FIRST
Improving Security Together

Final Program

20th ANNUAL FIRST Conference
VANCOUVER British Columbia
Canada June 22-27, 2008

Overview

Sunday, June 22nd

Registration
Ice Breaker Reception

Monday, June 23rd

Tutorials
SIG Meetings

Tuesday, June 24th

Tutorials
SIG Meetings
Beer & Gear
Pre-AGM

Wednesday, June 25th

Conference Opening
Breakout Sessions
SIG Meetings
Geek Zones
Sponsors' Luncheon

Thursday, June 26th

General Session
Breakout Sessions
Geek Zones
SIG Meetings
Annual General Meeting (AGM)

Friday, June 27th

General Session
Breakout Sessions
Geek Zones
SIG Meetings
Conference Closing

20th Annual Conference Sponsorship Team

Diamond Sponsor

BT

Platinum Best Practices

CERT
Software Engineering Institute
Carnegie Mellon

Platinum / Geek Lounge

Microsoft®

Gold

citi

Gold

Q-CERT

Network

cisco™

Podcast

incoming thought

Polo Shirt

Sun® microsystems

T-Shirt

Google™

Folder

HITACHI

Lanyard/Badge

BFK

Sunday, June 22nd

14:00 – 18:00	Registration
19:00 – 21:00	**Added Attraction** Ice Breaker Reception

Monday, June 23rd

08:30 – 10:50	**Tutorial** MSFT Defend the Flag - Day 1	**Tutorial** System, Network and Security Log Analysis for Incident Response *Anton Chuvakin (LogLogic, Inc., US)*	**Geek Zone** Detecting Intrusions - The latest forensics tools and techniques to identify Windows malware infections *Pär Österberg-Medina (Swedish IT Incident Centre, Sitic, SE)*	**Special Interest Group** CVSS SIG *Gavin Reid (Cisco Systems, US)*
10:50 – 11:10	Morning tea break			
11:10 – 12:30	MSFT Defend the Flag - Day 1 (continued)	System, Network and Security Log Analysis for Incident Response (continued)	Detecting Intrusions - The latest forensics tools and techniques to identify Windows malware infections (continued)	Vendor SIG *Bruce Monroe (Intel, US), Damir (Gaus) Rajnovic (Cisco PSIRT – Cisco Systems Co., UK)*
12:30 – 14:00	Lunch break			
14:00 – 15:20	MSFT Defend the Flag - Day 1 (continued)	System, Network and Security Log Analysis for Incident Response (continued)	Detecting Intrusions - The latest forensics tools and techniques to identify Windows malware infections (continued)	Vendor SIG (continued)
15:20 – 15:40	Afternoon tea break			
15:40 – 17:00	MSFT Defend the Flag - Day 1 (continued)	System, Network and Security Log Analysis for Incident Response (continued)	Detecting Intrusions - The latest forensics tools and techniques to identify Windows malware infections (continued)	Vendor SIG (continued)
	Tutorial I - Regency AB	Tutorial II - Regency C	Geek zone I - Plaza AB	SIG - Plaza C

Tuesday, June 24th

08:30 – 10:50	**Tutorial** MSFT Defend the Flag - Day 2	**Special Interest Group** FIRST Law Enforcement/ CSIRT Cooperation SIG (LECC-SIG) – Related G8: HI-Tech Crimes Workshop *Yurie Ito (JPCERT/CC, JP)*	**Tutorial** Creating and Managing Computer Security Incident Response Teams(CSIRTs) *Georgia Killcrece , Mark Zajicek , Robin Ruefle (CERT/CC – Carnegie Mellon University, US)*	**Tutorial** Techies Can Communicate Too ! *David Pybus (Diageo, UK), Don Stikvoort (S-CURE, NL)*
10:50 – 11:10	Morning tea break			
11:10 – 12:30	MSFT Defend the Flag - Day 2 (continued)	FIRST Law Enforcement/ CSIRT Cooperation SIG (LECC-SIG) – Related G8: HI-Tech Crimes Workshop (continued)	Creating and Managing Computer Security Incident Response Teams(CSIRTs) (continued)	Techies Can Communicate Too ! (continued)
12:30 – 14:00	Lunch break			
14:00 – 15:20	MSFT Defend the Flag - Day 2 (continued)	**Tutorial** The life cycle of infections and a botnet *Richard Perlotto (Shadowserver Foundation, US)*	Creating and Managing Computer Security Incident Response Teams(CSIRTs) (continued)	**Special Interest Group** Network Monitoring SIG - Monitoring and Detection of Fast-Flux Service Networks *Carol Overes (GOVCERT. NL, NL)*

15:20 – 15:40	Afternoon tea break			
15:40 – 16:30	MSFT Defend the Flag - Day 2 (continued)	The life cycle of infections and a botnet (continued)	Creating and Managing Computer Security Incident Response Teams(CSIRTs) (continued)	Network Monitoring SIG - Large-scale Monitoring of Fast-Flux Service Networks *Carol Overes (GOVCERT.NL, NL)*
16:30 – 18:00	**Added Attraction** Bear n' Gear			
18:00 – 19:00	**Pre AGM**			
	Tutorial I - Regency AB	Tutorial II - Regency C	Tutorial III - Plaza AB	Tutorial IV - Plaza C

Wednesday, June 25th

08:30 – 09:00	Opening Remarks *Derrick Scholl (FIRST Steering committee chair, US)*				
09:00 – 09:45	Enabling End-to-End Trust ***Scott Charney (Corporate Vice President, Trustworthy Computing, Microsoft, US)***				
09:50 – 10:20	The State of Internet Phishing and Fraud and Useful Means to Combat It *Foy Shiver (The Anti Phishing Working Group, US)*	Safety and Security of Networked LANs in Aircraft *Eric Fleischman (Boeing, US)*	A Collaborative Approach to Anti-Spam *Chia-Mei Chen (TWCERT/CC – National Sun Yat-Sen University, TW)*	**Geek Zone** Malcode Analysis Techniques for Incident Handlers *Russ McRee (holisticinfosec.org, US)*	**Geek Zone** Applied Security Visualization *Raffael Marty (Splunk, US)*
10:20 – 10:50	The State of Internet Phishing and Fraud and Useful Means to Combat It (continued)	Safety and Security of Networked LANs in Aircraft (continued)	Semantic Potential of Existing Security Advisory Standards *Stefan Fenz (Secure Business Austria, AT)*	Malcode Analysis Techniques for Incident Handlers (continued)	Applied Security Visualization (continued)
10:50 – 11:10	Morning tea break				
11:10 – 11:40	International Privacy & Security Compliance — Navigating the Maze *Steven Ringelberg (Vanguard Integrity Professionals, US)*	Malicious Websites on the Chinese Web: Overview and Case Study *Dr Minghua Wang (CNCERT/CC – National Computer Network Emergency Response Technical Team / Coordination Center of China, CN)*	**Geek Zone** Responding to Security Incidents: Are Security Tools Everything You Need? *Rodrigo Werlinger (University of British Columbia, CA)*	Practical RFID hacking without soldering irons (or Patent Attorneys) *Adam Laurie (RFIDIOt, UK)*	Applied Security Visualization (continued)
11:40 – 12:10	International Privacy & Security Compliance — Navigating the Maze (continued)	Push-Email in the Enterprise. Is it BlackBerry, WindowsMobile or Symbian? *Dr. Heiko Patzlaff (Siemens AG, Corporate Technology, CT IC CERT, DE)*	Tunisia's experience in building an information sharing and analysis center *Haythem EL MIR (Technical Department / NACS, TN)*	Practical RFID hacking without soldering irons (or Patent Attorneys) (continued)	Applied Security Visualization (continued)

12:10 – 12:50	Emerging Economies: The Vulnerability Market *Terri Forslof (TippingPoint, a division of 3Com, US)*	**Panel** Dutch Banking Panel: An overview and panel discussion about the cooperation between banks and the CSIRT community in light of phishing and other recent threats	CERTification: Assessing CSIRT Maturity *Klaus-Peter Kossakowski (PRE-CERT – PRESECURE Consulting GmbH, DE), Don Stikvoort (S-CURE, NL)*	Tales from the dark. Diary of a compromised Windows Vista *Jacomo Piccolini (CAIS/RNP – Brazilian Academic and Research Network, BR), Ivo Carvalho Peixinho (CAIS/RNP – Brazilian Federal Police, BR)*	Applied Security Visualization (continued)
12:50 – 14:10	Lunch break				
14:10 – 14:50	The Dark Future of Desktop Security and How to Stop It ***Ivan Krstić***				
14:50 – 15:40	Malware Without Borders - Multi-Party Response *Jeff Williams , Ziv Mador (Microsoft, US)*	SCADA Security – Who Is Really In Control of Our Control Systems? *Peter G. Allor (IBM Internet Security Systems, US)*	**Special Interest Group** Abuse Handling SIG *Martijn van der Heide (KPN-CERT – Chairman KPN-CERT, NL)*	Event Correlation for Early Warning Systems *Till Dörges (PRE-CERT – PRESECURE Consulting GmbH, DE)*	Incident Handling around the world in 80 ms. (Well not really that fast) *Greg Bassett, Steve Mancini (Intel Corporation, US)*
15:40 – 16:00	Afternoon tea break				
16:00 – 17:00	Intellectual Property Loss in the Global Marketplace *Christopher Burgess (Cisco, US)*	Has Pakistan stolen your traffic lately? – Threats to Internet Routing and Global Connectivity *Earl Zmijewski (Renesys, US)*	Abuse Handling SIG (continued)	The Most Important Thing: How Mozilla Does Security and What You Can Steal *Johnathan Nightingale (Mozilla, CA)*	Incident Handling around the world in 80 ms. (Well not really that fast) (continued)
19:00 – 23:00	**Social event** Conference Banquet *Pan Pacific Hotel Crystal Pavilion (Waterfront Road & Howe Street at Canada Place)*				
	Breakout I - Regency CDEF	Breakout II - Regency AB	Breakout III / SIG - Plaza A	Geek zone I / Breakout III - Georgia B	Geek Zone II / Geek Zone I - Georgia A

Thursday, June 26th

08:30 – 09:00	Opening Remarks				
09:00 – 10:00	The Enterprise’s Role in Protecting Critical Infrastructures ***John Stewart (Cisco Systems, US)***				
10:00 – 10:50	Computer Forensics for Managers and IT Administrators What you need to know *Chris van Breda (Cyberklix, CA)*	Incident Management Mission Diagnostic(IMMD) Method *Georgia Killcrece, Mark Zajicek, Robin Ruefle (CERT/CC – Carnegie Mellon University, US)*	FMC (Fixed Mobile Convergence) - What About Security *Franck Veysset (France Télécom R&D, FR)*	**Geek Zone** Inside a BBB Malware Scheme - Mapping and Dissecting Attacker Infrastructure *Michael La Pilla (VeriSign – iDefense, US)*	**Geek Zone** The future of hacking: Blended attacks using social engineering *Peter Wood (First Base Technologies, UK)*
10:50 – 11:10	Morning tea break				

11:10 – 11:40	Industry Briefing – An Exercise in Vendor Coordination *Peter G. Allor (IBM Internet Security Systems, US)*	Safely Sharing Data Between CSIRTs for Collaborative Security: The SCRUB* Anonymization Tool Infrastructure *William Yurcik (University of Texas at Dallas, US)*	Matrix, a Distributed Honeynet and its Applications *Yonglin Zhou (CNCERT/CC – National Computer Network Emergency Response Technical Team / Coordination Center of China, CN)*	Virtualization Technology A Manifold Arms Race *Michael H. Warfield (IBM Internet Security Systems, US)*	The future of hacking: Blended attacks using social engineering (continued)
11:40 – 12:10	Industry Briefing – An Exercise in Vendor Coordination (continued)	GridCERT Services - Modification of traditional and additional new CERT Services for Grids *Antonio Liu (PRESECURE, DE)*	Spotspam - Tackling Spam at New Frontiers *Przemyslaw Jaroszewski (CERT POLSKA, PL)*	Virtualization Technology A Manifold Arms Race (continued)	The future of hacking: Blended attacks using social engineering (continued)
12:10 – 12:50	Who's watching the watch dogs? Security Audits for network infrastructure security enforcement devices *Kowsik Guruswamy (Mu Dynamics, US)*	The HoneySpider Network: Fighting client-side threats *Piotr Kijewski (CERT POLSKA – NASK/CERT Polska, PL), Carol Overes (GOVCERT.NL, NL), Rogier J.L. Spoor (SURFnet-CERT – SURFnet, NL)*	National spam monitoring network *Juan Díez González, Luis Fernández (INTECO, ES)*	About the Security Pros and Cons of Server Virtualization *Dr. Martin Wimmer (Siemens AG, Corporate Technology, CT IC CERT, DE)*	Tracking and Detecting Trojan Command and Control Servers *Ryan Olson (VeriSign – Verisign/iDefense, US)*
12:50 – 14:10	Lunch break				
14:10 – 14:50	Insecurity ***J. D. Frazer (UserFriendly.org, CA)***				
14:50 – 15:20	The Easiest Score on the Internet - PII and corporate secrets for the taking on P2P file sharing networks. *Chris Gormley (Tiversa, Inc., US)*	Automating Vulnerability Management in a Heterogeneous Enterprise *Jeff Boerio (Intel Corporation, US)*	Barriers to CSIRTS cooperation with other CSIRTS and The CLOSER Project *Emin Akhundov, Krzysztof Silicki, Miroslaw Maj (NASK/CERT Polska, PL)*	Bot Herder Case Studies *Richard Perlotto (Shadowserver Foundation, US)*	Trends in the Internet Underground / Cyber Kadogos *Christopher Abad (20 GOTO 10, US)*
15:20 – 15:40	The Easiest Score on the Internet - PII and corporate secrets for the taking on P2P file sharing networks. (continued)	Automating Vulnerability Management in a Heterogeneous Enterprise (continued)	Barriers to CSIRTS cooperation with other CSIRTS and The CLOSER Project (continued)	Bot Herder Case Studies (continued)	Trends in the Internet Underground / Cyber Kadogos (continued)
15:40 – 17:50	**Annual General Meeting (AGM)** ** Limited to FIRST team members and their invited guests, subject to approval by the Steering Committee*				
	Breakout I - Regency CDEF	Breakout II - Georgia B	Breakout III / SIG - Plaza A	Geek zone I - Regency AB	Geek zone II - Georgia A

Friday, June 27th

08:30 – 08:50	Opening Remarks				
08:50 – 09:30	Internet Law Update 2008 William Cook (Wildman, Harrold, Allen and Dixon LLP, US)				
09:30 – 10:20	Public and Private Collaboration for Improved National Cyber Security *Peter G. Allor (IBM Internet Security Systems, US)*	Cyber Fraud Trends *Ralph Thomas (VERISIGN iDefense, US)*	Putting private and government CERT's to the test *Stephen Frei (ETH Zurich, CH)*	**Geek Zone** Security Testing: Moving Beyond the Penetration Test *Kenneth R. van Wyk (KRvW Associates, LLC, US)*	**Geek Zone** Building a no frills malware lab: How to construct a relatively inexpensive, yet effective, malware analysis lab for CIRTs *Andre Cormier, Robert Pitcher (CCIRC, CA)*
10:20 – 10:40	Morning tea break				
10:40 – 11:30	Securing Wiki-Style Technology in the Global Enterprise: The Competing Tensions of Privacy Law and Distributed Collaboration *Steven Michalove (Microsoft, US), Thomas Daemen (Microsoft, BE)*	Security Breaches: To Disclose or not to Disclose *Gib Sorebo (SAIC, US)*	**Special Interest Group** CSIRT Metrics SIG *Georgia Killcrece (CERT/CC – Carnegie Mellon University, US)*	Identifying network scanning tools *Kenneth R. van Wyk (KRvW Associates, LLC, US), Robert Floodeen (Spectrum, US)*	Building a no frills malware lab: How to construct a relatively inexpensive, yet effective, malware analysis lab for CIRTs (continued)
11:30 – 12:20	Models and Experiences for National and International Information Sharing *Andrea Rigoni (Symantec, UK)*	Security and Education – Bringing it all Together *Frank Wintle (PanMedia Ltd, UK)*	CSIRT Metrics SIG (continued)	Beyond a sensor: Towards the Globalization of SURFids *Wim Biemolt (SURFnet, NL)*	Building a no frills malware lab: How to construct a relatively inexpensive, yet effective, malware analysis lab for CIRTs (continued)
12:20 – 12:50	Managing Security & Privacy Incidents in the Health Care Environment *Bobby Singh (Smart Systems for Health Agency, CA)*	Efforts to Secure Electronic Financial Transactions *JinWook Choi (Financial Security Agency, KR)*	CSIRT Metrics SIG (continued)	Phishing without URL, when miscreants go malware *Atanai Sousa Ticianelli , Jacomo Piccolini (CAIS/RNP – Brazilian Academic and Research Network, BR)*	Building a no frills malware lab: How to construct a relatively inexpensive, yet effective, malware analysis lab for CIRTs (continued)
12:50 – 14:10	Lunch break				
14:10 – 14:30	Closing Remarks Derrick Scholl (FIRST Steering committee chair, US)				
	Breakout I - Regency CDEF	Breakout II - Regency AB	Breakout III / SIG - Plaza A	Geek zone I - Georgia B	Geek zone II - Georgia A