginsky, Mathematician, NIST	
15:15	Networking Break in Exhibits (Salon 214)			
15:45	Entropy Requirements Comparison between FIPS 140-2, Common Criteria and ISO 19790 Standards (C14a) Richard Wang, FIPS Laboratory Manager, Gossamer Security Solutions, Tony Apted, CCTL Technical Director, Leidos		GlobalPlatform's Secure Component and the Root of Trust (G14a) Olivier Van Nieuwenhuyze, Security Task Force Chair, GlobalPlatform, Senior R&D Engineer, STMicroelectronics	
16:30	Entropy As a Service: Unlocking the Full Potential of Cryptography (C14b) Apostol Vassilev, Research Lead–STVM, Computer Security Division, NIST		G14b. CTO Panel Discussion: The Future of Security (G14b) Moderator: Matt Keller, Vice President, Corsec; Panelists: Jon Geater, CTO, Thales e-Security; Gorav Arora, Director of Technology in the CTO Office, Gemalto; Jasper Van Woudenberg, CTO, North America, Riscure	
17:15	Wine & Cheese Reception in Exhibits (Salon 214) Depart for Dine-Around Ottawa (Sign up at Registration Desk)			

Thursday, May 19

End-User Experience Track

Salon 212

- 9:00 **Keynote: Worlds Collide: Are We Ready for Security at Warp Speed?** (U11a) Jon Geater, CTO, Thales e-Security
- 9:50 **The Pros and Cons of Using an Embedded FIPS Module vs. Validating an Entire Product** (U11b) Anthony Busciglio, Laboratory Manager, Acumen Security
- 10:15 **How Much is My Certification Really Worth—Keeping Standards Relevant in an Evolving World** (U11c) Graham Costa, Security and Certifications Manager, Gemalto; William Tung, Senior Security & Certifications Analyst, Gemalto
- 10:40 **Networking Break in Exhibits** (Salon 214)
- 11:10 **Getting Value for Money from Your Certification Investment** (U12a) Alan Gornall, Principal Consultant, Rycombe Consulting
- 11:35 **FIPS 140-2 Security Policy Template Review** (U12b) Ryan Thomas, FIPS 140-2 Program Manager, CGI Global Labs; Jennifer Cawthra, Security Testing, Validation and Measurement, NIST
- 12:00 **Requirements for Certification and Regulation to Secure IoT Devices** (U12c) Andreas Philipp, VP Marketing and Business Development, Utimaco
- 12:25 **Lunch in Exhibit Area, Sponsored by Oracle**
- 13:35 **FIPS Validated Cryptography with Back Doors: Oops!** (U13a) Valerie Fenwick, Software Engineering Manager, Oracle
- 14:25 **Reconciling Vulnerability Response with Certifications—Comparison of Experiences in Europe and USA** (U13b) Fabien Deboyser, Certification Engineer, Thales e-Security
- 14:50 **Show Me The Warrant: Why Encrypted Messages Are Like Cherry Pie for Uncle Sam** (U13c) Ray Potter, CEO & Founder, SafeLogic
- 15:15 **Networking Break in Exhibits** (Salon 214)
- 15:45 **The Life-Cycle of a Software Cryptographic Module** (U14a) Steven Schmalz, Principal Systems Engineer, RSA—the Security Division of EMC
- 16:10 **How to Build a Product Security Program with SDL & Certifications** (U14b) Ashit Vora, Co-founder and Laboratory Director, Acumen Security; Chris Romeo, Founder, Principal Consultant, Security Journey
- 17:00 **Wine & Cheese Reception in Exhibits** (Salon 214)

Take a Break Wednesday Afternoon

15:15-15:45 (Salon 215)

Cryptographic Module Game Program



Your Host: Nick Goble, Technical Marketing Engineer, Cisco Come watch three experienced contestants test their FIPS knowledge at the Cryptographic Module Game Program (CMGP). The CMGP covers FIPS validation trivia related to algorithms, derived testing requirements, entropy, implementation guidance and more. A few members from the audience will be selected to assist the contestants on specific questions and be eligible to win prizes.

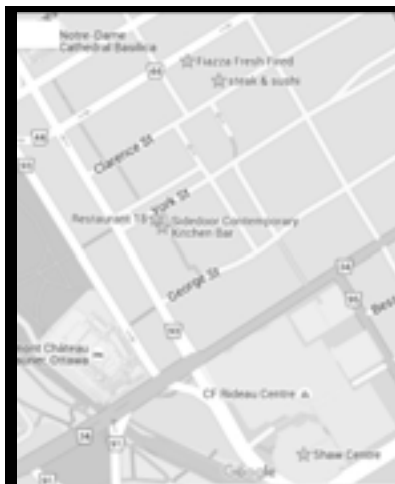
Thursday Lunch

Sponsored by

ORACLE

Friday, May 20

	Common Criteria and Crypto Track Salon 215	Advanced Technology Track Salon 213
9:00	Keynote: Securing Mobility through the Canadian Medium Assurance Solutions Program (R21a) Greg Hills, Director, Architecture & Technology Assurance, Communications Security Establishment (CSE)	A21a. Keynote: Quantum Computing Current Research and Standards for Quantum Safe Cryptography (A21a) Mark Pecen, CEO, Approach Infinity
9:50	NIAP Update (R21b) Dianne Hale, NIAP	Update on the Quantum Threat, Mitigation, and Relevant Timelines (A21b) Michele Mosca, University Research Chair and Co-Founder, Institute for Quantum Computing, University of Waterloo; Co-Founder & CEO, evolutionQ Inc., Canada
10:15	Cryptography and the Common Criteria in Canada (R21c) Cory Clark, IT Security Specialist, CSEC	Quantum Safety In Certified Cryptographic Modules (A21c) William Whyte, Chief Scientist, Security Innovation
10:40	Networking Break in Exhibits (Salon 214)	
11:10	Network Device Collaborative Cryptographic Module (R22a) Nick Goble, Technical Marketing Engineer, Cisco	Unboxing the White-Box: Practical Attacks Against Obfuscated Ciphers (A22b) Jasper van Woudenberg, CTO North America, Riscure
12:00	An Update from the CCUF Crypto Technical Working Group (R22b) Ashit Vora, Crypto Technical Working Group, Common Criteria Users Forum	Deep Tech Analysis to AES-GCM in TLS 1.2 and IPSec-v3 (A22b) Richard Wang, FIPS Laboratory Manager Gossamer Security Solutions; Ed Morris, Director, Gossamer Security Solutions
12:25	Lunch in Exhibits (Salon 214, Exhibits Close 13:40)	
13:40	The Economics of Security Certifications—FIPS 140-2, Common Criteria, and UC APL (R23a) John Morris, President, Corsec	An Approach for Entropy Assessment of Ring Oscillator-Based Noise Sources (A23a) Joshua Hill, Information Security Scientist, InfoGard Laboratories
14:30	The CC Threads within ISO 19790 (R23b) Iain Holness, Security Engineer, Cygnacom Solutions; Dayanandini Pathmanathan, Common Criteria Evaluator, CygnaCom CCCEL Canada	FIPS 202, the SHA-3 Standard (A23b) Michael Powers, Security Assurance Engineer, Leidos; Jason Tseng, CSTL Lab Manager, Leidos
15:00	Break (213-215 Foyer)	
15:10	Summary Panel Discussion: The Value of Certification in Other Industry Verticals (P24) (Salon 213) Moderator: Steve Weingart, Manager of Public Sector Certifications, Aruba, an HP Enterprise Company; Panelists: Mary Baish, Deputy Director, NIAP; Jon Green, Sr. Security Architect/CTO Federal Division, HP Enterprise; John Morris, President, Corsec; Shawn Wells, Chief Security Strategist, Public Sector Red Hat. What will it take for FIPS 140-2, ISO/IEC 19790, and Common Criteria to be a best practice or requirement in health care, automotive, financial, IoT and other industries? Adjourn 16:00.	



Join Your Colleagues: Dine-Around Ottawa

Sign up at the registration desk. Depart Thursday, May 19 at 17:30.

Enjoy an informal, on-your-own group dinner at one of the best restaurants in Ottawa's famous Byward Market district. Stop by the registration desk to grab a seat. Average dinner prices are shown.

Restaurant	CDN\$	Address	Type of Food
Fiazza Fresh Food	\$11-\$30	86 Murray St	Pizza/Italian
Restaurant 18	\$31-\$60	18 York St	Seafood/Steakhouse
SideDoor Contemporary	\$31-\$60	18b York St	Tapas & Small Plates
Steak & Sushi	\$31-\$60	87 Clarence St	Japanese

All restaurants are within walking distance. Meet Thursday at 17:30 during the wine and cheese reception in the exhibits, and depart from there. This is an "on your own" event—restaurants have reserved space for ICMC groups. Space is limited, so stop by the registration desk to save your seat.

Friday, May 20

Industry Vertical/Embedded Crypto Salon 212

- 9:00 **Keynote: Crypto as a Service (CaaS) for Embedded Security Infrastructures** (E21a) Matt Landrock, CEO, Cryptomathic
- 9:50 **Security Credential Management System (SCMS) Applications Beyond Vehicle to Vehicle Safety** (E21b) Brian Romansky, Vice President Strategic Technology, TrustPoint Innovation
- 10:15 **Connected Car Security in the V2X Infrastructure** (E21c) Richard Soja, Senior Principal Engineer, NXP
- 10:40 **Networking Break in Exhibits** (Salon 214)
- 11:10 **Cryptographic Modules for the Internet of Things** (E22a) Carol Cantlon, IT Security Specialist, EWA-Canada; Lawrence Dobranski, DSc, MBA, MSc (Eng), P.Eng., Director, ICT Security, Access & Compliance, Professional Affiliate, Department of Computer Science, University of Saskatchewan
- 12:00 **Hardware-Intrinsic Identity for Mobile Payments** (E22b) John Wallrabenstein, Chief Scientist, Sypris Research
- 12:25 **Lunch in Exhibits (Salon 214, Exhibits Close 13:40)**
- 13:40 **IoT and Security: A Defense in Depth Perspective** (E23a) Loren Shade, VP Marketing, Allegro Software
- 14:30 **Experience and Challenges with Encryption in Mobile Communications**, (E23b) James Muir, Senior Security Analyst, Graphite Software
- 15:00 **Break** (213-215 Foyer)
- 15:10 **Summary Panel Discussion: The Value of Certification in Other Industry Verticals** (P24) (Salon 213) Adjourn 16:00.

Conference Presentations

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

Password: XXXXXX

WiFi Access

WiFi Options at the Shaw Centre

CDN\$10 for 3 hours

CDN\$15 for 24 hours

CDN\$45 for the entire event (up to 5 days)

To Connect

- Search wireless networks and connect to **Freeman AV WiFi**
- Open your web browser and select credit card payment option
- Enter the required information and click "Continue."

WiFi is provided by the Shaw Centre. ICMC is not responsible for WiFi service.

Join the Conversation on Twitter



#CryptoModConf

Speakers

Speaker biographies are online at www.ICMConference.org



Dr. Najwa Aaraj

Senior Vice President, Special Projects, DarkMatter

G02a



Dawn Adams

PA and CST Lab Manager, EWA-Canada

C13a



Michael Angelo

Chief Security Architect, Micro Focus

Program Committee



Tony Apted

CCTL Technical Director, Leidos

C14a



Todd Arnold

Senior Technical Staff Member (STSM), IBM Master Inventor, IBM Cryptographic Coprocessor Development

C13a



Mary Baish

Deputy Director, NIAP

C11a & P24



Giovanni Bechis

Developer, Open BSD

G12c



Joshua Brickman

Director, Security Evaluations, Oracle

Program Committee



Tony Busciglio

Co-founder & Laboratory Director, Acumen Security

U11b



Jennifer Cawthra

Security Testing, Validation and Measurement, NIST

U12a



Carol Cantlon

IT Security Specialist, EWA-Canada

C12c



Hank Chavers

Technical Program Manager, Global Platform

C13c

GUARDED BY GENIUS.



GOVERNANCE,
RISK &
COMPLIANCE



CYBER NETWORK
DEFENCE



MANAGED
SECURITY
SERVICES



SECURE
COMMUNICATIONS



INFRASTRUCTURE
& SYSTEM
INTEGRATION



SMART
SOLUTIONS

**DARKMATTER UNITES THE BRIGHTEST
MINDS WITH THE MOST INNOVATIVE
TECHNOLOGY, AGAINST ONE OF THE
WORLD'S GREATEST THREATS:
ADVANCED CYBER-ATTACKS**

Working from the United Arab Emirates and Canada, we are a team of cyber security specialists dedicated to providing secure, trusted and integrated protection services globally. As a strategic partner to governments, we have the proven integrity, intelligence and security standards to safeguard city and nation.

To find out more about the next generation of cyber security visit **darkmatter.ae**



SPEAKERS



Cory Clark

IT Security Specialist, CSEC

R21c



Erin Connor

Director, EWA-Canada

Program Committee Chair & C04c



Graham Costa

Security and Certifications Manager, Gemalto

U11c



Fabien Deboyser

Certification Engineer, Thales e-Security

U13b



Kelvin Desplanque

Security Certification Engineer, Cisco Systems Limited

C12a



Dr. Lawrence Dobranski

P.Eng, Director, ICT Security, Access, & Compliance, University of Saskatchewan

E22a



Randall Easter

Computer Security Division, STVM, NIST

C02a & C11b



Valerie Fenwick

Software Engineering Manager, Oracle

G11b & U13a



Carolyn French

Manager, Cryptographic Module Validation Program

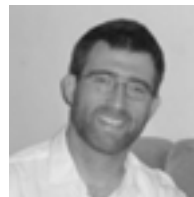
C022c



Barry Fussel

Software Technical Leader, Cisco Systems

C03a



Denis Gauthier

Senior Software Development Manager, Oracle

G11c



Jon Geater

CTO, Thales e-Security

U11a & G14b



Shawn Geddis

Security & Certifications Engineer, Apple Inc.

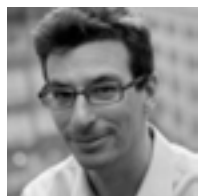
Program Committee



Nick Goble

Technical Marketing Engineer, Cisco

R22a & PM Break Wednesday

**Gilbert Goodwill**

Senior Principal Engineer, Rambus
Cryptography Research

G03b**Alan Gornwall**

Principal Consultant, Rycombe
Consulting

U12b & C13b**Jon Green**

Sr. Security Architect/CTO
Federal Division, HP Enterprise

P24**Tammy Green**

Senior Principal Security Architect,
Blue Coat Systems

Program Committee**Diane Hale****NSA****R21b****David Hernandez Garcia**

R&D Engineer, Applus

C11c**Joshua Hill**

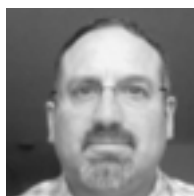
Information Security Scientist,
InfoGard Laboratories

A23a**Ryan Hill**

Community Outreach Manager,
atsec information services

Program Committee**Gregory Hills**

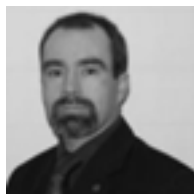
Director, Architecture and
Technology Assurance,
Communications Security
Establishment (CSE)

R21a**Lain Holness**

Security Engineer, Cygnacom
Solutions

R23b**Tim Hudson**

CTO and Technical Director,
Cryptsoft Pty Ltd.

G12a & G13a**Andrew Jamieson**

Security Laboratories Manager,
Underwriters Laboratories

C12b**Sangwoon Jang**

National Security Research
Institute

C03c**Scott Jones**

Deputy Chief, IT Security,
Communications Security
Establishment

P01a

SPEAKERS



Matt Keller

Vice President, Corsec

P01 & G14b



Sharon Keller

Computer Scientist, NIST

G02b



Leo Kool

Group Manager, BrightSight

C04b



Matt Landrock

CEO, Cryptomathic, Inc.

E21a



Hedy Leung

Senior Consultant, atsec China

G02b



Di Li

Senior Consultant, atsec China

C03b



Donald Malloy

Chairman, OATH

G04a



Yi Mao

Lab Director, atsec information security

G04b



David McGrew

Cisco Fellow, Cisco Systems

P01b & C03a



Edward Morris

Co-Founder, Gossamer Security Solutions

A22b



John Morris

President, Corsec

R23a & P24



Michele Mosca

University Research Chair and Co-Founder, Institute for Quantum Computing, University of Waterloo; Co-Founder & CEO, evolutionQ Inc., Canada

A21b



Stephan Mueller

Principal Consultant and Evaluator, atsec information security

G13b



James Muir

Senior Security Analyst, Graphite Software

E23b



Dayanandini Pathmanathan

Criteria Evaluator, CygnaCom
CCCEL Canada

R23b



Mark Pecan

CEO, Approach Infinity

A21a



Andreas Philipp

VP Marketing and Business
Development, Utimaco IS GmbH)

U12c



Ray Potter

CEO & Founder, SafeLogic

U13c



Michael Powers

Security Assurance Engineer,
Leidos

A23b



Ralph Spencer Poore

PCIP, CISSP, CISA, CFE, CHS-
III, Director, Emerging Standards,
PCI Security Standards Council

C13a



Nithya Rachamadugu

Director, Cygnacom

Program Committee



Allen Roginsky

Mathematician, NIST

G13c



Brian Romansky

Vice President Strategic
Technology, TrustPoint Innovation

E21b



Chris Romeo

Common Criteria Leader, Applus
Laboratories

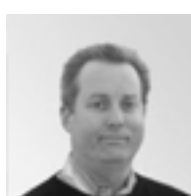
U14b



Jose Ruiz Gualda

Common Criteria Leader, Applus
Laboratories

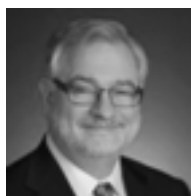
C11c



Bill Rutledge

Project Director, ICMC

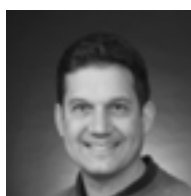
Program Committee



Steve Schmalz

Principal Systems Engineer, RSA—
the Security Division of EMC

U14a



Matthew Scholl

Deputy Division Chief, Computer
Security Division, NIST

C14a

SPEAKERS



Seog Chung Seo

National Security Research
Institute

C03c



Loren Shade

VP Marketing, Allegro Software

E23a



Richard Soja

Senior Principal Engineer, NXP

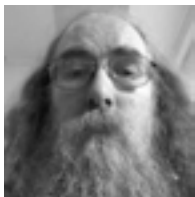
E21c



Terrence Spies

Chief Technologist, HP Security
Voltage

C13a



Marcus Streets

Program Committee



William Supernor

CTO, KoolSpan

G11a



Ryan Thomas

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

U12b



Jason Tseng

CSTL Lab Manager Leidos

A23b



William Tung

Senior Security & Certifications
Analyst, Gemalto

U11c



Michael Tunstall

Security Engineer, Rambus
Cryptography Research Division

G03b



Oliver Van Nieuwenhuyze

Chair of the GlobalPlatform
Security Task Force,
GlobalPlatform

G14a



Jasper Van Woudenberg

CTO North America, Riscure

G14b



Apostol Vassilev

Research Lead-STVM,
Computer Security Division,
NIST

C03a, C14b



Ashit Vora

Co-Founder & Lab Director,
Acumen Security

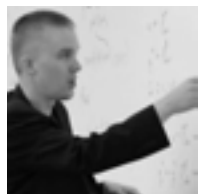
U14b, R22b



Zhiqiang [Richard] Wang

FIPS Laboratory Manager,
Gossamer

C14a, A22b



John Wallrabenstein

Chief Scientist, Sypris Research

E22b



Nino Walenta

Principle Research Scientist,
Battelle Memorial Institute

G02c



Steve Weingart

Manager of Public Sector
Certifications, Aruba, an HP
Enterprise Company

G03a, P24



Shawn Wells

Chief Security Strategist, Public
Sector, Red Hat

P24



Kenneth White

Director & Co-Founder, Open
Crypto Audit Project

G12b



William Whyte

Chief Scientist, Security Innovation

A21c



Yuan Xu

Information Security Consultant,
atsec information security corp.

G03c



Yongjin Yeom

Kookmin University

C03c



wolfCrypt FIPS

wolfSSL now has wolfCrypt 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

Exhibit Floor Plan



- | | |
|--|---|
| 1. atsec information security | 8. DarkMatter |
| 3. Rambus Cryptography Research | 10. Whitewood Encryption Systems |
| 4. Oracle | 13. ACT Canada |
| 5. Allegro Software Development | 14. Communications Security Establishment |
| 6. Brightsight | 15. Utimaco |
| 7. InfoSec Global/Asgard Cyber Assurance | 17. WolfSSL |

Sponsors & Exhibitors



Association Sponsor,
Booth 13

ACT Canada

Canada

www.actcda.com

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



Event Sponsor

Acumen Security

United States

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.



Your One Stop Shop For Government Certification

FIPS 140 | Common Criteria | FedRAMP | Secure Supply Chain | SCAP

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



Event Sponsor

AEGISOLVE

United States

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.



Silver Sponsor, Booth 10



**Allegro Software
Development**

United States

www.allegrosoft.com

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.

Platinum Sponsor, Booth 9



**atsec information
security**

United States

www.atsec.com

atsec information security is an independent, privately owned company that focuses on providing laboratory and consulting services for information security. We address commercial and government sectors around the world. Our consultants are expert in a variety of technologies including operating systems, databases, and network devices. Our laboratories specialise in evaluating and testing commercial products, using international standards to help provide assurance to end-users about the products they buy and use. We focus on assisting organizations, large and small, achieve compliance with

standards such as Common Criteria, FIPS 140-2, O-TTPS, PCI, ISO/IEC 27001 and FISMA and offer a variety of services that complement that goal



Booth 6

Brightsight

Netherlands

www.brightsight.com

Devices that store secure data require protection on both hardware and software level. Thorough security evaluation of Integrated Circuits, software applications and systems is mandated by industry schemes and organisations, to protect sensitive data. Without certification, security products cannot be launched. Brightsight offers security evaluations and certificates on behalf of the major payment schemes and industry organisations to ensure the right level of security is obtained. These services are provided to IC manufacturers, (embedded) secure device manufacturers, smart card suppliers and service providers such as banks/payment institutions. Brightsight can assure the quickest turn-around time of product evaluations. We have the most accreditations from industry organisations, the largest team of security evaluators and the most extensive evaluation equipment

Lab Showcase



COACT

United States

www.coact.com

COACT, Inc. is a Service Disabled Veteran Owned Small Business (SDVOSB). With over 25 years of history, COACT has evolved into a leading provider of independent verification and validation services (IV&V) in addition to supporting commercial and government clients in understanding and fulfilling their risk management and compliance needs. The COACT Lab is an independent test facility accredited for Common Criteria evaluations, FIPS 140-2 validations and SCAP testing. In addition, COACT is an ISO 9001:2015 registered company and a FedRAMP Accredited 3PAO. Our tiered service offerings range from focused efforts to address specific security objectives, to providing full information security programs for clients in commercial, healthcare, regulatory, defense, and intelligence domains.



COACT

Your one stop shop for all of your independent verification, validation and certification needs!

✓ FIPS 140-2	✓ NIST 800-171
✓ Common Criteria	✓ ICD-503
✓ SCAP Testing	✓ HIPAA
✓ DISA UC APL Consulting	✓ PCI DSS
✓ FedRAMP	✓ CDM
✓ FISMA	✓ DIACAP to DIARMF

www.COACT.com
info@coact.com
301.498.0150

With unimpeached ethics, COACT remains free from real or perceived conflicts of interest and does not engineer, manufacture, or resell any products.

Association Sponsor



Common Criteria User Forum

United States

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.

Booth 14

Communications Security Establishment

Canada

www.cse-cst.gc.ca



CSE is Canada's national cryptologic agency. Unique within Canada's security and intelligence community, CSE employs code-makers and code-breakers to provide the Government of Canada with information technology security (IT Security) and foreign signals intelligence (SIGINT) services. CSE also provides technical and operational assistance to federal law enforcement and security agencies.

Water Sponsor

Computer Sciences Canada Inc. (CSC)

Canada

www.csc.com



CSC leads clients on their digital transformation journey, providing innovative next-generation technology solutions and services that leverage deep industry expertise, global scale, technology independence and an extensive partner community. Our people help commercial and international public sector clients solve their toughest challenges by modernizing their business processes, applications and in infrastructure with next-generation technology solutions. CSC is a global provider of security testing services with facilities in Australia, Canada, and the United States. CSC's Canadian lab, located in Kanata, Ontario, is staffed by Government of Canada security cleared and accredited IT security experts. In addition to our core security testing services, we also provide consulting, risk assessment, vulnerability testing, and training services. For more information regarding CSC's global security testing capabilities please contact Maureen Barry, mbarry5@csc.com.



Association Sponsor
COUNTERMEASURE

Canada

www.countermeasure.ca

Now celebrating its fifth year in Ottawa, COUNTERMEASURE 2016 is Canada's premier government focused IT security conference. If you are interested in connecting with, talking to and hearing from the IT security community, there is no better platform than COUNTERMEASURE 2016. Past speakers have included globally recognized industry security experts, representatives from the Government of Canada, and some of the world's foremost security specialists from the private sector. Attendees have the option of attending three days of professional skills training prior to the two-day main conference. Enjoy a 20% discount at COUNTERMEASURE 2016 by registering at www.countermeasure.ca with discount code CMICMC16.



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

United States

www.cygnacom.com

Cygnacom Solutions Inc. specializes in information assurance and product certification. We offer a full range of security certification, testing and consultancy services enabling our clients to meet 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 compliance. Cygnacom Solutions laboratories are accredited to conduct FIPS 140-2 cryptographic module (CMVP) and algorithm testing and Common Criteria evaluations in US (NIAP), Canada (CSE) and Turkey (TSE).
Contact: Nithya@cygnacom.com



Badge/Lanyard Sponsor
Booth 8

DarkMatter

United Arab Emirates

www.darkmatter.ae

DarkMatter is an international cyber security company headquartered in the UAE. It is staffed by a team of tier one cyber security specialists with global experience, dedicated to providing secure, trusted and integrated cyber protection services to governments and enterprise. DarkMatter offers a complete portfolio of cyber security solutions underpinned by industry leading intelligence, research and development (R&D). Supported by R&D facilities in the UAE and Canada, DarkMatter develops its own intellectual property. The company also cooperates and partners with a range of vetted, global technology leaders in the development of products and solutions. DarkMatter does not just implement; we innovate, creating new security solutions to combat tomorrow's security threats today.



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

Canada

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

Canada's Premier provider of IT Security
Certification and Consulting Services
for 28 years.

Visit us at www.ewa-canada.com or
send email to info@ewa-canada.com to
discover how we can help you achieve
your Information and Communications
Technology Certification and
Accreditation goals.

**Visit us at the
Laboratory Showcase**



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: www.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



**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.

Booth 7



InfoSec Global/ Asgard Cyber Assurance

Canada

www.infosecglobal.com

InfoSec Global is a provider of premium, validated information security solutions. Our team of world-renowned cryptographers and cyber security professionals deliver customized and localized software, hardware and assurance solutions to our customers around the world. Asgard Cyber Assurance provides 3rd party security-testing and cyber assurance expertise for custom and commercial software/hardware products. We also specialize in turnkey design & delivery of custom & localized lab facilities worldwide. All Asgard solutions are based on industry best practices and industry-leading processes. Asgard Cyber Assurance is a division of InfoSec Global, Inc.



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.

Association Sponsor



OASIS

www.oasis-open.org

OASIS is a nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for security, Internet of Things, cloud

computing, energy, content technologies, emergency management, and other areas. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology. OASIS members broadly represent the marketplace of public and private sector technology leaders, users and influencers. The consortium has more than 5,000 participants representing over 600 organizations and individual members in more than 65 countries. OASIS is distinguished by its transparent governance and operating procedures.

Lunch Sponsor, Booth 4



Oracle

United States

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

United States

www.rambus.com/security

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.

ORACLE[®] **11**
SOLARIS



Oracle **SOLARIS 11.3**

SECURITY, SPEED, SIMPLICITY.

ORACLE IS PROUD TO SPONSOR

The ICMC16 Conference

Oracle Solaris 11

Protect all your data, everywhere, all the time.

CONNECT WITH US:



blogs.oracle.com/solaris



facebook.com/oraclesolaris



twitter.com/oracle_solaris



oracle.com/solaris

Integrated Cloud Applications & Platform Services

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. Oracle and Solaris are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

ORACLE[®]



Event Sponsor

Riscure

Netherlands

www.Riscure.com

Riscure is an international and independent security test laboratory founded in 2001 by Marc Wittman, 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

United States

www.SafeLogic.com

SafeLogic provides strong encryption products for solutions in mobile, server, Cloud, appliance, wearable, and IoT environments that are pursuing compliance to strict regulatory requirements. Our flagship product, CryptoComply, offers FIPS 140-2 validated cryptographic operations with Suite B algorithms in a module designed for drop-in compatibility with OpenSSL & Bouncy Castle. This allows SafeLogic customers to achieve instant compliance for federal deployments and to receive a FIPS 140-2 validation in their own company name, with no additional engineering effort or interaction with labs, in approximately 8 weeks. SafeLogic was established in 2012, is privately held, and is headquartered in Palo Alto, California.



Booth 2

Synopsys

United States

www.synopsys.com

Through its Software Integrity Platform, Synopsys provides advanced solutions for improving the quality and security of software. This comprehensive platform of automated analysis and testing technologies integrates seamlessly into the software development process and enables organizations to detect and remediate quality defects, security vulnerabilities, and compliance issues early in the software development lifecycle, as well as gain security assurance and visibility throughout their software supply chain.



Association Sponsor

Trusted Computing Group

United States

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

United States

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.

Booth 10



Whitewood

United States

www.whitewoodencryption.com

Whitewood addresses the challenge of random number generation across the datacenter, remote devices and distributed applications. Without truly random numbers, security systems that rely on cryptography are weakened. Whitewood utilizes a quantum source originally developed at Los Alamos National Laboratory to generate pure entropy and true random numbers at speeds of up to 200Mbit/s. The Whitewood Entropy Engine is a convenient PCIe card that easily integrates with local or networked applications. Visit online at www.whitewoodencryption.com.



Silver Sponsor Booth 17

WolfSSL

United States

www.wolfssl.com

wolfSSL is an open source Internet security company whose primary products include the wolfSSL embedded SSL/TLS library, wolfCrypt embedded crypto engine, and wolfCrypt FIPS module. Primary users are programmers building security functionality into their applications and devices. wolfSSL employs the dual licensing model, offering products under the GPLv2 as well as a standard commercial license. wolfSSL's products are designed to offer optimal performance, rapid integration, the ability to leverage hardware crypto, and support for the most current standards. All products are designed 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 @ May 9, 2016

Najwa Aaraj, Vice President - Special Projects, DarkMatter	Liu Chih-Ang, TTC Telecom Technology Center	SEPTIMIU-EUGEN FILIP, diplomatic agent, Embassy of Romania in Ottawa	Joshua Hill, Information Security Scientist, InfoGard Laboratories (a UL Company)
Admir Abdurahmanovic, VP Strategy, PrimeKey Solutions AB	Seog Chung Seo, Senior member of engineering staff, National Security Research Institute	James Fox, Computer Scientist, NIST	Ryan Hill, Consultant, atsec information security
Arnold Abromeit, CST Laboratory Manager, TUViT	Cory Clark, IT Security Specialist, CSE	Jose Francisco Ruiz Gualda, Common Criteria Leader, Applus Laboratories	Greggory Hills, Director, Architecture & Technology Assurance, CSEC
Richard Adams, IT Security Specialist, EWA-Canada	Alyson Comer, Senior Software Engineer, IBM	Carolyn French, Manager, Cryptographic Module Validation Program, Communications Security Establishment	Kaleb Himes, Engineer, wolfSSL INC
Dawn Adams, PA and CST Lab Manager, EWA-Canada	Erin Connor, Director, EWA-Canada	Ken Fuchs, Principal Staff Engineer, Motorola Solutions	Iain Holness, Common Criteria Evaluator, Security Engineer, Cygnacom Solutions
Saman Adham, Senior Manager, TSMC Design technology Canada	Christopher Constantinides, Principal Security Technologist, Wind River	Barry Fussell, Technical Leader, Cisco Systems	David Hook, Bouncy Castle/Crypto Workshop
Matthew Appler, CEO, Corsec Security, Inc.	David Cornwell, Lead Engineer, Booz Allen Hamilton	Denis Gauthier, Senior Software Development Manager, Oracle	Tim Hudson, CTO, Cryptsoft Pty Ltd
Anthony Apted, CCTL Technical Director, Leidos	Graham Costa, Security and Certifications Manager, Gemalto	Mark Gauvreau, CC Lab Manager, EWA-Canada	Brian Hwang, CGI
Todd Arnold, Senior Technical Staff Member, IBM	Bruno Couillard, President & CTO, Crypto4A	Timothy Gaylor, Chief Security Architect, Citrix	Marc Ireland, FIPS Program Manager, InfoGard/UL
Gorav Arora, Director of Technology, CTO, Gemalto	Jason Cunningham, CST Laboratory Manager, Computer Sciences Canada, Inc.	Jon Geater, CTO, Thales e-Security	Deden Irfan Afriansyah, Staff of Crypto Device Subdirectorate, Lembaga Sandi Negara
Mary Baish, NIAP	James Dean, FIPS 140-2 Tester, CGI	Shawn Geddis, Security & Certifications Engineer, Apple Inc.	Andrew Jamieson, Underwriters Laboratories
Indhu Balraj, Manager, Software Test Engineering, Brocade	Jatin Deshpande, Sr. Technical Account Manager, Giesecke & Devrient America Inc	Nick Goble, Cisco	Sangwoon Jang, Senior member of engineering staff, National Security Research Institute
Alexander Barclay, Product Line Manager, KEMP Technologies	Jatin Deshpande, Giesecke & Devrient America Inc	Juan Gonzalez, Technical Lead - Formal Lab Services, BAE Systems	Alex Johns, Security Engineer, COACT, Inc.
Mark Bauschke, Distinguished Engineer, Juniper Networks, Inc.	Kelvin Desplanque, Security Certification Engineer, Cisco Systems, Ltd,	Gilbert Goodwill, Senior Manager/DPA Team Lead, Rambus - Cryptography Research Division	David Johnston, Intel Corporation
Giovanni Bechis, SNB S.r.l.	Ignacio Dieguez, Certification Engineer, Thales e-Security	Alan Gornall, Principle Consultant, Rycombe Consulting	Mladen Jurkovic, Information Systems Security Bureau
Steve Beers, Product Security Specialist, Xerox	Lawrence Dobranski, Director, ICT Security, Access, & Compliance, University of Saskatchewan	Christophe GOYET, Technical Marketing Director, Oberthur Technologies	Vivek Kallankara, Sales Engineer, Synopsys
Chris Bender, Vice President - Secure Communications, DarkMatter	Ivica Draganjac, Information Systems Security Bureau	Bryan Grandy, VP of Engineering, Texas RT Systems	Yasuhiko Kawai, Security Evaluator, Information Technology Security Center
Chris Bender, Vice President - Secure Communications, Dark Matter LLC	Randall Easter, Electronics Engineer, NIST	Constantine Grantcharov, TrustPoint Innovation Technologies Ltd.	Alan Kaye, Director, Compliance Management, Fortinet
Erc Betts, Sr. Mgr, Security Programs, VMware, Inc.	Nevine Ebeid, Principal Engineer, TrustPoint Innovation Technologies, Ltd.	John Gray, Software Developer, Entrust Datacard	Matt Keller, Vice President, Corsec
Marc Boire, Lab Director, CGI	Jack Edington, Principal Systems Engineer, Rockwell Collins	Tammy Green, Senior Principal Security Architect, Blue Coat Systems	Sharon Keller, CAVP Program Manager, NIST
Joshua Brickman, Director, Security Evaluations, Oracle Corp.	Scott Ellett, Principal Software Engineer, Oracle	Jon Green, CTO, Government Solutions, Aruba / HPE	Rich Kelm, Account Manager, wolfSSL INC
Jean Brisard, Canadian Federal Employee	Ken Elliott, Principal Engineering Specialist - IA, The Aerospace Corp	Warren Grunbok, Sr Security Strategy Architect, IBM	John Kohnen, IT Security Specialist, EWA-Canada
Mike Brown, CTO, ISARA Corporation	Jose EMILIO RICO MARTA NEZ, Technical Manager, Epoche & Espri, SLU	Risto Hakala, Senior Specialist, Finnish Communications Regulatory Authority	Leo Kool, group manager, Brightsight BV
Trevor Brown, Sr Principal Product Manager, CA Technologies	Michael Eng, Technical Director, Asgard Labs	Dianne Hale, Department of Defense	Lucas Koops, Principal Software Developer, Entrust Datacard
Chris Brych, Senior Principal Security Analyst, Oracle	Randy Eyamic, Security Certification Manager, BlackBerry	Ian Hall, Blue Coat	Yann LAC TM Hyver, SERMA SAFETY & SECURITY
Gus Burgess, IT Security Engineer, CSC	Fernando F Fuentes, Federal Compliance Manager, Hewlett Packard Enterprise	Mark Hanson, Program Manager, Intel Corporation	ALAIN LACHAPELLE, Siemens Canada Limited
Robert Burns, CSO, Thales e-Security	Andreas Fabis, Marketing Director, atsec information security	Robert Harland, Canadian Federal Employee	Matt Landrock, CEO, Cryptomathic
Anthony Busciglio, Lab Manager, Acumen Security	Samuel Farthing, Software Engineer, Cisco	Steve Hayes, Sales Manager, Synopsys	Nicolas Larabie, IT Security Specialist, EWA-Canada
Jean Campbell, Canadian Federal Employee	Valerie Fenwick, Software Development Manager, Oracle	Kevin Healy, Executive Director Marketing and Corporate Communications, DarkMatter	Trevor Larock, Staff Engineer, Juniper Networks
Blair Canavan, General Manager, Asgard Cyber Assurance		Ying-Chong Hedy Leung, Senior Consultant, atsec information security corp.	Jason Lawlor, president, lightship security
Carol Cantlon, Senior Evaluator, EWA-Canada			Di Li, atsec
Denise Cater, IT Security Consultant, Icon Security Limited			Jaz Lin, Product Line Manager, Juniper Networks
Jennifer Cawthra, Program Manager, NIST			Johannes Lintzen, VP Sales and Business Development, Utimaco Inc.
Hank Chavers, Technical Program Manager, GlobalPlatform			

Shih-Lien Linus LU, Director, Taiwan Semiconductor Manufacturing Company, Ltd.	Zumrut Muftuoglu, Manager of Cyber Security Certification Department, Turkish Standards Institution	Ferenc Rakoczi, sw. engineer, Oracle Hungary	Tsun-Te Tsui, TUV NORD Asia Pacific
Emily Litz, Director, PwC	James Muir, Senior Security Analyst, Graphite Software	Steve Ratcliffe, TME, Cisco Systems	Benjamin Tucker, Citrix
Kun-shan Liu, Telecom Technology Center.	John Mulholland, Director, Quantum Risk Management, evolutionQ Inc.	Qusyairi Ridho, Staff of Crypto Device Subdirector, Lembaga Sandi Negara of Republic Indonesia	william tung, gemalto
Laurie Mack, Director Security & Certifications, Gemalto	Jerome Myers, Senior Engineering Specialist, The Aerospace Corporation	Carlie Robbins, Security & Certifications Analyst, Gemalto	Michael Tunstall, Security Engineer, Rambus Cryptography Research
Alex MacPherson, Communications Security Establishment	Tim Myers, Security Program Manager, Microsoft	Allen Roginsky, Mathematician, NIST	Lachlan Turner, Ark Infosec Labs Inc.
Smita Mahapatra, Security and Certification Analyst, Gemalto	Fathi Nasraoui, Cygnacom solutions	John Roman, Senior Software Engineer, F5 Networks	Anthony Ungerman, Director, Product Security, Citrix Systems
Rumman Mahmud, Compliance Engineer, Cisco Systems, Inc.	Brian Neill, Director, Product Management, Infosec Global	Brian Romansky, VP Strategic Technology, TrustPoint Innovation	Bob Van Andel, President, Allegro Software
Donald Malloy, Chairman, OATH	Dana Neustadter, Sr. Manager of Product Marketing, Synopsys	Chris Romeo, CEO, Security Journey	Olivier Van Nieuwenhuyze, Security System Architect, STMicroelectronics / GlobalPlatform
Yi Mao, CST Lab Manager, atsec information security corporation	Kerrie Newton, Fortinet Technologies Inc	Doug Rossie, Vice President, Business Development and Partnerships, SafeLogic	Jasper Van Woudenberg, CTO Riscure North America, Riscure
Chris Marks, Federal Program Manager, Brocade	Van Nguyen, JUNIPER NETWORKS	Bill Rulledge, Director, Cnxt Media Corp.	Apostol Vassilev, Research Lead - STVM, CSD, NIST
Luther Martin, Distinguished Technologist, Hewlett Packard Enterprise	Charles Nightingale, Sr Manager, CSC	Genya Sakurai, IPA	Ashit Vora, Co-Founder and Laboratory Director, Acumen Security
Manoj Maskara, VMware, Inc.	Denis Niles, Sr Design Specialist - Mobile Devices, TELUS Communications	William Sandberg-Maitland, Principal Scientist, SPYRUS Inc.	Nino Walenta, Principle Research Scientist, Battelle
David Maxwell, Chief Security Officer, InfoSec Global	Martin Oczko, Product Manager, PrimeKey Labs	Rory Saunders, Senior Security Analyst, COACT, Inc.	John Ross Wallrabenstein, Staff Research Scientist, Sypris Electronics
Alexander Mazuruc, Senior Software Developer, WinMagic Inc	Gesa Ott, Head of Cryptographic Analysis, Utimaco IS GmbH	Stephen Savard, Canadian Federal Employee	Richard Wang, Lab Manager, Gossamer Security Solutions
mike mccarll, ICOSA Labs	Gesa Ott, Head of Cryptographic Analysis, Utimaco IS GmbH	Steve Schmalz, CISSP Principal Systems Engineer, RSA, The Security Division of EMC	Patrick Warley, Head Of R&D, Integral Memory
Daniel McCarthy, Canadian Federal Employee	Mike Ounsworth, Software Developer, Entrust Datacard	Nikolaus Schnitzer, Head of electronic engineering, mils electronic gmbh&co	Steve Weingart, Manager of Public Sector Certifications, Aruba, a Hewlett Packard Enterprise company
Matthew McGehee, Lab Director, COACT, Inc.	Steve Pate, Chief Architect, HyTrust	Matt Scholl, Deputy Division Chief, Computer Security Division, NIST	Shawn Wells, Chief Security Strategist, Public Sector, RedHat
David McGrew, Cisco Fellow, Cisco Systems	Dayanandini Pathmanathan, Cygnacom Solutions	Jonathan Sero, IT Security Specialist, EWA-Canada	Debbie White, Canadian Federal Government
Greg McLearn, Lightship Security, Inc.	Mark Pecan, CEO, Approach Infinity	Loren Shade, VP Marketing, Allegro Software	William Whyte, Chief Scientist, Security Innovation
Gregory McNulty, VP/GM of Sales, NA, InfoSec Global	Andreas Philipp, VP Business Development, utimaco	Keelan Smith, Vice President, Research & Development, InfoSec Global	Clint Winebrenner, Technical Lead, FIPS, Cisco Systems, Inc.
Paul Meadowcroft, Director, Product Management, Thales UK Ltd	Shawn Pinet, Senior Certifications Analyst, Gemalto	Jonathan Smith, Senior Security Tester, Cygnacom Solutions	Kwok Wong, CygnaCom Solutions, Inc.
Michael Mehlberg, Senior Director, Sales, Rambus Cryptography Research	Bob Pittman, Hewlett Packard Enterprise	Hamid Sobouti, Federal Certification Program Manager, Brocade	Jesse Wood, IT Security Specialist, EWA-Canada
Keith Merlo, Canadian Federal Employee	Diana Polulyakh, VP of Marketing, Advanced Data Security	Richard Soja, Automotive Electronics Systems Engineer, NXP	Brian Wood, Device Security Certification Manager, Samsung Research America
Alexandre Miede, Director, Lightship Security	Eugene Polulyakh, General Manager, Advanced Data Security	Daniel Southern, Systems Security, Oracle	Paul Wouters, Sr. Software Engineer, Red Hat
Mark Minnoch, Technical Account Manager, SafeLogic	Ralph Spencer Poore, Director, Emerging Standards, PCI Security Standards Council	Travis Spann, AEGISOLVE	Yuan Xu, atsec information security corporation
Johannes Mittmann, Federal Office for Information Security	Holly Porteous, Analyst, Library of Parliament	Terrence Spies, Chief Technologist, HP Security Voltage	Tatsuya Yanagisawa, General Manager, CM Testing, ECSEC Laboratory Inc.
Edward Morris, Lab Director, Gossamer Security Solutions	Ray Potter, CEO & Founder, SafeLogic	Ron Starman, EWA-Canada	Yongjin Yeom, Professor, Kookmin University
John Morris, President, Corsec	Michael Powers, Info Security, Leidos	Rob Stubbs, Product Director, Ultra Electronics AEP	cheng-hsien yu, Telecom Technology Center
Michele Mosca, Institute for Quantum Computing, University of Waterloo & evolutionQ Inc.	Alan Presser, Engineer, Allegro Software	William Supernor, CTO, Koolspan	Li Yu Wang, Project Manager, TUV NORD Asia Pacific
Nagy Moustafa, CEO, InfoSec Global & Asgard Cyber Assurance	Nikki Principe, CNXTD Event Services	Erin Swanson, Austin Sigma, Inc.	
Tomas Mraz, FIPS Tech Lead, Red Hat	Bradley Proffitt, Special Projects - Labs, DarkMatter	Ryan Thomas, FIPS 140-2 Program Manager, CGI Global Labs	
Stephan Mueller, Principal Consultant, atsec information security corporation	Brian Pruss, Motorola Solutions, Inc.	Mike Thompson, PCI SSC	
	Nithya Rachamadugu, Director, Cygnacom Solutions Inc	Peter Tsai, Principal Product Architect, Vometric	
		Jason Tseng, Software Engineer, Leidos, Inc.	



utimaco®

We keep your cryptographic keys safe

CryptoServer CS-Serie

- 100% FIPS 140-2 approved hardware and software
- Certified 256-bit drive with 1024-bit RSA and 256-bit symmetric encryption
- Single user interface and management
- Open standard (PKCS#11) interface
- PCI 3.0 (Express/Gen2)

utimaco AG, 70372 Stuttgart, Germany



SecurityServer

The most purpose HSM



CryptoServer SDK

The Software Development Kit



TimeStamp Server

Geographical TimeStamp



Deutschland HSM

The German ID card chip

CryptoServer Se-Serie

- 100% FIPS 140-2 approved
- German standard technology
- High performance hardware and software
- Open standard (PKCS#11) interface
- PCI 3.0 (Express/Gen2)

utimaco AG, 70372 Stuttgart, Germany





INTERCONNECTED IOT DEVICES REQUIRE LAYERED SECURITY SERVICES

LEVERAGE FIPS VALIDATED CRYPTOGRAPHY TO MEET YOUR IOT SECURITY NEEDS

As the number of interconnected IoT devices continues to increase, security concerns are growing at an exponential rate. In an interconnected IoT ecosystem, a single vulnerability on a single device can be an opening for attacking thousands of devices. In light of the sensitive data that IoT devices can access and take action upon, embedded developers must adopt a security-focused approach when creating IoT devices and cloud based applications.

Allegro's strong encryption technology and suite of lightweight connectivity and security toolkits enable project teams to meet compressed timelines while helping mitigate and reduce the risk of potential vulnerabilities in their designs.

To learn more at ICMC 2016 visit Booth #5 and explore how Allegro's FIPS validated solutions deliver time to market and reduce risk for your specific application.

www.allegrosoft.com/ICMC2016

