



Improving Security Together

PAST THE FADED PERIMETER

Threat & Incident Response

INTERCONTINENTAL MIAMI | USA
JUNE 13-18, 2010



22nd ANNUAL
FIRST MIAMI
CONFERENCE

It is with great joy and pleasure that I welcome you to the 22nd Annual FIRST conference here in Miami, Florida.

In the next couple of days, we will treat you to expert presentations on a great number of fascinating topics in security. You will have the opportunity to take away good ideas/solutions based on knowledge, expertise and lessons learned from events that presenters and attendees alike will share. The only challenging task is for each attendee to make the most of this week in whatever fashion that suits them. If you can do that, I promise you the conference will deliver an unforgettable week.

This year's conference theme (Past the Faded Perimeter) really speaks to our security community's current state. When you think about the type of year it has been for security, you see a lot of change. As security professionals, we have had to deal with complex threat events that outstrip the technologies we have in place today. This coupled with economic uncertainties has stretched security professionals ingenuity in order to incorporate flexible and viable security strategies. The need for smarter tactics and strategies has never been so prominently highlighted. This is why I believe that the FIRST organization is more critical now than when it was formed two decades ago.

The evolution of new technologies like cloud computing, virtualization and social media computing is ushering in a new transition for corporate technology. This new transition is opening up an era where owner operated solutions are being replaced by lighter-weight services to add more capacity and save costs. The only question that nags me is this, "what about the perimeter?" In the days where we deployed owner operated solutions, we scaled our perimeter defense to protect our assets. In a new lighter services world, that perimeter is altered in some facets; faded from the perspective we once knew and understood. These changes will challenge us as a collaborative security community to evolve our Threat and Incident Response processes.

It's important this week to take the time to think, talk and exchange ideas about challenges and possible solutions. Last but not least, make that all too important connection with your colleagues. This is what FIRST is truly about. It's what we on the Steering Committee at times refer to as "Trusted Connections." These trusted connections are what foster our community and help us to share and collaborate - a key component needed to solve global problems in the long term.

I would like to thank a few people for putting together this wonderful opportunity to gather, share, and connect. First, I would like to thank all the keynotes and expert speakers who are sharing their time, knowledge, and experience with us this week. I would like to thank this year's Program Chair, Andrew Cushman, and the rest of the program committee who worked so tirelessly to create a spectacular program. Thank you Pete, Phoebe, Traci, and Kristen - without your year round dedication, this conference would not be as memorable as I know it will be. To the Steering Committee members, and their employers, who dedicate time and resources to help keep this organization strong and viable year round, I thank you. And, last but not least, I thank you, the attendees and members, as you are the key reason for this gathering. I hope you enjoy this conference as much as I know I will.

Welcome again! I know we are going to have a great conference and I hope to see many of you next year in Vienna.




STEPHEN ADEGBITE
Chairman, FIRST.Org
Microsoft Corporation, US

**2009-2010
STEERING COMMITTEE**

KENNETH VAN WYK | Vice Chair
KRvW Associates LLC, US

CHRIS GIBSON | CFO
Citigroup, UK

PETER ALLOR | Conference Liaison
IBM, US

THOMAS MULLEN | CEP Liaison
BT, UK

DERRICK SCHOLL
Oracle, US

YURIE ITO
ICANN, Japan

SCOTT MCINTYRE
KPN-CERT, NL

JORDI VILÀ AGUILÀ
La Caixa, ES

KURT SAUER
Spinlock Technologies, Japan/US

FIRST SECRETARIAT

FIRST.Org, Inc.
 PO Box 1187
 Morrisville, North Carolina
 27560-1187
 United States of America

first-sec@first.org

REGISTRATION OFFICE

FIRST.Org, Inc.
 Conference Coordination Office
 213 W. Institute Place, Suite 405
 Chicago, Illinois 60610
 United States of America

first-2010@first.org
 +1.312.646.1013

VENUE INFORMATION

InterContinental Hotel Miami
 100 Chopin Plaza
 Miami, Florida 33131
 United States of America

<http://www.icmiamihotel.com>
 +1.305.577.1000

FIRST WEBSITES

<http://www.first.org>
<http://conference.first.org>

**LOST & FOUND
 REGISTRATION DESK**

Please bring lost items to the registration desk. The conference staff will hold all lost items until the conference close on Friday, June 18th. Items that have not been claimed will be discarded or donated.

Welcome Letter & 2009-2010 Steering Committee.....2

Table of Contents & Office Information.....3

Attendee Notes.....4

Reminders & Conference Policies.....5

Program-at-a-Glance.....6

Floor Plans.....7

Conference Program.....8-15

 Sunday.....8

 Monday.....9

 Tuesday.....10-11

 Wednesday.....12-13

 Thursday.....14

 Friday.....15


Keynote Speakers.....16-17

Exhibitors.....18-19

Program Committee, Staff & About FIRST.....20

SAVE THE DATE: FIRST 2011 VIENNA.....21

2010 Conference Sponsors.....Back Cover

 LIVE CONFERENCE UPDATES @FIRSTDOTORG
 Hashtag #FIRST2010



CONFERENCE NOTES

Lined area for writing conference notes.



INTERNET ACCESS 2ND LEVEL MEETING ROOMS

Free wireless internet will be available to attendees throughout the 2nd Level meeting rooms for the duration of the conference.

For access, please use the following:

SSID: FIRST2010
WPA2: firstmia10

If you have trouble connecting, please ask for assistance at the registration desk.

Attendees are responsible for internet access in their sleeping rooms.

NETWORK MONITORING PRIVACY STATEMENT

Cisco's Computer Security Incident Response Team (CSIRT) has developed a mobile monitoring and networking solution for providing on-site network and computer security monitoring during conferences and events. The first use of the solution at FIRST 2007 was showcased in a Cisco-on-Cisco article. The CSIRT team monitors 2-3 events per year with this kit, and usually sends 1-2 people to each event to provide security monitoring and a follow-up report.

For more information, please visit <http://www.first.org/conference/monitoring>.

You may direct questions about this setup, such as the network, security, or privacy assurances, to the Cisco team by emailing first-2010-miami@cisco.com.

CONFERENCE POLICIES

Please note the following policies will be in effect during the conference. We ask for your compliance in respecting the privacy of your fellow attendees and limiting distraction and interruptions of the speakers and presenters.

ATTENDEE LIST

Unless the Conference Office has received an explicit request from a registrant disallowing to share their contact information (through the Registration Form), a list of all attendees, their affiliation institutions and email addresses will be included in the delegate packs. Please note this delegate list is for personal contact use only and may not be used for marketing purposes or shared with other individuals or sources. Violation of this information sharing policy may result in suspension from FIRST and future events.

MOBILE DEVICES

A kind reminder to please turn-off or silence all mobile devices during conference sessions.

PHOTOGRAPHY, VIDEOGRAPHY & VOICE RECORDING

Photography, videography and voice recording of any FIRST Conference sessions is strictly prohibited. If the policy is violated, the offender will be issued a warning. Any second offense may result in removal (non-refundable) from the conference.

Photography will be permitted at the following FIRST Conference events: Ice Breaker Reception, Vendor Showcase and Wednesday Banquet.

SOCIAL MEDIA

Please use common sense and respect during conference week. Any individual caught disclosing information from a closed session or a members-only meeting will be issued a warning. Any second offense may result in removal (non-refundable) from the conference.

Use of any social media medium is strictly prohibited during the Annual General Meeting (AGM), this includes, but is not limited to: Twitter, Facebook, IRC, blogging, etc. Any communications are for those in physical attendance at the AGM. Exceptions can only be granted by the FIRST Steering Committee for a limited purpose.

PRESS

All press must pre-registered with the FIRST Secretariat (first-sec@first.org) and have been granted approval to attend sessions by the FIRST Conference Liaison.

Any opinions expressed are that of the individual and not FIRST.

SECTION REMOVED FOR WEB VERSION

*Meeting rooms are all on the 2ND LEVEL unless otherwise noted.

MONDAY | JUNE 14

0845-1030	Conference Opening & Keynotes	Versailles
1030-1100	Networking Break	Grand Ballroom Foyer
1100-1200	General Session	Versailles
1200-1330	Lunch	Mezzanine East & West
1330-1530	Track I: Incident Response	Versailles
1330-1530	Track II: Management	Trianon
1330-1530	Track III: Technical	Chopin
1530-1600	Networking Break	Grand Ballroom Foyer
1530-1700	Track I: Incident Response	Versailles
1530-1700	Track II: Management	Trianon
1530-1700	Track III: Technical	Chopin
1700-1800	Lightning Talks	Versailles

TUESDAY | JUNE 15

0845-1050	Opening Remarks & Keynotes	Versailles
1050-1110	Networking Break	Grand Ballroom Foyer
1110-1200	General Session	Versailles
1200-1330	Lunch	Mezzanine East & West
1330-1530	Track I: Incident Response	Versailles
1330-1530	Track II: Management	Trianon
1330-1530	Track III: Technical	Chopin
1530-1600	Networking Break	Grand Ballroom Foyer
1600-1700	Track I: Incident Response	Versailles
1600-1700	Track II: Management	Trianon
1600-1700	Track III: Technical	Chopin
1700-1930	Vendor Showcase	Grand Ballroom Foyer

WEDNESDAY | JUNE 16

0845-1050	Opening Remarks & Keynotes	Versailles
1050-1110	Networking Break w/Exhibitors	Grand Ballroom Foyer
1110-1200	General Session	Versailles
1200-1330	Lunch & Open Exhibits	Mezzanine East & West
1330-1530	Day 2: Joint FIRST/ICANN	Versailles
1330-1530	Track II: Management	Trianon
1330-1530	Track III: Technical	Chopin
1530-1600	Networking Break w/Exhibitors	Grand Ballroom Foyer
1600-1700	Day 2: Joint FIRST/ICANN	Versailles
1600-1700	Track II: Management	Trianon
1600-1700	Track III: Technical	Chopin
1600-1800	Lightning Talks	Versailles
1900-2200	Conference Banquet	Poolside on Plaza Level

THURSDAY | JUNE 17

0845-1030	Opening Remarks & Keynote	Versailles
1030-1100	Networking Break w/Exhibitors	Grand Ballroom Foyer
1100-1200	General Session	Versailles
1200-1300	Lunch & Open Exhibits	Mezzanine East & West
1300-1500	Track I: Incident Response	Versailles
1300-1500	Track II: Management	Trianon
1300-1500	LECC-SIG	Chopin
1500-1830	AGM (Members Only)	Versailles

FRIDAY | JUNE 18

0845-1000	Opening Remarks & Keynote	Versailles
1000-1200	Track I: Incident Response	Versailles
1000-1200	Track II: Management	Trianon
1000-1200	Track III: Technical	Chopin
1200-1330	Lunch & Open Exhibits	Mezzanine East & West
1330-1430	Track I: Incident Response	Versailles
1330-1430	Track II: Management	Trianon
1330-1430	Track III: Technical	Chopin
1430-1500	Closing Remarks	Versailles

**SUNDAY, JUNE 13
PRE-CONFERENCE**

1330-1700
Day I: FIRST/ICANN Workshop
Theatre Room

1330-1730
Vendor SIG Meeting
Windsor

1800-1900
2010 Session Chairs Meeting
Windsor

1830-1900
Newbies Meet & Greet
Lobby Level - Bayfront AB

1900-2100
Ice Breaker Reception - All
Lobby Level - Bayfront AB

**VENDOR SHOWCASE
GRAND BALLROOM FOYER**

Tuesday 1700-1930

Network with your peers while meeting sponsor security teams and incident response technology vendors. Special raffles and FIRST membership information will also be available. Beer and light snacks will be provided. See page 18-19 for a full listing of exhibitors.



REGISTRATION
MEZZANINE EAST

Sunday	1400-1800
Monday-Wednesday	0800-1600
Thursday-Friday	0800-1500

CONTINENTAL BREAKFAST
MEZZANINE EAST & WEST

Monday-Friday	0800-0845
---------------	-----------

LUNCH
MEZZANINE EAST & WEST

M, T, W, F	1200-1330
Thursday	1200-1300

GEEK LOUNGE & BRAIN BAR
ESCORIAL & ALHAMBRA

Monday-Friday	1200-1700
---------------	-----------

ICE BREAKER RECEPTION
SUNDAY | JUNE 13
LOBBY LEVEL BAYFRONT AB

Newbies Meet & Greet	1830-1900
General Conference Attendance	1900-2100

VENDOR SHOWCASE
GRAND BALLROOM FOYER

Tuesday	1700-1930
---------	-----------

CONFERENCE BANQUET
POOLSIDE ON PLAZA LEVEL

Wednesday	1900-2200
-----------	-----------

ANNUAL GENERAL MEETING - MEMBERS ONLY
VERSAILLES

Thursday	1500-1830
----------	-----------

*Must have valid government issued photo ID for entry



SUNDAY | JUNE 13

1330-1700	Day I: Joint FIRST/ICANN Workshop <i>Theatre Room</i> *Limited to 150 seats. Pre-registered attendees will be seated first. First-come, first-served for remaining seats.
1330-1430	Fundamentals of DNS - How DNS operates, hierarchical structure, organizational dependence via case study on checkfree.com Chris Evans ICANN
1430-1500	Coffee Break
1500-1700	Attack Scenario Demonstrations 1. Cache Poisoning 2. Name Server Redirection 3. Malicious Use of DNS Chris Evans ICANN
1330-1730	Vendor Special Interest Group (Vendor-SIG) Windsor
1400-1800	Registration Mezzanine East
1800-1900	2010 Session Chairs Meeting Windsor
1830-1900	FIRST Newbies & 1st Time Attendees Meet & Greet with the FIRST Steering Committee <i>Lobby Level Bayfront AB</i> Relaxed dress code – t-shirts, shorts and sandals!
1900-2100	Ice Breaker Reception <i>Lobby Level Bayfront AB</i> Relaxed dress code – t-shirts, shorts and sandals!

GEEK LOUNGE & BRAIN BAR**ESCORIAL & ALHAMBRA | M-F 1200-1700**

Make sure to stop by the lounge & bar starting Monday @ Noon. Special snacks, smoothie bar and Wii consoles will be available to attendees. A power-up corner will also be available.

In addition, Terremark will be offering goodies including giveaways, raffles and tours to their flagship facility, the NAP of the Americas®.

Sponsored by 

YOU LIKE WINNING FREE STUFF RIGHT?**REGISTRATION DESK**

Stop by the registration desk and drop off your business card for a chance to win one of ten titles. Winners will be announced throughout the week! Special thanks to Syngress Publishing for providing the books.

0800–1600	Registration <i>Mezzanine East</i>		
0845–0900	Conference Opening & Welcome <i>Versailles</i> Stephen Adegbite Chairman, FIRST.Org Senior Security Program Manager Lead, Microsoft Corporation, US		
0900–1030	Keynote: Cybersecurity Collaboration: Partnering Across the Cyber Ecosystem <i>Versailles</i> Philip R. Reiting Deputy Under Secretary for the National Protection and Programs Directorate (NPPD) Director of the National Cybersecurity Center (NCSC) U.S. Department of Homeland Security		
1030–1100	Networking Break <i>Grand Ballroom Foyer</i>		
1100–1200	How Change to All-IP World Impact Attack Scenarios and How CERT Teams Can Be Prepared? <i>Versailles</i> Anu Puhakainen Michael Skogberg Ericsson, FI		
1200–1330	Lunch <i>Mezzanine East & West</i>		
	TRACK I: INCIDENT RESPONSE <i>Versailles</i>	TRACK II: MANAGEMENT <i>Trianon</i>	TRACK III: TECHNICAL <i>Chopin Ballroom</i>
1330–1430	Incident Response to Social Engineering Attacks Ramses Martinez VeriSign, US	Know Thy Enemy: Cataloguing Agents of Threat for Improved Risk Assessments Timothy Casey Steve Mancini Intel Corporation, US	Targeted Intrusions & Cyber Espionage—Wake Up! Steven Adair Shadowserver Foundation, US
1430–1530	Got Spies in Your Wires? Marshall Heilman MANDIANT, US	Understanding the Insider Threat: Lessons Learned from Actual Insider Cyber Crime Randall Trzeciak CERT/CC, US	Portable Destructive File(PDF) Attacks and Analysis Mahmud Ab Rahman CyberSecurity Malaysia(MyCERT), MY
1530–1600	Networking Break <i>Grand Ballroom Foyer</i>		
1600–1700	Security in a Peer to Peer World Adrian Asher Skype, US	R&D Projects Launched in Response to the Dynamic Evolution of Internet Security Threats—CERT View Krzysztof Silicki CERT Polska / NASK, PL	Locale-specific Threats: Security Challenges Due to Globalization Anthony Bettini McAfee, US
1700–1800	Lightning Talks <i>Versailles</i> Sign-up sheet is available at the registration desk. Participants have 5-minutes to present. No sales presentations.		

TUESDAY | JUNE 15

0800-1600	Registration Mezzanine East		
0845-0900	Opening Remarks <i>Versailles</i> Stephen Adegbite Chairman, FIRST.Org Senior Security Program Manager Lead, Microsoft Corporation, US		
0900-1000	Keynote: Why Attackers Win <i>Versailles</i> Dave Aitel CTO, Immunity, US		
1000-1050	Incident Response at Scale <i>Versailles</i> Heather Adkins Google, US		
1050-1110	Networking Break Grand Ballroom Foyer		
1110-1200	Your Other Network's Attack Surface <i>Versailles</i> Fabian "Fabs" Yamaguchi Recurity Labs GmbH, DE		
1200-1330	Lunch Mezzanine East & West		
	TRACK I: INCIDENT RESPONSE <i>Versailles</i>	TRACK II: MANAGEMENT <i>Trianon</i>	TRACK III: TECHNICAL <i>Chopin Ballroom</i>
1330-1430	CERT-EE and CERT-FI: AbuseHelper framework for community-wide automated abuse handling Juhani Eronen CERT-FI, FI Anto Veldre CERT-EE, EE	13 Things to Consider Before DNSSEC John Kristoff Team Cymru, US	Cyber[Crime/War] – Drawing the Hidden Links Iftach "Ian" Amit Security & Innovation, IL
1430-1530	Cooperation and Self-regulation of Polish ISPs in Combating Online Crime Przemek Jaroszewski CERT Polska / NASK, PL	Risk Intelligence: Business Intelligence Meets Information Security Matt White Intel Corporation, US	Opt-in Social Protesting Botnet Günter Ollmann Damballa, US
1530-1600	Networking Break Grand Ballroom Foyer		

DID YOU KNOW...

Did you know that this year's conference theme was submitted by Steve Mancini of Intel? Theme winners receive a complimentary pass to the conference. Keep a look out in January 2011 when we start the search for the 2012 theme.

WEDNESDAY | JUNE 16

0800-1500	Registration Mezzanine East		
0845-0900	Opening Remarks <i>Versailles</i> Stephen Adegbite Chairman, FIRST.Org Senior Security Program Manager Lead, Microsoft Corporation, US		
0900-1000	Keynote: Securing Europe's Information Society <i>Versailles</i> Dr. Udo Helmbrecht Executive Director, ENISA		
1000-1050	That Pesky Critical Infrastructure <i>Versailles</i> Jason Larsen Idaho National Laboratory U.S. Department of Defense		
1050-1110	Networking Break with Exhibitors Grand Ballroom Foyer		
1110-1200	The Botnet Ecosystem <i>Versailles</i> Vitaly Kamluk Kaspersky Lab, RU & JP		
1200-1330	Lunch Mezzanine East & West		
	DAY II: FIRST/ICANN WORKSHOP <i>Versailles</i>	TRACK II: MANAGEMENT <i>Trianon</i>	TRACK III: TECHNICAL <i>Chopin Ballroom</i>
1330-1430	DNS Organizational Structure Yurie Ito Greg Rattray ICANN	Clearing the Brush: Lessons Learned in Gutting a CIRT and Rebuilding with Free Tools Michael La Pilla NetCentrics, US	Fingerprinting Malware Developers Rich Cummings HBGary, US
1430-1500*	DNS Incident Response Tips Andre Ludwig CACI Robert Schischka CERT.at, AT	After the Acquisition: A Software Security Assurance Perspective Bruce Lowenthal Oracle, US	Phishing Malware vs. Brazilian Banks: What each side is doing to raise the bar Ivo Peixinho Brazilian Federal Police, BR Jacomo Piccolini RNP/ESR, BR
1500-1530*	DNS Incident Response Tips (continued)	After the Acquisition: A Software Security Assurance Perspective (continued)	Understanding and Combating Man-in-the-Browser Attacks Jason Military SecureWorks, US
1530-1600	Networking Break with Exhibitors Grand Ballroom Foyer		

* Track III from 1430-1530 is broken out into two 30-minute sessions.

THURSDAY | JUNE 17

0800-1500	Registration Mezzanine East		
0845-0900	<p>Opening Remarks <i>Versailles</i></p> <p>Stephen Adegbite Chairman, FIRST.Org Senior Security Program Manager Lead, Microsoft Corporation, US</p>		
0900-1030	<p>Keynote: Cloudification-Indiscriminate Information Intercourse Involving Internet Infrastructure <i>Versailles</i></p> <p>Christofer Hoff Director, Cloud and Virtualization Solutions, Cisco Systems, US</p>		
1030-1100	Networking Break with Exhibitors Grand Ballroom Foyer		
1100-1200	<p>Panel Discussion: Implications of the Cloud <i>Versailles</i></p> <p>Moderator: Andrew Cushman, Microsoft Corporation, US</p> <p>Panelists: Christofer Hoff, Cisco Systems, US Jose Nazario, Arbor Networks, US Udo Schweigert, Siemens, DE</p>		
1200-1300	Lunch Mezzanine East & West		
	TRACK I: INCIDENT RESPONSE <i>Versailles</i>	TRACK II: MANAGEMENT <i>Trianon</i>	TRACK III: TECHNICAL <i>Chopin Ballroom</i>
1300-1400	<p>Incident Response in Virtual Environments: Challenges in the Cloud</p> <p>Bryan Casper Russ McRee Microsoft Corporation, US</p>	<p>Supply Chain Assurance: Incident Response in the Global IT Supply Chain</p> <p>Hart Rossman SAIC, US</p>	<p>Law Enforcement/CSIRT Co-operation Special Interest Group (LECC-SIG)</p>
1400-1500	<p>Forensics Considerations in the Next Generation Cloud Environments</p> <p>Robert Rounsavall Terremark, US</p>	<p>Critical Functions: A Functions Based Approach to IT Sector Risk Assessment</p> <p>Scott Algeier IT-ISAC, US Jerry Cochran Microsoft Corporation, US</p>	<p>LECC-SIG (continued)</p>
1500-1830	<p>Annual General Meeting (AGM) Versailles **Members Only. **Must have valid government issued photo ID for entry. **Please be prompt. Once doors have closed, you will not be permitted entry. No exceptions.</p>		

FRIDAY | JUNE 18

0800-1500	Registration <i>Mezzanine East</i>		
0845-0900	Opening Remarks <i>Versailles</i> Stephen Adegbite Chairman, FIRST.Org Senior Security Program Manager Lead, Microsoft Corporation, US		
0900-1000	Keynote: Who Moved My Cheese? Why The Security Industry Has Been Turned Upside Down <i>Versailles</i> John N. Stewart Vice President and Chief Security Officer, Cisco Systems, US		
	TRACK I: INCIDENT RESPONSE <i>Versailles</i> *AM Coffee Breaks in Rooms	TRACK II: MANAGEMENT <i>Trianon</i> *AM Coffee Breaks in Rooms	TRACK III: TECHNICAL <i>Chopin Ballroom</i> *AM Coffee Breaks in Rooms
1000-1100	Hands-on Computer Forensics with FOSS Tools Sandro Melo Locaweb, BR Nelson Uto CPqD, BR	Intrusion Response Reality Check Jamie Butler Kris Harms MANDIANT, US	A Day in the Life of a Web Application Kenneth van Wyk KRvW Associates, LLC, US
1100-1200	Hands-on Computer Forensics with FOSS Tools (continued)	Challenges for Digital Forensic Acquisition on Virtualization and Cloud Computing Platforms Christopher Day Terremark, US	Getting Ahead of Malware Jeff Boerio Intel Corporation, US
1200-1330	Lunch <i>Mezzanine East & West</i>		
1330-1430	Ad hoc File System Forensics Andreas Schuster Deutsche Telekom AG, DE	Building a Fortune 5 CIRT Under Fire Richard Bejtlich General Electric, US	Dragon Research Group Security Distro Dave Dobrotka Dragon Research Group Team Cymru, US Jacomo Piccolini RNP/ESR, BR
1430-1500	Closing Remarks <i>Versailles</i> Stephen Adegbite Chairman, FIRST.Org Senior Security Program Manager Lead, Microsoft Corporation, US		

WANT TO BE PART OF THE VIENNA 2011 PROGRAM?

Interested in presenting at 2011? Interested in becoming a member of the 2011 Program Committee? Head over the Registration Desk for details, or introduce yourself to Gavin Reid of Cisco Systems, our 2011 Program Chair.

MONDAY | JUNE 14 @ 0900-1030



PHILIP R. REITINGER

Deputy Under Secretary for the National Protection and Program Directorate (NPPD) Director of the National Cybersecurity Center (NCSC), U.S. Department of Homeland Security

Philip R. Reitingger was appointed by U.S. Department of Homeland Security (DHS) Secretary Janet Napolitano to serve as the Deputy Under Secretary for the National Protection and Programs Directorate (NPPD) on March 11, 2009. In this role, Reitingger leads the Department's integrated efforts to reduce risks across physical and cyber infrastructures. He oversees the coordinated operational and policy functions of the Directorate's subcomponents, which include Cybersecurity and Communications (CS&C), Infrastructure Protection (IP), Risk Management and Analysis (RMA), and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program.

On June 1, 2009 Reitingger also became the Director of the National Cybersecurity Center (NCSC), which is charged with enhancing the security of federal networks and systems by collecting, analyzing, integrating and sharing information among interagency partners. In this role, Reitingger is responsible for coordinating situational awareness and reporting for federal cybersecurity organizations and personnel.

As Deputy Under Secretary for NPPD and Director of NCSC, Reitingger provides strategic direction to the Department's cybersecurity efforts while ensuring preparedness and response capabilities across all federal computer systems.

Prior to joining DHS, Mr. Reitingger was the Chief Trustworthy Infrastructure Strategist at Microsoft Corporation. In that role, he worked with government agencies and private sector partners to enhance cybersecurity and infrastructure protection. In November 2001, Mr. Reitingger became the Executive Director of the U.S. Department of Defense's (DOD) Cyber Crime Center, which provides electronic forensic services and supports cyber investigative functions at DOD. Before joining DOD, Mr. Reitingger was Deputy Chief of the Computer Crime and Intellectual Property Section at the U.S. Department of Justice. At the Department of Justice, Mr. Reitingger chaired the G8 subgroup on High Tech Crime.

Reitingger has represented government and industry on critical information technology and security initiatives throughout his career, including the Industry Executive Subcommittee of the President's National Security Telecommunications Advisory Committee (NSTAC), where he chaired the Next Generation Networks Task Force. He was the first Chairman of the Software Assurance Forum for Excellence in Code (SAFE-Code), the President of the Information Technology-Information Sharing and Analysis Center (IT-ISAC), and a member of the Executive Committee of the IT Sector Coordinating Council (IT SCC). Mr. Reitingger was a member of the Federal Emergency Management Agency National Advisory Council and the Information Security and Privacy Advisory Board (ISPAB) of the National Institute of Standards and Technology. He was

also a member of the CSIS Commission on Cybersecurity, which developed recommendations for the 44th Presidency.

Reitingger holds a law degree from Yale Law School and a bachelor's degree in electrical engineering and computer science from Vanderbilt University.

"Cybersecurity Collaboration: Partnering Across the Cyber Ecosystem"

Cybersecurity has evolved from an intimate circle of simple web hackers into one of our nations' most important and formidable national security issues. As we increasingly build network capabilities into everything we do, we are also increasing our exposure to adversaries wanting to do significant harm to our national and shared global infrastructure. This means that sharing information and collaboration among nations plays a crucial role in developing effective and coordinated responses to incidences. But as much as we focus in our specific mission spaces, we also recognize that cybersecurity isn't just a government problem; it's also a business concern. Therefore, we need to leverage cyber and information technology expertise across the cybersecurity spectrum, to include industry, academia, other government agencies, as well as national Cyber Emergency Response Teams, in order to create shared situational awareness, and thus a common operational picture. Threats to cybersecurity do not discriminate between borders, and nor should our unified response. It's only through partnership and collaboration that can begin to gain the upper hand in the cybersecurity fight.

TUESDAY | JUNE 15 @ 0900-1000



DAVE AITEL

CTO, Immunity

Dave Aitel is a computer security professional. He joined the NSA as a research scientist at age 18 where he worked for six years before being employed as a consultant at @stake for three years. In 2002 he founded a software security company, Immunity, where he is now the CTO.

"Why Attackers Win"

Incident response happens when your secure development lifecycle fails. At Immunity, my job is to directly attack the overall process of SDLC of large companies in a measurable, concrete way. This talk sheds light on lessons learned, metrics, and growing trends in the attack space.

WEDNESDAY | JUNE 16 @ 0900-1000



DR. UDO HELMBRECHT

Executive Director, ENISA

Dr. Udo Helmbrecht is originally from Castrop-Rauxel, North Rhine-Westphalia, Germany. He has more than 30 years of professional, management experience in the IT sector. His experience has been gained in various sectors of society. This includes e.g. energy industry, insurance company engineering, aviation, defence, and space industry.

Since March 2003, Udo Helmbrecht has served as President of the Federal Office for Information Security (BSI) in Bonn. He has successfully developed the agency's central service provision for information security within the German Federal Government. In addition, he has spearheaded the cooperation between BSI and the IT security industry, as well as raised public awareness of information security issues.

In April 2009, Dr Helmbrecht was appointed Executive Director of ENISA by its Management Board after a presentation for the European Parliament's ITRE committee; a position he assumed on 16th October.

"Securing Europe's Information Society"

The EU policy agenda - Network and information security among top priorities.

Under the umbrella of the Lisbon Strategy, the European Commission Communication "i2010 - A European Information Society for growth and employment"¹, highlighted the importance of network and information security for the creation of a single European information space. The availability, reliability and security of networks and information systems are increasingly central to our economies and society. In his speech the Executive Director of the European Network and Information Security Agency (ENISA) will give an overview of the policy process on European level, new tasks and functions for the ENISA and his vision for the future of NIS in Europe - and beyond!

THURSDAY | JUNE 17 @ 0900-1030



CHRISTOFER HOFF

Director, Cloud & Virtualization Solutions
Cisco Systems

Chris Hoff has over 19 years of experience in high-profile global roles in network and information security architecture, engineering, operations and management with a passion for virtualization and all things Cloud. Hoff is currently Director of Cloud and Virtualization Solutions, Data Center Solutions at Cisco Systems. Prior to Cisco, he was Unisys Corporation's Systems & Technology Division's Chief Security Architect. Additionally, he served as Crossbeam Systems' chief security strategist; was the Chief Information Security Officer for a \$25 billion financial services company; and was founder/Chief Technology Officer of a national security consultancy.

"Cloudifornication - Indiscriminate Information Intercourse Involving Internet Infrastructure"

What was in is now out.

This metaphor holds true not only as an accurate analysis of adoption trends of disruptive technology and innovation in the enterprise, but also parallels the amazing velocity of how our data centers are being re-perimeterized and quite literally turned inside out thanks to cloud computing and virtualization.

One of the really scary things that is happening with the massive convergence of virtualization and cloud computing is its effect on security models and the information they are designed to protect.

Where and how our data is created, processed, accessed, stored, backed up and destroyed in what is sure to become massively overlaid cloud-based services — and by whom and using whose infrastructure — yields significant concerns related to security, privacy, compliance, and survivability.

Further, the "stacked turtle" problem becomes incredibly scary as the notion of nested clouds becomes reality: cloud SaaS providers depending on cloud IaaS providers which rely on cloud network providers. It's a house of, well, turtles.

We will show multiple cascading levels of failure associated with relying on cloud-on-cloud infrastructure and services, including exposing flawed assumptions and untested theories as they relate to security, privacy, and confidentiality in the cloud, with some unique attack vectors.

FRIDAY | JUNE 18 @ 0900-1000



JOHN N. STEWART

VP and Chief Security Officer
Cisco Systems

Mr. Stewart provides leadership and direction to multiple corporate security and government teams throughout Cisco, strategically aligning with business units and the IT organization to generate leading corporate security practices, policies, and processes. His organization focuses on global information security consulting and services, security evaluation, critical infrastructure assurance, eDiscovery, source code security, identification management, as well as special programs that promote Cisco, Internet, national and global security. Additionally, he is responsible for overseeing the security for Cisco.com—the infrastructure supporting Cisco's more than \$35 billion business.

"Who Moved My Cheese? Why The Security Industry Has Been Turned Upside Down"

In a world of no boundaries and digital warfare, electronic attacks upon national IT systems are becoming more frequent, sophisticated and effective. These attacks against the IT infrastructure of governments, defense departments, and the large financial institutions on which we rely are challenging current defense operating systems to their fullest, and may have lasting adverse effects to the nation's economy, security, and overall way of life. Research has found that these attacks have progressed from initial curiosity probes to well-funded and organized operations for political, military, economic and technical espionage and maliciousness. As threats continue to evolve in this multifaceted world, we must develop macro, strategic solutions that can help to protect our interests. Each stolen document has a monetary cost. And at a time when many of us carry valuable information on multiple devices, we must each accept the responsibility of creating the architecture of assurance. As IT security professionals, are we asking the right questions regarding information assurance? Are we providing the right set of solutions to today's challenges and are they enough to protect our IT systems? John N. Stewart questions established practices by asking the hard questions that require real-world answers for today's security challenges.

BOOTH #1 | SOLERA NETWORKS

Solera Networks develops high-speed network forensics solutions for physical and virtual networks. Unmatched in speed and scalability – complete access to network traffic is possible. Solera Networks provides open platform interoperability, extensible storage, and portability. This enables professionals to identify the source of attack, then remediate and fortify against further risk. www.soleranetworks.com

BOOTH #2 | NEUSTAR

NeuStar, Inc. (NYSE: NSR) solves complex communications challenges and provides innovative solutions and directory services that enable trusted communication across networks, applications, and enterprises around the world. For more information about Neustar, as well as our UltraDNS and Webmetrics services, visit www.neustar.biz, www.ultradns.biz and www.webmetrics.com.

BOOTH #3 | BT

Working together

BT is one of the world's leading providers of communications solutions and services operating in 170 countries. BT's "Business Continuity, Security and Governance" practice is a centrally managed, global practice, working to help corporate and government customers around the world to manage and maintain secure and resilient networked IT infrastructures. www.globalservices.bt.com

BOOTH #4 | TELEFONICA

Telefonica is one of the largest telecommunications companies in the world in terms of

market capitalization. Its activities are centered mainly on the fixed and mobile telephony businesses with broadband as the key tool for the development of both. The company has a significant presence in 25 countries and a customer base that amounts to 265 million accesses around the world. For more information please visit: www.us.telefonica.com.

BOOTH #5 | MANDIANT

MANDIANT is an information security company that provides proactive and responsive consulting services, education and incident response software to Fortune 500 companies, financial institutions, government agencies, domestic and foreign police departments and several of the U.S.'s leading law firms. For more information visit www.mandiant.com.

BOOTH #6 | US-CERT

US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry and international partners. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public. www.us-cert.gov

US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry and international partners. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public. www.us-cert.gov

BOOTH #7 | NETWITNESS

NETWITNESS

NetWitness® Corporation is the world leader in real-time network forensics and automated threat intelligence solutions, helping government and commercial organizations detect,

prioritize and remediate complex IT risks. NetWitness solutions concurrently solve a wide variety of information security problems including: advanced persistent threat management; sensitive data discovery and advanced data leakage detection; malware activity discovery; insider threat management; policy and controls verification and e-discovery. www.netwitness.com

BOOTH #8 | HBGARY

DETECT. DIAGNOSE. RESPOND.

HBGary, Inc is the leading provider of solutions to detect, diagnose and respond to advance malware threats in a thorough and

forensically sound manner. We provide the active intelligence that is critical to understanding the intent of the threat, the traits associated with the malware and information that will help make your existing investment in your security infrastructure more valuable. www.hbgary.com

BOOTH #9 | MICROSOFT**Microsoft®**

Founded in 1975, Microsoft is the worldwide leader in software, services and solutions that help people and businesses realize their full potential. www.microsoft.com

BOOTH #10 | SECUNIA

Secunia
Stay Secure

Secunia is the leading Vulnerability Intelligence company with a strong community commitment.

Secunia provides:

- * Accurate and reliable Vulnerability Intelligence
- * Most accurate Vulnerability Scanning technology
- * WSUS integration for automated patching
- * A very active security community
- * Most active Vulnerability Research house
- * Free Vulnerability Scanning for private users

Visit: www.secunia.com

BOOTH #11 | ICS-CERT

The ICS-CERT responds to and analyzes cyber threats and control systems incidents, conducts vulnerability and malware analysis, and provides onsite support for forensic investigations and analysis. The ICS-CERT shares and coordinates vulnerability information and threat analysis through actionable

information products and alerts. Website available at www.us-cert.gov/control_systems

BOOTH #12 | CISCO SYSTEMS

Cisco is the worldwide leader in networking for the Internet. Its hardware, software, and service offerings are used to create Internet solutions that allow individuals, companies, and countries

to increase productivity, improve customer satisfaction and strengthen competitive advantage. Our vision is to change the way people work, live, play and learn. www.cisco.com

BOOTH #13 | DAMBALLA

Damballa helps enterprise organizations take back command and control of their networks from botnets, advanced persistent threats (APTs) and other advanced targeted attacks. Our concentrated focus on malicious remote control delivers fast, accurate detection, powerful mitigation, and detailed forensics to understand what happened and how to prevent future attacks. Visit www.damballa.com

VENDOR SHOWCASE EXTRAS!

Adobe Systems Incorporated offers business, creative, and mobile software solutions that revolutionize how the world engages with ideas and information. With a reputation for excellence and a portfolio of many of the most respected and recognizable software brands, Adobe is one of the world's largest and most diversified software companies. www.adobe.com

Adobe will be raffling off a copy of their popular CS5 software suite to one lucky attendee!

MEMBERSHIP TABLES**SPECIAL BAR SETUP WITH**

Provided by

DIAGEO



ABOUT FIRST

The Forum of Incident Response and Security Teams (FIRST) is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactively as well as proactively.

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

Apart from the trust network that FIRST forms in the global incident response community, FIRST also provides value added services. Some of these are:

- Access to up-to-date best practice documents
- Technical colloquia for security experts
- Hands-on classes
- Annual incident response conference
- Publications and webservicees
- Special interest groups
- Corporate Executive Programme (CEP)

Currently FIRST has over 214 members, spread over Africa, the Americas, Asia, Europe and Oceania.

MISSION STATEMENT

FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs.

BECOME A TRUSTED CONNECTION

Computer security incidents do not respect geographical or administrative boundaries in the global Internet. FIRST is designed to facilitate global communication between incident response and security teams to assist in promoting prompt and effective resolution to computer security incidents.

Please leave your business card or email address and phone number at the FIRST Membership Table or Registration Desk and a Steering Committee member will contact you and guide you through the process. You may also contact the FIRST Secretariat at first-sec@first.org.

2010 PROGRAM CHAIR

ANDREW CUSHMAN.....MICROSOFT, US

2010 PROGRAM COMMITTEE

SHIN ADACHI.....NTT-CERT, US

JEFF BOERIO.....INTEL US

JEFFREY CARPENTER.....CERT/CC, US

RALF DÖRRIE.....DEUTSCHE TELEKOM, DE

LIONEL FERETTE.....BELNET, BE

ROBERT FLOODEEN.....CERT/CC, US

MIRASLAW MAJ.....CERT POLSKA/NASK, PL

MATTHEW MCGLASHAN.....AUSCERT, AU

JOSE NAZARIO.....ARBOR NETWORKS, US

JACOMO PICCOLINI.....RNP/ESR BRAZIL, BR

GAVIN REID.....CISCO SYSTEMS, US

UDO SCHWEIGERT.....SIEMENS, DE

MARCO THORBRUEGGE.....ENISA

YONGLIN ZHOU.....CNCERT, CN

FIRST SECRETARIAT SERVICES

NEUSTAR SECRETARIAT SERVICES

NORA DUHIG
MICHAEL LEE
VID LUTHER

FIRST CONFERENCE COORDINATORS

CONFERENCE & PUBLICATION SERVICES, LLC

PHOEBE J. BOELTER
KRISTEN JACOBUCCI
TRACI WEI



Improving Security Together

12 - 17 June 2011

23rd  Vienna

Annual **FIRST** Conference

Do yesterday's IT security governance models still apply, or will they lead to catastrophe? Can new analysis theories transform the world?

Join us in Vienna, Austria for the 23rd Annual FIRST Conference to reflect on the state of network security and address modern challenges facing incident response while enjoying the rich history and cultural heritage of the Imperial City.

SECURITY LESSONS: WHAT CAN HISTORY TEACH US?



2010 SPONSORSHIP TEAM

DIAMOND



Working together

GOLD



CHOICE PRIMARY SPONSORS



SUPPORTING SPONSORS



EXHIBITORS

