FIRST

Improving Security Together

Hilton Vienna | Austria | 12 - 17 June 2011

23rd Vienna

Annual **FIRST** Conference

SECURITY LESSONS

what can history teach us?

Conference Program

Willkommen in Wien!

Welcome to the 23rd Annual FIRST conference here in the great city of Vienna, Austria.

I am thrilled to welcome you to another great week of exciting and informative talks on key security topics. The rich history of Vienna will lend itself well in complimenting the rich history that the Forum of Incident Response and Security Teams (FIRST) organization possesses in the Incident Handling ecosystem. I encourage you to take advantage of this opportunity to immerse yourself in the culture and knowledge that surrounds us.

As I move to the end of my 2nd and final term as chair, I am still in awe of the amazing and truly impactful things the members of this organization continue to accomplish within the security landscape. It makes me extremely proud that FIRST is as relevant today as it was when the organization was created decades ago.

Though technologies are rapidly changing and this change continues to stretch security professionals, FIRST remains poised on the frontline to aid Incident Handlers and Security Teams with valuable lessons learned and trusted connections to aid them in their time of need. This capacity to help has been recognized by important organizations such as the International Telecommunication Union (ITU), as a valuable contribution to the global consumer digital community.

This week I want to ask each attendee to "push the envelope" in their thought process. Use this week to absorb as much information as possible while building those important connections with your fellow colleagues. Use it to create the early framework for creative security strategies to help your organizations. Think of new innovative ways to share speedy, relevant, and actionable security incident information. Who knows, maybe the stories you share will be the important key solution to another's security problem. The history sharing that takes place at FIRST conferences is what makes events like this continue to play a key part in any long lasting global security initiative.

In closing I want to thank Gavin Reid (2011 Program Chair) and his program committee, Kurt Sauer (Conference Liaison), CAPS LLC (Phoebe Boelter, Kristen Jacobucci and Traci Wei), and the countless other volunteers that help to make this conference a memorable occasion.

Thank you for attending and I look forward to sharing stories with you over a mug of Vienna's amazing hot chocolate ☺.

Stephen Adegbite

Stephen Adegbite
Chairman, FIRST.Org
Adobe Systems, US

2010-2011 Steering Committee

Kenneth van Wyk
Vice Chairman
KRvW Associates LLC, US

Peter Allor
CFO
IBM, US

Kurt Sauer
Conference Liaison
PayPal, JP

Thomas Mullen
CEP Liaison
BT, UK

Jordi Vila Aguilà
la Caixa, ES

Chris Gibson
Citi, UK

Yurie Ito
ICANN, US
JPCERT/CC, JP

Reneaué Railton
Cisco Systems, US

Robert Schischka
CERT.at, AT

12 - 17 June 2011
23rd Vienna
Annual **FIRST** Conference

Table of Contents

FIRST Secretariat

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

first-sec@first.org

Conference Office

FIRST.Org, Inc.
Conference Coordination Office
c/o CAPS, LLC
219 W. Chicago, Suite 300
Chicago, Illinois 60654
United States of America

first-2011@first.org
+1 312 646 1013

Venue Information

Hilton Vienna Hotel
Am Stadtpark 1
1030 Vienna
Austria

+43 (0) 1 717000

FIRST Websites

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

Lost & Found

Registration Desk

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

@firstdotorg
#FIRST2011

http://www.facebook.com/firstcon

General Reminders

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-refund able) from the conference.

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

Use of 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.Org.

Internet Access

Conference Meeting Rooms

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

For access, please use the following:

SSID:	**FIRST2011**
WPA & WPA2:	**FIRST23Vienna**

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-2011-vienna@cisco.com.

At-a-Glance & Extras

Registration Hours

Park Congress Prefunction Area

Sunday	1400-1800
Monday-Wednesday	0800-1600
Thursday, Friday	0800-1530

Breakfast Hours

Strauss/Brahms/Mahler/Bruckner
Complex & Klimt Ballroom 2

Monday-Friday	0800-0915

Lunch Hours

Strauss/Brahms/Mahler/Bruckner
Complex & Klimt Ballroom 2+3

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

Geek Lounge

Kafka, Mezzanine 1

Sunday	1830-2100
Monday-Friday	1200-1700

About the Wednesday Banquet

Cocktail Reception in Hilton 1800-1930
Buses Leave at 1930
Dinner Starts at Rathaus 2000-2400

This year's annual conference banquet dinner will be held at the beautiful Vienna Rathaus (City Hall). Transportation will be provided to conference attendees to and from the Rathaus. **All buses will leave at 19:30, please be prompt.**

Buses to Rathaus:	1930
Buses to Hilton:	2300, 2315, 2330, 2345

Suggested Attire
Men: collared shirt, suit, blazer, trousers (no jeans)
Women: blouse, skirt, trousers (no jeans), cocktail/summer dress

If you have any questions about the banquet prior to Wednesday, please feel free to stop by the registration desk.

We look forward to another memorable evening!

Top: Steve Adegbite, Chair of FIRST.Org networking with attendees 2010; Bottom: 2010 attendees with exhibitor.

Network & Win Raffle - *Due Friday*

If you would like to participate in the "Network & Win" raffle, please pick up a raffle card at the Registration Desk.

The goal of this networking exercise is to visit all of our conference exhibitors this week starting with the Vendor Showcase on Tuesday evening open exhibit hours through to Friday morning. Each exhibitor will have a unique stamp for your card—some exhibitors may have an interesting task or survey for you to complete before receiving your stamp!

Completed cards are due to the Registration Desk no later than 12:00 on Friday in order to be counted in the raffle. The raffle will take place during the Closing Remarks. FIRST will raffle four prizes. One lucky winner will receive a Fellowship Sponsorship to attend the 24th Annual FIRST Conference, 17-22 June 2011 in Malta. The Fellowship Sponsorship includes one complimentary conference registration and a travel stipend.

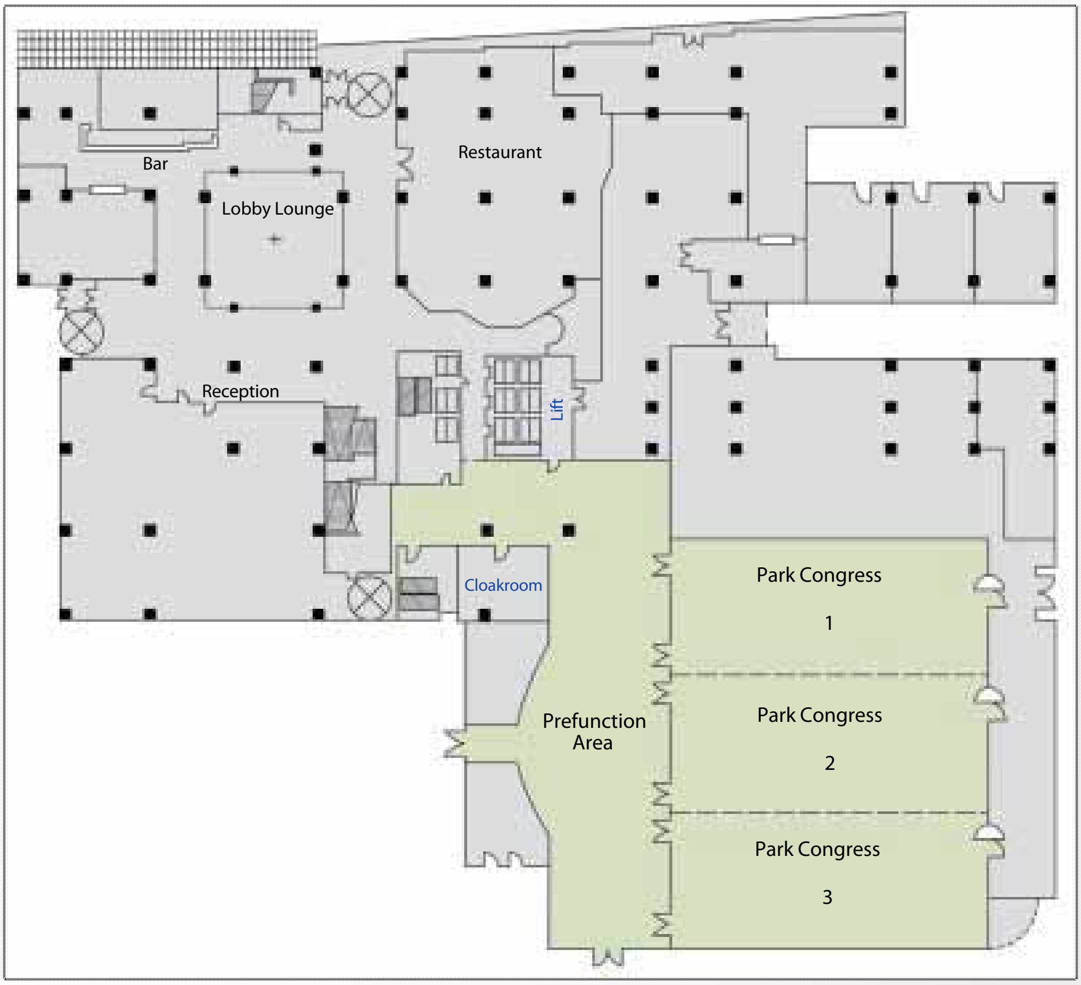
Fellowship Sponsors 2011-2012:

NORTHWESTERN UNIVERSITY

PCH Packet Clearing House

Floor Plans

Ground Floor



Park Congress Prefunction Area

Registration	Sunday-Friday
Coffee Breaks	Monday-Friday
Exhibits	Tuesday-Friday
Vendor Showcase	Tuesday 1800-2000

Park Congress Ballrooms 2+3

ROCK TRACK	Monday-Friday
Special Japan Panel	Tuesday
Lightning Talks	Wednesday
Member AGM	Thursday

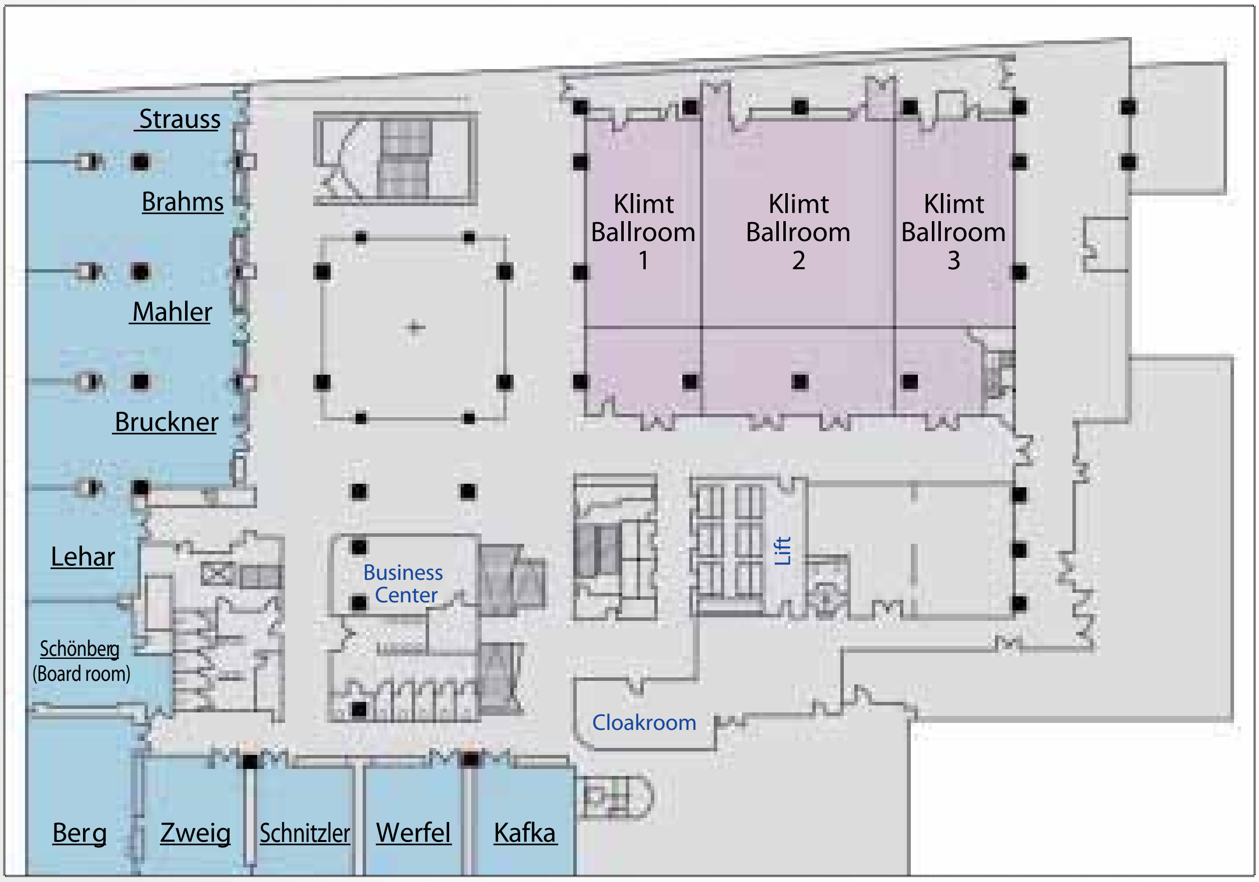
Park Congress Ballrooms 1+2+3

Opening Remarks	Monday-Friday
Keynotes	Monday-Friday
General Sessions	Monday-Friday

Park Congress Ballrooms 1

PAPER TRACK	Monday-Friday

Mezzanine 1



Mezzanine Foyer

Newbie Reception	Sunday, 1830-1900
Ice Breaker	Sunday, 1900-2100

Klimt Ballroom 1

SCISSORS TRACK	Monday-Friday

Klimt Ballroom 2+3
Strauss/Brahms/Mahler/Bruckner Complex

Breakfast	Monday-Friday
Lunch	Monday-Friday

Kafka

Geek Lounge	Sunday, 1830-2100 Mon-Fri, 1200-1700

Program

Saturday, 11th June

1100-1700	**FIRST Education & Training Committee Meeting //** Bruckner, Mezzanine 1 Closed meeting.

Sunday, 12th June

0900-1700	**FIRST Education & Training Committee Meeting //** Bruckner, Mezzanine 1 Closed meeting.
1400-1800	**Registration** // Park Congress Prefunction, Ground Floor
1500-1600	**Session Chairs Meeting** // Berg, Mezzanine 1
1830-1900	**Newbie Reception with FIRST Steering Committee** // Foyer, Mezzanine 1 FIRST Newbies (non-members) & 1st Time Attendees (members and non-members) are cordially invited to mix and mingle with each other and the FIRST Steering Committee. Beverages and appetizers will be served.
1900-2100	**Ice Breaker Reception** // Foyer, Mezzanine 1 All attendees are encouraged to attend this kick-off event. Come and mingle with your colleagues, new and old, over drinks, appetizers and great conversation.

Rock, Paper, Scissors... what's what?

Rock: presentations by law enforcement, talks on trends, and industry exercises.

Paper: presentations covering industry case studies, best practices, and forensics.

Scissors: presentations spanning advanced persisten theats (APT), CSIRTs, small form factor, and policy.

Lightning Talks...what are they and how can I participate?

Want to present next year and get a feel for the FIRST crowd? Have something to share with your peers? Want to let your colleagues know what your organization is working on? Then get up on stage and be heard! Sign-up to present a 5-minute presentation on Wednesday. Slides are not necessary, but encouraged if you have the time!

NO SALES PRESENTATIONS!

Sign-up is located at the registration desk.
First-come, first-served basis.

Monday, 13th June

0800-0900	**Welcome to FIRST Roundtable Breakfast** // Klimt 3, Mezzanine 1 Invitation-only, informational breakfast for first-time, non-members.		
0800-0915	**Breakfast** // Strauss/Brahms/Mahler/Bruckner Complex & Klimt 2, Mezzanine 1		
0800-1600	**Registration //** Park Congress Prefunction, Ground Floor		
0930-0945	**Conference Opening & Welcome //** Park Congress 1+2+3, Ground Floor **Steve Adegbite** Chair, FIRST.Org & Senior Security Strategist/Senior Security Product Manager, Adobe Systems, US		
0945-1045	***CERTS, cops, and criminals*** // Park Congress 1+2+3, Ground Floor **Peter Zinn** Sr. High Tech Crime Advisor, KLPD (National Crime Squad), NL		
1045-1100	**Coffee & Networking Break //** Park Congress Prefunction, Ground Floor		
1100-1200	***Digital Dependence: Cybersecurity in the 21st Century*** // Park Congress 1+2+3, Ground Floor **Melissa Hathaway** President, Hathaway Global Strategies, US Senior Advisor, Harvard Kennedy School's Belfer Center, US		
1200-1330	**Lunch Break //** Strauss/Brahms/Mahler/Bruckner Complex & Klimt 2+3, Mezzanine 1		
BREAKOUTS			
	Rock // Park Congress 2+3	**Paper** // Park Congress 1	**Scissors** // Klimt 1
1330-1430	***Working effectively against criminals and criminal activities through boundaries and minds.*** **Ireneusz Parafjanczuk** Team Cymru, US / PL **Mikhail Ganev** RU-CERT, RU	***Remediating Compromised Environments: Case Studies from Large and Small Enterprises*** **Wendi Rafferty** Mandiant, US	***Five Years of Persistent Targeted Attacks*** **Maarten Van Horenbeeck** Microsoft Corporation, US
1430-1530	***Security Challenges for Future Systems*** **Steve Purser** ENISA	***A Wrench in the Cogwheels of P2P Botnets*** **Tillmann Werner** Kaspersky Lab, DE	***Intrusion Suppression— A Different Approach to Threat Management and Mitigation*** **Christopher Day** Terremark, US
1530-1600	**Coffee & Networking Break //** Park Congress Prefunction, Ground Floor		
1600-1700	***Looking into Malicious Insiders*** **Koichiro Komiyama** JPCERT/CC, JP	***Targeted and Opportunistic Botnet Building*** **Günter Ollmann** Damballa, US	***Data Exfiltration— Not just for Hollywood*** **Iftach 'Ian' Amit** Security Art, IL
1930-2130	**FIRST Financials & Budgeting - 2010 to Current** // Park Congress 1, Ground Floor FIRST members are welcome to discuss organizational financials and budgeting. This is a meeting and not a program session.		

Program

Tuesday, 14th June

0800-0915	**Breakfast** // Strauss/Brahms/Mahler/Bruckner Complex & Klimt 2		
0800-1600	**Registration** // Park Congress Prefunction, Ground Floor		
0930-0945	**Conference Opening & Welcome** // Park Congress 1+2+3, Ground Floor **Steve Adegbite** Chair, FIRST.Org & Senior Security Strategist/Senior Security Product Manager, Adobe Systems, US		
0945-1045	***Funny Pharma: Inside the Web's Leading Rogue Pharmacies*** // Park Congress 1+2+3, Ground Floor **Brian Krebs** Reporter, Tech Policy & Security, Krebs on Security LLC, US		
1045-1100	**Coffee & Networking Break** // Park Congress Prefunction, Ground Floor		
1100-1200	***Lessons from Our Past Fuel the Success of Our Future*** // Park Congress 1+2+3, Ground Floor **John Stewart** Vice President and Chief Security Officer, Cisco Systems, US		
1200-1330	**Lunch Break** // Strauss/Brahms/Mahler/Bruckner Complex & Klimt 2+3		
	BREAKOUTS		
	Rock // Park Congress 2+3	**Paper** // Park Congress 1	**Scissors** // Klimt 1
1330-1430	***Operation Carder Kaos*** **Richard LaTulip** United States Secret Service	***Collection, analysis and response stages which consist of 6 core modules*** **Jae Ho Ahn** **Jin Myeong Chung** ECSC (KERIS), KR	***Data Security Challenges in the all too Public and not so Private Sectors*** **Patrick Gray** Cisco Systems, US
1430-1530	***Securing the podium with incident response during an Olympics (Vancouver 2010 Olympic Lesson's Learned)*** **Robert Pitcher** Canadian Cyber Incident Response Centre, CA	***SCADA Vulnerability Disclosure*** **Kevin Hemsley** ICS-CERT, US	***The Implementation and Management of a CSIRT Team in the African Arena*** **Rudolph Pretorius** First National Bank, ZA
1530-1600	**Coffee & Networking Break** // Park Congress Prefunction, Ground Floor		
1600-1700	***Regulation of Cybercrime in LAC—A Status of the Region*** **Erick Iriarte** LACTLD, PE	***Don't Lose Sight of the Extended Enterprise*** **Rod Rasmussen** Internet Identity (IID), US	***Cyber Clean Center Project—A five year retrospective*** **You Nakatsuru** JPCERT/CC, JP
1700-1800	**SPECIAL PANEL: *The day disaster struck the northeastern part of Japan //*** Park Congress 2+3 **Moderator: Takayuki Uchiyama**, JPCERT/CC **Panelists: Teruo Fujikawa**, NCSIRT, **Yusuke Gunji**, Rakuten-CERT, **Itaru Kamiya**, NTT-CERT, **Yoshinobu Matsuzaki**, IIJ-SECT		
1800-2000	**Vendor Showcase** // Park Congress Prefunction, Ground Floor		

Wednesday, 15th June

0800-0915	**Breakfast** // Strauss/Brahms/Mahler/Bruckner Complex & Klimt 2, Mezzanine 1		
0800-1600	**Registration //** Park Congress Prefunction, Ground Floor		
0930-0945	**Opening Remarks** // Park Congress 1+2+3, Ground Floor **Steve Adegbite** Chair, FIRST.Org Senior Security Strategist/Senior Security Product Manager, Adobe Systems, US		
0945-1045	***The Future is YOU!*** // Park Congress 1+2+3, Ground Floor **Rob Thomas** CEO and Founder, Team Cymru, US		
1045-1100	**Coffee & Networking Break //** Park Congress Prefunction, Ground Floor		
1100-1200	***Are we really learning from History? An investigator's perspective.*** // Park Congress 1+2+3, Ground Floor **Rajeev Kumar** Additional Commissioner of Police, Kolkata, Department of Home, Government of West Bengal, India		
1200-1330	**Lunch Break** // Strauss/Brahms/Mahler/Bruckner Complex & Klimt 2+3, Mezzanine 1		
	BREAKOUTS		
	Rock // Park Congress 2+3	**Paper** // Park Congress 1	**Scissors** // Klimt 1
1330-1430	***Cloud Security vs. Cybercrime Economy: The Kaspersky Vision*** **Eugene Kaspersky** Kaspersky Lab, RU	***Lessons Learned from a Bredolab Takedown*** **Dave Woutersen** GOVCERT.NL	***Developing and testing secure iPhone apps*** **Kenneth van Wyk** KRvW Associates, LLC, US
1430-1530	***Botnets, Collective Defense and Project MARS*** **Jeff Williams** Microsoft Corporation, US	***Listening to the Network: Leveraging Network Flow Telemetry for Security Applications*** **Darren Anstee** Arbor Networks, US	***Good intentions, bad policies. Repaving the road to IT Security Nirvana*** **Scott McIntyre** Telstra Corporation, AU
1530-1600	**Coffee & Networking Break** // Park Congress Prefunction, Ground Floor		
1600-1700	***Operational Security in EGI*** **Tobias Dussa** KIT-CERT, DE **Sven Gabriel** NIKHEF / EGI-CERT, NL **Leif Nixon** European Grid Infrastructure, SE	***The Underground Economy and Ecosystem of SMS-based Cybercrime*** **Denis Maslennikov** Kaspersky Lab, RU	***Dissecting the Trojan-Patcher Gang*** **Peter Kruse** CSIS Security Group A/S, DK
1700-1800	**Lightning Talks** // Park Congress 2+3		
1700-1800	**Open Exhibit Hour //** Park Congress Prefunction, Ground Floor		
1800-1930	**Banquet Cocktail Reception in Hilton** // Park Congress Prefunction, Ground Floor		
2000-2400	**Conference Banquet at the Vienna Rathaus** // Please see page 5 for transportation details.		

Program

Thursday, 16th June

0800-0915	**Breakfast** // Strauss/Brahms/Mahler/Bruckner Complex & Klimt 2, Mezzanine 1		
0800-1600	**Registration** // Park Congress Prefunction, Ground Floor		
0930-0945	**Opening Remarks** // Park Congress 1+2+3, Ground Floor **Steve Adegbite** Chair, FIRST.Org & Senior Security Strategist/Senior Security Product Manager, Adobe Systems, US		
0945-1045	***IT Security in the European Digital Agenda*** // Park Congress 1+2+3, Ground Floor **Marc Feidt** Head of Unit, Corporate Infrastructure Service, DIGIT, European Commission (EU)		
1045-1100	**Coffee & Networking Break** // Park Congress Prefunction, Ground Floor		
1100-1200	***Online exploitation of children—What's it got to do with me?*** // Park Congress 1+2+3, Ground Floor **Michael Moran** Coordinator, Crimes Against Children, Serious Crimes Directorate, INTERPOL		
1200-1300	**Lunch Break** // Strauss/Brahms/Mahler/Bruckner Complex & Klimt 2+3, Mezzanine 1		
BREAKOUTS			
	Rock // Park Congress 2+3	**Paper** // Park Congress 1	**Scissors** // Klimt 1
1300-1400	***The Stuxnet Incident*** **Heiko Patzlaff** Siemens, DE	***Data Mining the eCriminals: Interesting things lurking in APWG statistics*** **Patrick Cain** AWPG, US	***Blitzableiter—Countering Flash Exploits*** **Joern Bratzke** **Robert Tezli** Recurity Labs, DE
1400-1500	***Worldwide Security and Resiliancy of Cyber Infrastructures: The Role of the Domain Name System*** **Igor Nai Fovino** Global Cyber Security Center, IT	***Understanding and Mitigating Internet Routing Threats*** **John Kristoff** Team Cymru, US **Danny McPherson** VeriSign, US	***A Pragmatic Approach to Cloud Security Modeling*** **Richard Puckett** General Electric, US
1500-1600	**Open Exhibit Hour & Coffee Break for Non-Members** // Park Congress Prefunction, Ground Floor		
1530-1730	**Annual General Meeting (AGM)** // Park Congress 2+3, Ground Floor Members Only & Approved Guests only. Must have a valid government issued photo ID for entry. No exceptions will be made. Please be prompt, once doors close and the meeting begins you will not be permitted in or out.		

Program

Friday, 17th June

0800-0915	**Breakfast** // Strauss/Brahms/Mahler/Bruckner Complex & Klimt 2, Mezzanine 1		
0830-1200	**Registration** // Park Congress Prefunction, Ground Floor		
0930-0945	**Opening Remarks** // Park Congress 1+2+3, Ground Floor **Steve Adegbite** Chair, FIRST.Org Senior Security Strategist/Senior Security Product Manager, Adobe Systems, US		
0945-1045	***State Of The Net*** // Park Congress 1+2+3, Ground Floor **Mikko Hypponen** Chief Research Officer, F-Secure, FI		
1045-1100	**Coffee & Networking Break** // Park Congress Prefunction, Ground Floor		
1100-1200	***Cybercrime in the Kenyan Context*** // Park Congress 1+2+3, Ground Floor **Mwende Njiraini** Associate and Internet Governance Tutor, DiploFoundation, KE		
1200-1330	**Lunch Break** // Strauss/Brahms/Mahler/Bruckner Complex & Klimt 2+3, Mezzanine 1		
	BREAKOUTS		
	Rock // Park Congress 2+3	**Paper** // Park Congress 1	**Scissors** // Klimt 1
1330-1430	***The road to hell is paved with best practices...*** **Frank Breedijk** **Ian Southam** Schuberg Philis, NL	***Lessons Learned from Security Incidents?*** **Mikko Karikytö** **Anu Puhakainen** Ericsson, FI	***CANCELLED SESSION***
1430-1530	***The Dynamics and Threats of End-Point Software Portfolios*** **Stefan Frei** Secunia, DK	***Learning from the Past: Tools and Techniques for Timeline Analysis*** **Andreas Schuster** Deutsche Telekom AG, DE	***Benefits of an Exploit Disclosure Process*** **Tom Cross** IBM ISS, US **Holly Stewart** Microsoft Corporation, US
1530-1600	**Closing Remarks & Raffle Drawings** Park Congress 2+3, Ground Floor **Chairman** **FIRST.Org, Inc.**		

See you in Malta!
17-22 June 2012

Keynotes

Peter Zinn—Monday @ 09:45-10:45

Sr. High Tech Crime Advisor, KLPD (National Crime Squad), NL

Peter Zinn is Senior Cybercrime Advisor for the Dutch National High Tech Crime Unit (NHTCU). Acting as the liaison between law enforcement and the private sector, he strongly believes in transparency and the sharing of information. He authored two books on the current state of trends in cybercrime. He developed strategy and tactical program for the NHTCU, thus translating his expertise into a high tech crime policy for the Dutch police.

Peter leads the Botnet Working Group of the Interpol European Working Party on IT Crime, aiming to optimise the efforts of different countries in this area. He is a member of several public-private information sharing centres concerning national and European vital infrastructures, including the financial sector.

An award winning speaker, Peter presented at various congresses like Interpol, Europol, FBI, DCC, PCI/SSC and SOCA.

CERTS, cops, and criminals

Attend the presentation and find out!

Melissa Hathaway—Monday @ 11:00-12:00

President, Hathaway Global Strategies, US
Senior Advisor, Harvard Kennedy School's Belfer Center, US

Melissa Hathaway is President of Hathaway Global Strategies, LLC and A Senior Advisor at Harvard Kennedy School's Belfer Center. Having served in two Presidential administrations, Hathaway brings a multi-disciplinary and multi-institutional perspective to strategic consulting and strategy formulation for public and private sector clients. She served in the Obama Administration as Action Senior Director for Cyberspace in the National Security Council and led the Cyberspace Policy Review. During the last two years of the administration of George W. Bush, Hathaway served as Cyber Coordination Executive and Director of the Joint Interagency Cyber Task force in the Office of the Director of National Intelligence where she led the development of the Comprehensive National Cybersecurity Initiative (CNCI). At the conclusion of her government service she received the National Intelligence Reform Medal in recognition of her achievements.

Digital Dependence: Cybersecurity in the 21st Centuary

The Internet has co-mingled and connected every nation and nearly all essential services, and has blurred the lines of sovereign assets and commercial space. This digital entanglement of private and public infrastructure has occurred over time --since the dawn of the Internet. This presentation will describe the history of technology innovation around the Internet, describe the early adopters, and illustrate the economic benefits and security challenges.

Brian Krebs—Tuesday @ 09:45-10:45

Reporter, Tech Policy & Security, Krebs on Security LLC, US

Brian Krebs worked as a reporter for The Washington Post from 1995 to 2009, authoring more than 1,300 blog posts for the Security Fix blog, as well as hundreds of stories for washingtonpost.com and The Washington Post newspaper, including eight front-page stories in the dead-tree edition and a Post Magazine cover piece on botnet operators.

But you didn't really want to read my résumé, did you? What most people want to know is how I got into computer security, and whether I have a technical background in the field.

The short answer is "by accident," and "no," respectively. I earned a Bachelor of Arts in International Studies from George Mason University in 1994, and at the time I wasn't much interested in computers, although I had programmed a bit on an

Apple II and spent quite a bit of time visiting online bulletin boards as a kid.

It wasn't until 2001 — when my entire home network was overrun by a Chinese hacking group — that I became intensely interested in computer security. I had been monkeying with a default installation of Red Hat Linux (6.2) on an old Hewlett-Packard system, because for some reason I had it in my head that it would be fun to teach myself how to turn the spare computer into an oversized firewall [ah, the irony]. That is, until the Lion Worm came around and locked me out of my system. Twice.

After that incident, I decided to learn as much as I could about computer and Internet security, and read most everything on the subject that I could get my hands on at the time. It's an obsession that hasn't let up.

Much of my knowledge about computers and Internet security comes from having cultivated regular and direct access to some of the smartest and most clueful geeks on the planet. The rest I think probably comes from a willingness to take risks, make
mistakes, and learn from them.

I am 38 years old, and live with my wife Jennifer in Northern Virginia. When I'm not at the computer, I most often spend my free time reading, writing, cooking, studying Russian and playing guitar. I also enjoy corresponding with readers, so shoot me a note and tell me what you think of the blog (**http://krebsonsecurity.com**).

Funny Pharma: Inside the Web's Leading Rogue Pharmacies

Last year, insiders stole the confidential customer and affiliate databases from two of the largest rogue Internet pharmacy programs -- generic pill mills advertised via spam botnets and black hat search engine trickery. Through routes both comical and creepy, the two databases wound up in Krebs's hands. He has been mining the data ever since for nuggets of insight into the structure and day-to-day operations of these online apothecaries, and has interviewed dozens of buyers to find out what motivated them to purchase and ingest pills ordered through spam. In his keynote, Krebs will explain how this misunderstood marketplace is evolving well beyond little blue pills, and how the growing demand for knockoff prescription drugs is driving much of the cybercrime economy today.

John Stewart—Tuesday @ 11:00-12:00

Vice President and Chief Security Officer, Cisco Systems, Inc., US

Throughout his career spanning more than two decades, John Stewart has led or participated in security efforts ranging from elementary school IT design to national security programs. A heavily sought public and closed-door speaker, blogger to blogs.cisco.com/security, and 2010 Federal 100 Award recipient, Stewarts' drive is simple: results.

As Vice President and Chief Security Officer for Cisco, Stewart leads the security operations, product security, and government security functions. His team focuses on global information security consulting and services, security evaluation, critical infrastructure assurance, source code security, identification management, and special programs that promote Cisco, Internet, national, and global security. He is also responsible for overseeing security for Cisco.com, the infrastructure supporting Cisco's $40+ billion business, WebEX, the collaboration service providing 73 million online meetings per year, among other Cisco functions.

Stewart is an active member in the broad security industry. Currently, he sits on technical advisory boards for Core Security Technologies, Panorama Capital, and RedSeal Networks; is on the board of directors for KoolSpan, Fixmo, and the National Cyber-Forensics Training Alliance (NCFTA); is a member of the Cyber Security Think Tank at University of Maryland University College (UMUC); and is a standing member of the CSIS Commission on Cyber Security. In the past, he served on advisory boards for successful companies such as Akonix, Cloudshield, Finjan, Ingrian Networks, Riverhead, and TripWire.

Stewart holds a Master of Science degree in computer and information science with honors from Syracuse University, Syracuse, New York.

Lessons from Our Past Fuel the Success of Our Future

Since well before the Internet's inception, security professionals have been fighting the good fight to protect information technology systems and infrastructure from those who would try to disrupt business, steal information, or do us harm. Today, we continue to grapple with new and varied electronic security threats: from nation-state attacks to the wikileaks exposure and SCADA vulnerabilities; from ID theft to phishing to unseen bots controlling our systems; from cyber-bullying to… the list goes on and on. What effect do these threats have on our confidence and assurance in information security?

Keynotes

While security professionals have come a long way in developing and delivering on the technologies, processes, and behavioral changes that improve information security, there is still certainly far to go. We must learn from our past to ensure that we don't reenact the mistakes of yesterday, and are able to move the security needle forward effectively and with confidence. As computer scientist Alan Kay says, "the best way to predict the future is to invent it." It's time to invent a better future. Join Cisco Vice President and Chief Security Officer, John N. Stewart, as he shares his perspective on some of our past successes, discusses today's security challenges, and proposes new models and approaches to close the cybersecurity gap and improve our future security posture.

Rob Thomas—Wednesday @ 09:45-10:45

CEO and Founder, Team Cymru, US

Rob Thomas is CEO and founder of Team Cymru. Rob has worked as a network engineer, Unix kernel developer, systems administrator, and security architect at companies as diverse as Motorola, Sun, Cisco, and Ameritech. Rob has a passion for all things technical, and it shows in his dynamic writings and presentation style.

The future is YOU!

Over a decade ago, when I founded Team Cymru with 3 friends, the Internet, and indeed the World, was a very different place. I've worked with FIRST members around the world as we've seen things evolve, sometimes for the better, often, despite our best efforts, to the detriment of people, businesses and our hopes for the future.

One thing that has remained constant is YOU. This presentation will touch on what I've discovered about our community and how that translates into lessons for the next generation of Security professionals. Hopefully it'll be a fun and entertaining trip for us all!

Rajeev Kumar—Wednesday @ 11:00-12:00

Additional Commissioner of Police, Kolkata
Government of West Bengal, India

Rajeev Kumar is heading the counter terrorism unit of Kolkata Metropolitan Police for last three years. He has an been actively associated with the field of counter terrorism for more than a decade. He holds a degree in B.Tech (Computer Science & Technology) from University of Roorkee. In the year 1990, he joined prestigious Indian Police Service.

He stays in Kolkata with his wife and 14 year old son.

Are we really learning from History? An investigator's perspective.

During this presentation, through Indian case study of terrorism related case and other examples, focus is brought on the importance of co-operation, between industry and Law enforcement, in cyber space. Co-operation between the two can produce excellent results for society as a whole and indifference towards each other can lead to catastrophic results, is brought out clearly in this talk. Is cyber space turning into pardise for terrorist and criminals? If so, is the computer industry, unwittingly contributing to it? Are we really learning from our past mistakes? An attempt to answers these questions is also made through this talk.

Marc Feidt—Thursday @ 09:45-10:45

Head of Unit, Corporate Infrastructure Service, DIGIT
European Commission (EU)

Marc J. Feidt holds a degree in Computer Science from the University of Karlsruhe since 1979.

He started his carrier as a software developer in the field of compiler construction and simulation systems. Subsequently, he worked for several years as consultant for relational database design, migration and operations.

Since he joined the European Commission in May 1989, he has continued working in the IT area, first at Eurostat, then the Informatics Directorate and finally at Directorate-General for Informatics (DIGIT).

In 2004 he was appointed Head of Unit for Planning and Resources in DIGIT and since 2008, he became responsible for the unit in charge of Corporate Infrastructure Services within DIGIT.

The unit "Corporate Infrastructure Services" provides the Commission with secure, reliable and high performance Corporate Information Technology and Telecommunications Infrastructure. The unit's services portfolio are the physical network infrastructure service, the data network services supporting internal and external data communications including the sTESTA network and the IT infrastructure services in the Commission's Data Centres.

Marc is a member of the "Gesellschaft für Informatik (GI)".

IT Security in the European Digital Agenda

TBA

Michael Moran—Thursday @ 11:00-12:00

Coordinator, Crimes Against Children
Serious Crime Directorate, INTERPOL

Michael Moran is a Detective Sergeant in An Garda Síochána; and is currently the coordinator of Crimes against Children at INTERPOL. This team handle all aspects of international crimes against children especially online child exploitation and travelling sex offenders. He has been seconded to Interpol since 2006. He started working in online Child Exploitation in Dublin around 1997. He has worked in Mainstream Policing, Drugs, Serious Crime and Computer Crime.

Prior to coming to Interpol he was a supervisor at the Computer Crime Unit, Garda Bureau of Fraud Investigation, Dublin.

Michael holds a degree in IT from the Institute of Public Administration in Dublin and has a diploma in project management from University College Cork and the Irish Institute of project management. He is also a Certified Internet Webmaster. He also holds a MSc in Forensic Computing and Cybercrime investigation from the Center for Cybercrime investigation at the school of informatics in University College Dublin. He is an advisor at that school and lectures on the use of ICT by child sex offenders.

He has presented and lectured around the world on the issue of online child exploitation and is a lecturer at UCD on the investigation of cyber crimes against children.

Online exploitation of children—What's it got to do with me?

Child abuse material (child pornography) is a reality in the modern connected society and any corporate association with it can lead to prosecution and permanent brand damage. This talk will explain in detail the issues surrounding this phenomenon, the difficulties from a corporate point of view and give an understanding why risk management must also include the welfare of the children abused to produce it.

Mikko Hypponen—Friday @ 09:45-10:45

Chief Research Officer, F-Secure, FI

Mikko Hypponen is the Chief Research Officer for F-Secure, and has worked with F-Secure in Finland since 1991. Mr. Hypponen has assisted law enforcement in USA, Europe and Asia on cybercrime cases. He has written for magazines such as Scientific American, Foreign Policy and for newspapers like The New York Times.

State of the Net

25 years, and what have we got?

Mwende Njiraini—Friday @ 11:00-12:00

Associate and Internet Governance Tutor, DiploFoundation, KE

Mwende Njiraini is a DiploFoundation Internet Governance Building Programme (IGCBP) tutor. In this capacity she facilitates, on a yearly basis, collaborative learning on the internet governance process and associated infrastructure, legal, economic and social-cultural aspects for a group of approximately 15 participants from the African Region.

Mwende also works at the Communications Commission of Kenya, the ICT regulator, where she is in-charge of research on new and emerging communication technologies and their impact on the regulatory framework. In addition she has managed various projects including the establishment of the Kenya Network Information Centre, the .KE ccTLD manager where she was the acting Administrative Manager in the formative stages of the organisation. Most recently, as the Mobile Number Portability Project Manager, she has been facilited in the development of the Procedures and Guidelines for the Provision of Mobile Number Portability (MNP) Services in Kenya and the Mobile Number Portability Service Agreement.

Mwende represents her country in various ICT forums and meetings, most notably the ITU-T Study Group 17 on Cybersecurity and Internet Governance Forums. She is a Telecommunication Engineer by profession and holds a Master of Communications Management with Merit in Business Management from Coventry University, and a Master of Communications Management from University of Strathclyde, Glasgow.

Cybercrime in the Kenyan Context

The mobile phone has become the standard means of communication in Kenya providing basic voice and data services. Though volume of voice traffic continues to grow averaging 6.63 billion minutes as at September 2010, mobile data services including SMS, Internet, premium rate, mobile money and banking services hold a high growth potential.

With mobile penetration averaging 60% and 99% of the approximate 3.2 million internet/data subscriptions being through mobile phones, mobile telephony has changed the perception of cybersecurity in Kenya. Additionally, the range of critical services delivered over mobile networks continues to increase. Of particular concern is mobile money, it has gone beyond its initial role of providing financial services to the unbanked population, to providing value-added services which include payment of utility bills such as water, electricity and pay-TV.

Each of the four mobile operators in Kenya has a variant of mobile money services with Safaricom offering M-pesa; Essar Telecom, Yu-cash, Telkom Kenya, Orange-money and Airtel Networks, Airtel Money. However the entrance of network agnostic mobile money providers, mobile number portability as well as the potential implementation of money mobility across networks will undoubtedly increase the complexity of cybersecurity threats.

Using relevant examples, this presentation will explore the changing landscape of cybersecurity in Kenya as influenced by mobile services.

Do you want to present at the 2012 Annual Conference? Want to be on the 2012 Program Committee?

The Official Call for Speakers occurs every Autumn. Please ensure you watch for our conference emails and news announcements for all the latest information. All submissions must be made through the submission site.

Need some direction on topics? Want to join the program committee? Make sure to talk to the 2012 Program Chair, Jose Nazario of Arbor Networks. Jose will be walking around the conference and will be available to chat with interested individuals. Not sure where to find him? Head to the Registration Desk for assistance.

Conference Notes

Exhibits

BT

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 custromers around the world to manage and maintain secure and resilient networked IT infrastructures. http://www.globalservices.bt.com

Secunia

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 us at http://www.secunia.com

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. http://www.cisco.com

Lancope

Lancope®, Inc. is a leading provider of flow-based monitoring solutions to ensure high-performing and secure networks for global enterprises. Unifying critical network performance and security information for borderless network visibility, Lancope provides actionable insight that reduces the time between problem identification and resolution. http://www.lancope.com

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. http://www.netwitness.com

GFI Adanced Technology Group

GFI's Advanced Technology Group (ATG) markets and licenses GFI's threat analysis and malware detection technologies to large enterprises, government and defense agencies with uniquely sensitive and demanding IT security requirements; as well as to software developers and hardware manufacturers whose products require proven, embedded security solutions. http://www.gfi.com/atg

Exhibits

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 **http://www.mandiant.com.**

FireEye

FireEye is the leading provider of next-generation threat protection to combat advanced malware, zero-day and targeted APT attacks. FireEye's solutions supplement traditional and next-generation firewalls, IPS, Web gateways and antivirus, which cannot stop advanced threats leaving security holes in networks. Based in Milpitas, California, FireEye is backed by premier financial partners. **http://www.fireeye.com**

Fidelis Security

Fidelis Security Systems provides organizations with the network visibility, analysis and control necessary to manage advanced threats and prevent data breaches. Built on a patented Deep Session Inspection®, platform, Fidelis XPS™ is the industry's only network security solution capable of seeing, studying, and stopping advanced threats in real-time by uniquely working at the session-level where today's threats occur. **http://www.fidelissecurity.com**

AccessData

AccessData Group has pioneered digital investigations for 20+ years. Clients rely on AccessData's technologies for incident response and cyber security. Its new CIRT security framework integrates network analysis, host analysis and large-scale auditing into a single interface and facilitates continuous monitoring, while enabling more effective handling of advanced persistent threats and data spillage. **http://www.accessdata.com**

Splunk

Splunk Enables Operational Intelligence
Splunk is the world's leading software for monitoring, reporting and analyzing IT data. IT data is massive, unstructured and contains a definitive record of transactions, systems and user activity. Over 2,300 customers in 74 countries use Splunk to improve service levels, reduce operations costs, mitigate risk and gain operational intelligence. **http://www.splunk.com**

ValidEdge

Organizations under targeted attack use ValidEdge systems to eradicate malware-based threats. ValidEdge offers the world's leading anti-malware solution for faster identification and better mitigation against zero day and single target malware attacks in real time. ValidEdge purpose-built anti-malware systems allow you to detect, analyze and heal compromised systems.
http://www.validedge.com

Program Committee & Staff

About FIRST.Org

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 webservices
- Special interest groups
- Corporate Executive Programme (CEP)

Currently FIRST has over **240** 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 globale 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 Desk (located in the Geek Lounge) 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.

2011 Program Chair

Gavin Reid..............Cisco Systems, US

2011 Program Committee

Shin Adachi	NTT-CERT, US
Jeff Boerio	Intel, US
Andrew Cushman	Microsoft, US
Vafa Izadinia	Cisco Systems, US
Jose Nazario	Arbor Networks, US
Jacomo Piccolini	RNP/ESR Brazil, BR
Anu Puhakainen	Ericsson, FI
David Pybus	Diageo, UK
Bernd Reske	SAP, DE
Udo Schweigert	Siemens, DE
Marco Thorbruegge	ENISA
Ronaldo Vasconcellos	Independent, BR
Adrian Wiedemann	BFK, DE

FIRST Secretariat Services

NeuStar Secretariat Services

Nora Duhig
Michael Lee
Vid Luther

FIRST Conference Staff

Conference & Publication Services, LLC

Phoebe J. Boelter
Kristen Jacobucci
Traci Wei

FIRST™

Improving Security Together

save the date

security is not an island

HILTONMALTA

24th Annual FIRST Conference

MALTA

17 - 22 June 2012

© Image: Malta Tourism Authority/ Péter Vanicsek

FIRST gratefully acknowledges the 2011 Sponsorship Team.
Special thanks to our **2011 Local Host and Diamond Sponsor.**

CERT.at

BT

Platinum Sponsors

enisa
European Network
and Information
Security Agency

Microsoft®

citi

Gold Sponsor

Secunia
Stay Secure

Network Sponsor

CISCO™

Internet Sponsors

aconet
Austrian Academic Computer Network

A1 TELEKOM AUSTRIA

Banquet Sponsors

aconet
Austrian Academic Computer Network

CERT.at

kav
wiener
krankenanstalten verbund
Vienna Hospital Association

MA14
ICT for the City.

2011-2012 Fellowship Sponsors

NORTHWESTERN UNIVERSITY · QUAECUMQUE SUNT VERA · 1851
NORTHWESTERN
UNIVERSITY

PCH
Packet Clearing House

Supporting Sponsors

Google™

BFK
edv-consulting GmbH
www.bfk.de

RAIFFEISEN INFORMATIK

HITACHI

SAP®

SYNGRESS

netsecpodcast.com
THE NETWORK SECURITY PODCAST

EUROTRASH
Security with Funny Accents

NETWITNESS

Lancope®
The Leader in NetFlow Collection & Analysis™

GFI

MANDIANT®

FireEye™

FIDELIS
SECURITY SYSTEMS

AccessData®

splunk>

validEDGE