



## Conference schedule

### June 25th (Sunday)

14:00 - 18:00	Registration
16:00 - 17:00	Program Committee Meeting
19:00 - 21:00	Welcome Icebreaker Reception

### June 26th (Monday)

	Business/Management Track	Technical Track
07:30 - 17:00	Registration	
08:00 - 09:00	Continental Breakfast	
09:00 - 09:10	The Day Ahead	The Day Ahead
09:10 - 10:30	<b>Exploring the Next Level of Cyber Attacks: Methodologies and Demonstration of Web Application Hacks</b> Matt Fisher (SPI Dynamics, US)	<b>Secure Coding in C and C++</b> Robert Seacord (CERT/CC – Carnegie Mellon University, US)
10:30 - 11:00	Coffee break	
11:00 - 12:30	<b>Exploring the Next Level of Cyber Attacks: Methodologies and Demonstration of Web Application Hacks</b> (continued) Matt Fisher (SPI Dynamics, US)	<b>Secure Coding in C and C++</b> (continued) Robert Seacord (CERT/CC – Carnegie Mellon University, US)
12:30 - 14:00	Lunch	
14:00 - 15:30	<b>Evaluating CSIRT Operations</b> Audrey Dorofee, Chris Alberts, Robin Ruefle (CERT/CC – Carnegie Mellon University, US)	<b>Design Your Network to Aid Forensic Investigation</b> Robert Sisk (IBM MSS – IBM Corporation, US)
15:30 - 16:00	Coffee break	
16:00 - 17:30	<b>Evaluating CSIRT Operations</b> (continued) Audrey Dorofee, Chris Alberts, Robin Ruefle (CERT/CC – Carnegie Mellon University, US)	<b>Design Your Network to Aid Forensic Investigation</b> (continued) Robert Sisk (IBM MSS – IBM Corporation, US)
18:00 - 19:00	Pre AGM Discussions (FIRST members only)	

18<sup>th</sup> Annual FIRST Conference  
 June 26 — 30, 2006  
 Baltimore, Maryland, USA

---

June 27th (Tuesday)

	Business/Management Track	Technical Track
07:30 - 17:00	Registration	
08:00 - 09:00	Continental Breakfast	
09:00 - 09:10	The Day Ahead	The Day Ahead
09:10 - 10:30	<b>Log Data Analysis for Incident Response</b> Anton Chuvakin (LogLogic, Inc., US)	<b>Next Steps in Bridging the Gap</b> Gary McGraw (Cigital, Inc., US), Kenneth van Wyk (KRvW Associates, LLC, US)
10:30 - 11:00	Coffee break	
11:00 - 12:30	<b>Log Data Analysis for Incident Response</b> (continued) Anton Chuvakin (LogLogic, Inc., US)	<b>Next Steps in Bridging the Gap</b> (continued) Gary McGraw (Cigital, Inc., US), Kenneth van Wyk (KRvW Associates, LLC, US)
12:30 - 14:00	Lunch	
14:00 - 15:30	<b>IT Security Teams and Outsourced Managed Security Services - working together</b> Chris van Breda (Cyberklix, CA)	<b>Honeypot Technology: Principles and Applications</b> Franck Veysset, Laurent Butti (France Télécom R&D, FR)
15:30 - 16:00	Coffee break	
16:00 - 17:30	<b>IT Security Teams and Outsourced Managed Security Services - working together</b> (continued) Chris van Breda (Cyberklix, CA)	<b>Honeypot Technology: Principles and Applications</b> (continued) Franck Veysset, Laurent Butti (France Télécom R&D, FR)
19:00 - 21:00	Birds of a Feather Sessions	

June 28th (Wednesday)

07:30 - 17:00	Registration
08:00 - 09:00	Continental Breakfast
09:00 - 09:10	Welcome and Conference opening
09:10 - 09:50	<b>Keynote: Computer Security Incident Response - Past, Present, Future</b> Richard Pethia (CERT/CC – Carnegie Mellon University, US)
09:50 - 10:30	<b>Sharing Sensitive Information without Compromising Data</b> Peter Allor (ISS – Internet Security Systems, US)
10:30 - 11:00	Coffee break

18<sup>th</sup> Annual FIRST Conference  
 June 26 — 30, 2006  
 Baltimore, Maryland, USA

June 28th (Wednesday) – continued

	Business/Management Track	Technical Track
11:00 - 12:00	<b>CERT's Virtual Training Environment: A New Model for Security and Compliance Training</b> James Wrubel (CERT/CC – Carnegie Mellon University, US)	
12:00 - 12:30	<b>If You Don't Know What You Don't Know</b> Arjen de Landgraaf (Co-Logic Security, Ltd, NZ)	
12:30 - 14:00	Lunch	
14:00 - 14:30	<b>Risk Analysis Methodology for New IT Service</b> Jun Heo Yoojae Won (KrCERT/CC – Korea Information Security Agency, KR)	<b>Reliably Determining the Outcome of Computer Network Attacks</b> Barry Mullins, David Chaboya, Richard Raines, Rusty Baldwin (AFCERT – Air Force Institute of Technology, US)
14:30 - 15:00	<b>The Impact of Honeynets for CSIRTs</b> Jan Kohlrausch, Jochen Schönfelder (DFN-CERT – DFN-CERT Services GmbH, DE)	<b>Automated Extraction of Threat Signatures from Network Flows</b> Piotr Kijewski (CERT POLSKA – Research and Academic Computer Network in Poland, PL)
15:00 - 15:30	<b>A Strategy for Inexpensive Automated Containment of Infected or Vulnerable Systems</b> Steven Sim Kok Leong (NUSCERT – National University of Singapore, SG)	<b>Behavioral Study of Bot Obedience using Causal Relationship Analysis</b> Lari Huttunen, Pekka Pietikäinen (University of Oulu, FI)
15:30 - 16:00	Coffee break	
16:00 - 16:30	<b>Maximizing the Benefits of Intrusion Prevention Systems: Effective Deployment Strategies</b> Calvin Miller, Charles Iheagwara, Farrukh Awan, Yusuf Acar (District of Columbia Government, US)	<b>A Distributed Intrusion Detection System Based on Passive Sensors</b> Rogier Spoor (SURFnet-CERT – SURFnet, NL)
16:30 - 17:00	<b>Designing and Developing an Application for Incident Response Teams</b> Kees Leune, Sebastiaan Tesink (Tilburg University, NL)	<b>Netflow Tools NfSen and NFDUMP</b> Peter Haag (SWITCH-CERT – The Swiss Education and Research Network, CH)
17:00 - 17:30	<b>Threats of P2P File Sharing Software - a Japanese Situation About "Winny"</b> Keisuke Kamata, Yuichi Miyagawa (JPCERT/CC – JPCERT Coordination Center, JP)	<b>Proactive Security Monitoring in a Policy Managed Network</b> Klaus-Peter Kossakowski (Software Engineering Institute, DE), Till Dörge (PRE-CERT – PRESECURE Consulting GmbH, DE)
19:00 - 23:00	Evening at the Aquarium – Sponsored by Co-Logic Security, Ltd.	

18<sup>th</sup> Annual FIRST Conference  
 June 26 — 30, 2006  
 Baltimore, Maryland, USA

---

June 29th (Thursday)

	Business/Management Track	Technical Track
07:30 - 17:00	Registration	
08:00 - 09:00	Continental Breakfast	
09:00 - 09:10	The Day Ahead	
09:10 - 09:50	<b>Keynote: Building Effective Relationships between CSIRTs and Law Enforcement</b> Brian Nagel (Assistant Director, Office of Investigations, U.S. Secret Service, US)	
09:50 - 10:30	<b>The Underground Economy</b> Rob Thomas (Team Cymru – Team Cymru, US)	
10:30 - 11:00	Coffee break	
11:00 - 11:45	<b>A Year's Evolution on Attacks Against Online Banking Customers</b> Matthew Pemble (RBSG – Royal Bank of Scotland, UK)	
11:45 - 12:30	<b>Botnets as Vehicle for Online Crime</b> Aaron Hackworth, Nicholas Ianelli (CERT/CC – Carnegie Mellon University, US)	
12:30 - 14:00	Lunch	
14:00 - 14:30	<b>CarmentiS - a German Early Warning Information System - Challenges and Approaches</b> Jürgen Sander (PRE-CERT – PRESECURE Consulting, GmbH, DE), Klaus-Peter Kossakowski (Software Engineering Institute, DE)	<b>Building and Deploying Billy Goat: a Worm-Detection System</b> Diego Zamboni, James Riordan, Yann Duponchel (IBM MSS – IBM Zurich Reserch Laboratory, CH)
14:30 - 15:00	<b>Counter-Forensic Tools: Analysis and Data Recovery</b> Matthew Geiger (CERT/CC – Carnegie Mellon University, US)	<b>RAPIER - A 1st Responders Info Collection Tool</b> Joseph Schwendt, Steven Mancini (IFT – Intel Corporation, US)
15:00 - 15:30	Coffee break	
15:30 - 17:30	FIRST Annual General Meeting	

18<sup>th</sup> Annual FIRST Conference  
 June 26 — 30, 2006  
 Baltimore, Maryland, USA

June 30th (Friday)

	Business/Management Track	Technical Track
07:30 - 17:00	Registration	
08:00 - 09:00	Continental Breakfast	
09:00 - 09:10	The Day Ahead	
09:10 - 09:50	<b>Keynote: Fixing Internet Security by Hacking the Business Climate</b> Bruce Schneier (Counterpane Internet Security, Inc., US)	
09:50 - 10:30	<b>The Survivability and Information Assurance (SIA) Curriculum</b> Lawrence Rogers (CERT/CC – Carnegie Mellon University, US)	
10:30 - 11:00	Coffee break	
11:00 - 11:45	<b>Legal Representatives - CERT Panel Discussion</b> Chris Painter (Department of Justice, US), Damir Rajnovic (Cisco PSIRT – Cisco Systems Co., UK), Etsuo Doi (Attorney-at-law, JP), Tara Flanagan (Cisco Systems – Cisco Systems Ltd., US), Terence Palfrey (Crown Prosecution Services, UK)	
11:45 - 12:30	<b>VisFlowConnect-IP : A Link-Based Visualization of NetFlows for Security Monitoring</b> William Yurcik (NCSA-IRST – National Center for Supercomputing Applications, US)	
12:30 - 14:00	Lunch	
14:00 - 14:30	<b>Effectiveness of Proactive CSIRT Services</b> Johannes Wiik, Jose Gonzalez (Agder University, NO), Klaus-Peter Kossakowski (Software Engineering Institute, DE)	<b>Worm Poisoning Technology and Application</b> Cui Xiang, Wu Bing, Yonglin Zhou, Zou Xin (CNCERT/CC – National Computer Network Emergency Response Technical Team / Coordination Center of China, CN)
14:30 - 15:00	<b>Proposal of RSS Extension for Security Information Exchange</b> Masato Terada (HIRT – Hitachi, JP)	<b>A Framework for Effective Alert Visualization</b> Jon Ramsey, Uday Banerjee (SWRX CERT – SecureWorks, US)
15:00 - 15:30	<b>The Network-Centric Incident Response and Forensics Imperative</b> Richard Bejtlich (TaoSecurity, US)	<b>Time Signatures to Detect Multi-headed Stealthy Attack Tools</b> Fabien Pouget (CERTA – French Government, FR), Guillaume Urvoy-Keller, Marc Dacier (Institut EURECOM, FR)
15:30 - 16:00	Closing	