FIRST™

Improving Security Together

CONFERENCE PROGRAM

Aftermath: Crafts and Lessons of Incident Recovery

HOTEL GRANVIA KYOTO STATION
KYOTO, JAPAN

21st Annual FIRST Conference
KYOTO June 28-July 3, 2009

WELCOME

Dear Participant,

It is my great privilege and pleasure to welcome you to the 21st Annual FIRST conference here in Kyoto, Japan. The list of speakers and events coupled with the knowledge, experience, expertise and variety of attendees promises to make this a fantastic week.

As I'm nearing the end of my 2nd and final term as Chairman of the Steering Committee, I remain convinced that FIRST is a wonderful and important organization. Through changing technologies, economic fortunes and misfortunes, and an ever evolving list of threats, the need for smart security practitioners to work together and share ideas and information is as crucial now as it was when FIRST was founded over two decades ago.

I applaud you and your organizations for making the commitment to attend this conference. As the economy shrinks and budgets tighten, it is often easy to take funding from areas like security that don't appear to have a direct return on investment. But, as all of us know, financial difficulties certainly don't lessen the threats to our IT environments, if anything it might increase the motivation of the attackers. By recognizing the importance of staying current and informed, we have an opportunity to strengthen our skills during this challenging time.

While I applaud you for being here, I think we also must realize the challenge and responsibility we have in being able to spend this week together. I challenge you to make as much of this opportunity as possible. In addition to the great sessions, spend as much time as you can speaking with your colleagues gathered here. Spend some time with old friends, but reach out and make new connections. Talk about what works well for you and what challenges you face. And, of course, have some fun.

I thank all of our experts who are sharing their time, experience and expertise by presenting at this conference. I'd also like to thank the attendee for bringing their knowledge and sharing that knowledge with the rest of us. There is a long line of people who make this conference possible who also deserve our deepest gratitude. The members of the program committee worked hard to bring us the best possible program, and for that I thank them. To the Steering Committee, and their employers, who dedicate large amounts of time and money to work year round to keep this organization strong and moving forward my thanks as well. To Phoebe, Kristen, Traci, and the rest of the staff who work so long and mostly behind the scenes, thank you again for your great work and dedication, we truly couldn't do this without you. And to Mick who has been working with us for a year and a half, I alone can't thank you enough for the work you have done.

It has been my great honor to have been able to serve as the Chairman of the Steering Committee for the last two years. Thank you for that opportunity, and thank you for coming. I know we're going to have a great conference, and I hope to see all of you again next year in Miami.

Derrick Scholl

Derrick Scholl
Chairman, FIRST Steering Committee

FIRST™
Improving Security Together

2008-2009 Steering Committee

Kenneth Van Wyk | Vice Chair
KRvW Associates LLC, USA

Chris Gibson | CFO
Citigroup, UK

Peter Allor | Conference Liaison
IBM, USA

Yurie Ito
JPCERT/CC, Japan

Scott McIntyre
KPN-CERT, Netherlands

Arnold Yoon
National Energy Technology Lab, USA

Thomas Mullen
BT, UK

Stephen Adegbite
Microsoft, USA

Francisco Jesus Monserrat Coll
RedIRIS, Spain

21st Annual FIRST Conference
KYOTO June 28-July 3, 2009

TABLE OF CONTENTS

FIRST Secretariat

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

Email: 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

Email: first-2009@first.org
Phone: +1-312-372..1255

Venue Information

HOTEL GRANVIA KYOTO
901 Higashi-Shiokoji-cho, Shiokoji
Sagaru,Karasuma-Dori,
Shimogyo-ku, Kyoto 600-8216
Japan

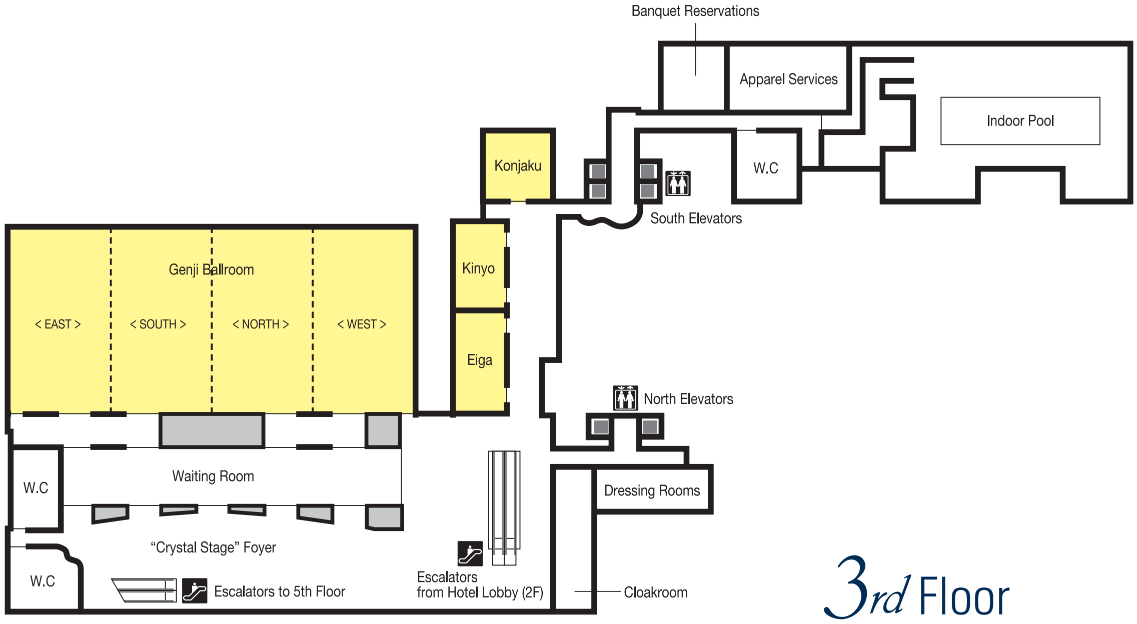
Phone: +81-075-344-8888

Websites

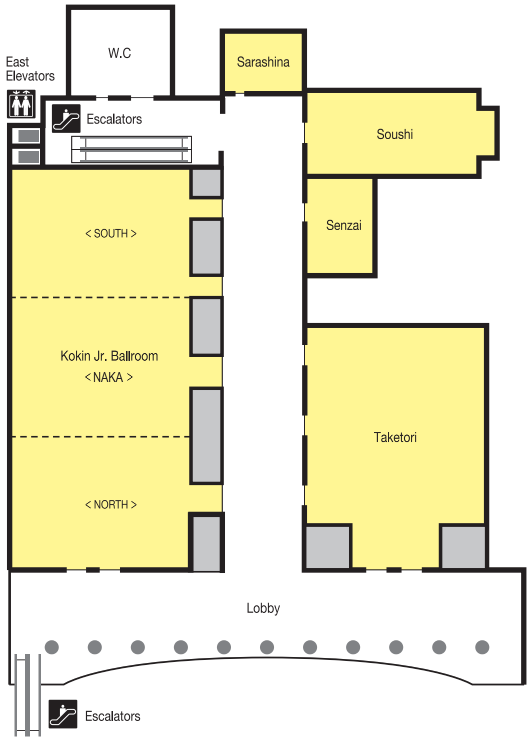
http://www.first.org
http://conference.first.org

Follow live conference updates on Twitter! @firstdotorg

FLOOR PLANS

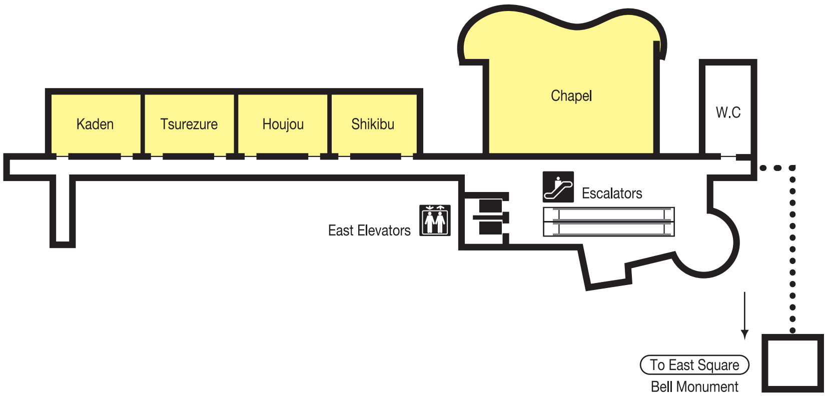


3rd Floor



5th Floor

7th Floor



SCHEDULE AT-A-GLANCE

Schedule At-A-Glance

Registration | 3F Genji Waiting Room
Sunday, 14:00-18:00
Monday-Friday, 08:00-16:30

High Tech Experience Lounge | 3F Konjaku
Monday-Friday, 08:00-18:00

Vendor Tables | 3F Genji Waiting Room
Tuesday - 17:00-19:30
Wednesday-Friday - 08:00-18:00

Continental Breakfast | 3F Genji South & East
Monday-Friday, 07:30-08:45

Lunch | 12:00-13:30
M, T, TH - 3F Genji South & 5F Taketori
Wednesday - 3F Genji South
Friday - 3F Genji South & East

Saturday, June 27

13:00-17:00	Train the Trainers (Open)	5F Kokin North

Sunday, June 28

09:00-17:00	Train the Trainers (Open)	3F Genji West
19:00-21:00	Ice Breaker Reception	3F Genji West & North

Monday, June 29

08:45-10:30	Conference Opening	3F Genji West & North
11:00-17:30	Track I: Technical	3F Genji West & North
11:00-17:30	Track II: Management	5F Kokin North
11:00-12:00	Track III: Incident Response	5F Kokin Naka
13:30-17:30	Law Enforcement Special Interest Group (LE SIG)	5F Kokin Naka

Tuesday, June 30

08:45-10:30	General Session	3F Genji West & North
11:00-12:00	Track I: Technical	5F Kokin Naka
11:00-17:00	Track II: Managment	5F Kokin North
11:00-17:00	Track III: Incident Response	3F Genji West & North
11:00-17:00	Network Monitoring Special Interest Group (NM SIG)	5F Kokin Naka
13:30-17:00	Vendor Special Interest Group (Vendor SIG)	7F Houjou
17:00-19:30	Vendor Showcase	3F Genji Waiting Room
18:00-19:30	Pre-Annual General Meeting (Open)	3F Genji West & North

Wednesday, July 1

08:45-10:30	General Session	3F Genji West & North
11:00-17:30	Track I: Technical	5F Kokin North
11:00-17:30	Track II: Managment	3F Genji West & North
11:00-17:30	Track III: Incident Response	5F Kokin Naka
19:00-22:00	Banquet	3F Genji Ballroom

Thursday, July 2

08:45-10:30	General Session	3F Genji West & North
11:00-15:00	Track I: Technical	5F Kokin Naka
11:00-15:00	Track II: Managment	3F Genji West & North
11:00-15:00	Track III: Incident Response	5F Kokin North
15:15-18:30	AGM (Members only)	3F Genji West & North

Friday, July 3

08:45-10:30	General Session	3F Genji West & North
11:00-14:30	Track I: Technical	5F Kokin North
11:00-14:30	Track II: Managment	3F Genji West & North
11:00-14:00	Track III: Incident Response	5F Kokin Naka
14:30-15:00	Conference Closing	3F Genji West & North

Translation Services Available

Saturday, June 27

13:00-17:00	**Train the Trainers (Open) – 5F Kokin North**

Sunday, June 28

09:00-17:00	**Train the Trainers (Open) – 3F Genji West**
14:00-18:00	**Registration – 3F Genji Waiting Room**
17:30-18:30	**Program Committee – 5F Soushi**
19:00-21:00	**Ice Breaker Reception – 3F Genji West & North**

Monday, June 29

08:00-16:30	**Registration – 3F Genji Waiting Room**		
08:45-10:30	**Conference Opening – 3F Genji West & North** **08:45-09:00 | Opening Welcome: Derrick Scholl**, Chair, FIRST, US **2009 & 2010 Program Chairs: Peter Allor**, Conference Liaison, FIRST, US **09:00-10:30 | Keynote: Suguru Yamaguchi, *Information Security Management and Economic Crisis,*** JPCERT Member & Advisor on Information Security, National Information Security Center, Cabinet Office Japan		
10:30-11:00	**Networking Break – 3F Genji Waiting Room and 5F Taketori + Foyer**		
11:00-12:00	**Track I: Technical** **3F Genji West & North**	**Track II: Management** **5F Kokin North**	**Track III: Incident Response** **5F Kokin Naka**
11:00-11:30	*Attacker Illusions: Finding the Real "Who" and "Why"* Michael La Pilla iDefense-VeriSign, US	*Architecting Systems of Systems for Response* Andrew McDermott SAIC, US	*Anti-Phishing Working Group and the Internet Policy Committee* Jordi Aguilà e-la Caixa CSIRT, ES Foy Shiver Anti-Phishing Working Group, US
11:30-12:00	*Attacker Illusions: Finding the Real "Who" and "Why"* (continued)	*Architecting Systems of Systems for Response* (continued)	*Measuring the Root Cause of Incidents* Karon Scarfone NIST, US
12:00-13:30	**Lunch – 3F Genji South & 5F Taketori**		
13:30-15:30	**Track I: Technical** **3F Genji West & North**	**Track II: Management** **5F Kokin North**	**Track III: Incident Response** **5F Kokin Naka**
13:30-14:00	*Proprietary Data Leaks: Response and Recovery* Sherri Davidoff Davidoff Information Security Consulting, LLC, US Jonathan Ham Lake Missoula Group, US	*Recapturing the Wheel-Media Perspectives on Crisis and Recovery* Frank Wintle PanMedia, UK	Law Enforcement Special Interest Group (LE SIG) See Attached Agenda
14:00-14:30	*Proprietary Data Leaks: Response and Recovery* (continued)	*Recapturing the Wheel-Media Perspectives on Crisis and Recovery* (continued)	LE SIG (continued) See Attached Agenda

Monday, June 29 (continued)

14:30-15:00	*The State of Phishing/Fraud and Efforts to Deliver Forensic Tools & Resources for ECrime Fighters* Foy Shiver Anti-Phishing Working Group, US	*Using Social Media in Incident Response* Martin McKeay The Network Security Blog, US	LE SIG (continued) See Attached Agenda
15:00-15:30	*The State of Phishing/Fraud and Efforts to Deliver Forensic Tools & Resources for ECrime Fighters* (continued)	*Public Relations & Incident Response Panel Discussion* Panelists: Martin McKeay The Network Security Blog, US Frank Wintle PanMedia, UK	LE SIG (continued) See Attached Agenda
15:30-16:00	**Networking Break – 3F Genji Waiting Room and 5F Taketori + Foyer**		
16:00-17:30	**Track I: Technical 3F Genji West & North**	**Track II: Management 5F Kokin North**	**Track III: Incident Response 5F Kokin Naka**
16:00-16:30	*Effective Software Vulnerability Discovery within a Time Constraint* Kaveh Razavi Dr. Babak Sadeghian Dr. Mehdi Shajari Amirkabir University of Technology, IR	*Trouble Ahead: Cyber Security Policy Developments...or the lack thereof* Eli Jellenc iDefense-VeriSign, US	LE SIG (continued) See Attached Agenda
16:30-17:00	*Effective Software Vulnerability Discovery within a Time Constraint* (continued)	*Emerging Threats and Attack Trends* Paul Oxman Cisco Systems, US	LE SIG (continued) See Attached Agenda
17:00-17:30	*What can FIRST do for you: a look at the available infrastructure options* Kenneth Van Wyk KRvW Associates, LLC	*Emerging Threats and Attack Trends* (continued)	LE SIG (continued) See Attached Agenda

Notes

Tuesday, June 30

08:00-16:30	**Registration – 3F Genji Waiting Room**		
08:45-10:30	**Conference Opening – 3F Genji West & North** **08:45-09:00 | Opening Remarks: Derrick Scholl**, Chair, FIRST, US **Best Practices Contest Winner Announcement: Jeffrey Carpenter**, CERT/CC, US **09:00-10:30 | Keynote: Bruce Schneier**, ***Reconceptualizing Security***, Chief Security Technology Officer, BT, UK		
10:30-11:00	**Networking Break – 3F Genji Waiting Room and 5F Taketori + Foyer**		
11:00-12:00	**Track I: Technical** **5F Kokin Naka**	**Track II: Management** **5F Kokin North**	**Track III: Incident Response** **3F Genji West & North**
11:00-11:30	*Network Monitoring Special Interest Group (NM SIG): Monitoring & Analyzing Client-side Attacks** Carol Overes GOVCERT.NL, NL Instructors: Tomasz Grudziecki Piotr Kijewski NASK, CERT-POLSKA	*Missing Clues: How to Prevent Critical Gaps in Your Security Monitoring* Martin Nystrom David Schwartzburg Cisco Systems, US	*Establishing Collaborative Response to Abuse of the Domain Name System* Greg Rattray ICANN, US
11:30-12:00	NM SIG: *Monitoring & Analyzing Client-side Attacks** (continued)	*Missing Clues: How to Prevent Critical Gaps in Your Security Monitoring* (continued)	*Establishing Collaborative Response to Abuse of the Domain Name System* (continued)
12:00-13:30	**Lunch – 3F Genji South & 5F Taketori**		
13:30-17:00	**Vendor Special Interest Group (Vendor SIG) – 7F Houjou** Damir "Gaus" Rajnovic Cisco Systems, UK		
13:30-15:30	**Track I: Technical** **5F Kokin Naka**	**Track II: Management** **5F Kokin North**	**Track III: Incident Response** **3F Genji West & North**
13:30-14:00	NM SIG: *Monitoring & Analyzing Client-side Attacks** (continued)	*The Next Generation of Incident Response* Gib Sorebo SAIC, US	*Comprehensive Response: A Bird's Eye View of Microsoft Critical Security Update MS08-067* Steve Adegbite Ziv Mador Jonathan Ness Microsoft, US
14:00-14:30	NM SIG: *Monitoring & Analyzing Client-side Attacks** (continued)	*The Next Generation of Incident Response* (continued)	*Comprehensive Response: A Bird's Eye View of Microsoft Critical Security Update MS08-067* (continued)
14:30-15:00	NM SIG: *Monitoring & Analyzing Client-side Attacks** (continued)	*Deriving information from raw data: making business decisions with logs* Toby Weir-Jones BT, US	*Comprehensive Response: A Bird's Eye View of Microsoft Critical Security Update MS08-067* (continued)

* *NM SIG agenda can be found: http://www.first.org/meetings/nm-sig/20090730.html.*
Please see the registration desk for advance DVD install.

Tuesday, June 30 (continued)

15:00-15:30	NM SIG: *Monitoring & Analyzing Client-side Attacks** (continued)	*Deriving information from raw data: making business decisions with logs* (continued)	*Comprehensive Response: A Bird's Eye View of Microsoft Critical Security Update MS08-067* (continued)
15:30-16:00	**Networking Break – 3F Genji Waiting Room and 5F Taketori + Foyer**		
16:00-17:00	**Track I: Technical 5F Kokin Naka**	**Track II: Management 5F Kokin North**	**Track III: Incident Response 3F Genji West & North**
16:00-16:30	NM SIG: *Monitoring & Analyzing Client-side Attacks** (continued)		*INTERPOL Initiatives to Enhance Cyber Security* Vincent Danjean INTERPOL, FR
16:30-17:00	NM SIG: *Monitoring & Analyzing Client-side Attacks** (continued)	*Information Security's Third Wave* Eli Jellenc iDefense-VeriSign, US	*INTERPOL Initiatives to Enhance Cyber Security* (continued)
17:00-19:30	**Vendor Showcase – 3F Genji Waiting Room**		
18:00-19:30	**Pre-Annual General Meeting (AGM) – 3F Genji West & North**		
20:00-22:00	**Metrics SIG** Georgia Killcrece CERT/CC		

2009 Best Practices Contest - Winners to be announced!

FIRST and CERT Coordination Center hosted a Best Practices Contest in conjunction with the 21st Annual FIRST Conference. Winners will be announced during Tuesday morning's opening remarks. For more information on the contest, please visit: **http://www.first.org/global/practices**.

Notes

Wednesday, July 1

08:00-16:30	**Registration – 3F Genji Waiting Room**		
08:45-10:30	**Conference Opening – 3F Genji West & North** **08:45-09:00 | Opening Remarks: Derrick Scholl**, Chair, FIRST, US **09:00-10:00 | Keynote: Jose Nazario**, ***Attacks Against the Cloud: Combating Denial-of-Service***, Arbor Networks, US **10:00-10:30 | Keynote: Kurt Sauer**, ***Information security one character at a time***, Spinlock Technologies, JP		
10:30-11:00	**Networking Break – 3F Genji Waiting Room and 5F Taketori + Foyer**		
11:00-12:00	**Track I: Technical** **5F Kokin North**	**Track II: Management** **3F Genji West & North**	**Track III: Incident Response** **5F Kokin Naka**
11:00-11:30	*A Method for Detecting Wide-scale Network Anomolies* Dr. Minghua Wang CNCERT/CC, PRC	*Threat Response–doing the right thing first time!* Greg Day McAfee, UK	*Windows Memory Forensics with Volatility** Andreas Schuster Deutche Telekom AG, DE
11:30-12:00	*Malicious Webpage Detection* Chia-Mei Chen TWCERT/CC Sun Yat-Sen University, TW	*Threat Response–doing the right thing first time!* (continued)	*Windows Memory Forensics with Volatility** (continued)
12:00-13:30	**Lunch – 3F Genji South**		
13:30-15:30	**Track I: Technical** **5F Kokin North**	**Track II: Management** **3F Genji West & North**	**Track III: Incident Response** **5F Kokin Naka**
13:30-14:00	*Information Security Exchange Formats and Standards* Till Dörges PRESENSE Technologies GmbH, DE	*SCADA Security - Who Is Really In Control of Our Control Systems?* Peter Allor IBM, US	*Windows Memory Forensics with Volatility** (continued)
14:00-14:30	*How to handle Domain Hijacking Incidents* Dr. Mehdi Shajari Amirkabir University of Technology, IR	*SCADA Security - Who Is Really In Control of Our Control Systems?* (continued)	*Windows Memory Forensics with Volatility** (continued)
14:30-15:00	*Mashup Security & Incident Response Considerations* Andrew McDermott SAIC, US	*When Worlds Collide: Understanding Telco Fraud in a VoIP World* Scott McIntyre KPN-CERT, NL	*Windows Memory Forensics with Volatility** (continued)
15:00-15:30	*Mashup Security & Incident Response Considerations* (continued)	*When Worlds Collide: Understanding Telco Fraud in a VoIP World* (continued)	*Windows Memory Forensics with Volatility** (continued)
15:30-16:00	**Meet the Candidates - 3F Next at the Membership Table**		
15:30-16:00	**Networking Break – 3F Genji Waiting Room and 5F Taketori + Foyer**		
16:00-17:30	**Track I: Technical** **5F Kokin North**	**Track II: Management** **3F Genji West & North**	**Track III: Incident Response** **5F Kokin Naka**
16:00-16:30	*Proactively Blacklisting Fast-Flux Domains and IP Addresses* Shahan Sudusinghe iDefense-VeriSign, US	*Incident Response and Voice for Voice Services* Lee Sutterfield SecureLogix, US	*Network Security Assistance to the Beijing Olympic Games* Yonglin Zhou CNCERT/CC, PRC

* *Windows Memory Forensics with Volatility prerequisites can be downloaded: http://conference.first.org/program/Schuster-Memory_analysis-Prerequisites.pdf*

Wednesday, July 1 (continued)

16:30-17:00	*Proposal of MyJVN for Security Information Exchange Infrastructure* Masato Terada IPA, JP	*Incident Response and Voice for Voice Services* (continued)	*Creating an End-to-End Identity Management Architecture* Jeff Crume IBM, US
17:00-17:30	*Handling Incidents from Honeynet Data* Adli Wahid CyberSecurity Malaysia, MY	*VoIP Panel Discussion* Panelists: Scott McIntyre KPN-CERT, NL Kurt Sauer Spinlock Technologies, JP Lee Sutterfield SecureLogix, US	*Creating an End-to-End Identity Management Architecture* (continued)
19:00-22:00	**Conference Banquet – 3F Genji Ballroom** ** Please wear you namebadges. ** Attendees with dietary requirements, please ensure you bring the colored card that was included in your badge at registration. Place your card on top of your plate allowing the wait staff to clearly see your card.		

Notes

Thursday, July 2

08:00-16:30	**Registration – 3F Genji Waiting Room**		
08:45-10:30	**Conference Opening – 3F Genji West & North** **08:45-09:00 | Opening Remarks: Derrick Scholl**, Chair, FIRST, US **09:00-10:00 | Keynote: Takayuki Sasaki**, ***The Great Hanshin-Awaji Earthquake***, Vice Chairman and Representative Director, JR West, JP		
10:30-11:00	**Networking Break – 3F Genji Waiting Room and 5F Taketori + Foyer**		
11:00-12:00	**Track I: Technical** **5F Kokin Naka**	**Track II: Management** **3F Genji West & North**	**Track III: Incident Response** **5F Kokin North**
11:00-11:30	*In the Cloud Security* Greg Day McAfee, UK	*More of What Hackers Don't Want You to Know* Jeff Crume IBM, US	*To be or not to be–An Incident Recovery Case Study* Chunyan "Sherman" Xie National University of Singapore, SG
11:30-12:00	*In the Cloud Security* (continued)	*More of What Hackers Don't Want You to Know* (continued)	*To be or not to be–An Incident Recovery Case Study* (continued)
12:00-13:30	**Lunch – 3F Genji South & 5F Taketori**		
13:30-15:00	**Track I: Technical** **5F Kokin Naka**	**Track II: Management** **3F Genji West & North**	**Track III: Incident Response** **5F Kokin North**
13:30-14:00	*Chinese Hacker Community and Culture, Underground Malware Industry* Wei Zhao KnownSec, PRC	*Closing the Gap between Policy Creation and Enforcement* Sven Bruelisauer Open Systems AG, CH	*The Threat of Banking Trojans: Detection Forensics and Response (Insights from a Bank CSIRT)* Marc Vilanova e-la Caixa CSIRT, ES
14:00-14:30	*Chinese Hacker Community and Culture, Underground Malware Industry* (continued)	*The Incident Response and the Law Enforcement* Yoshio Yamada National Police Agency of Japan, JP	*Analysis of the DDoS Attacks on Georgia & Estonia* Toomas Lepik CERT-EE, EE David Tabatadze CERT-GE, GE
14:30-15:00	*FIRST Business Plan* Peter Allor IBM, US	*Contradictions in Current European Security Policy* Dr. Jan K. Koecher DFN-CERT Services GmbH	*CSIRT Modeling Architecture* Yoshida Takahiko NTT, JP
15:15-18:30	**Annual General Meeting (AGM) – 3F Genji West & North – Members Only** **Members must have a valid government issued photo ID in order to enter the AGM. No exceptions.		

Notes

Friday, July 3

08:00-16:30	**Registration – 3F Genji Waiting Room**		
08:45-10:30	**Conference Opening – 3F Genji West & North** **08:45-09:00 | Opening Remarks: Derrick Scholl**, Chair, FIRST, US **09:00-10:30 | Keynote: Ray Stanton**, ***Security and the Future Generation***, Global Head, Business Continuity, Security and Governance Practice, BT, UK		
10:30-11:00	**Networking Break – 3F Genji Waiting Room & Kokin South**		
11:00-12:00	**Track I: Technical** **5F Kokin North**	**Track II: Management** **3F Genji West & North**	**Track III: Incident Response** **5F Kokin Naka**
11:00-11:30	*Update on Carrier Infrastructure Security Attacks* Jose Nazario Arbor Networks, US	*Show Me The Evil–A Graphical Look at Online Crime* Dave Deitrich Team Cymru, US	*ICASI Update* Peter Allor IBM, US
11:30-12:00	*Update on Carrier Infrastructure Security Attacks* (continued)	*Show Me The Evil–A Graphical Look at Online Crime* (continued)	*Internet Analysis System (IAS) -–Module of the German IT Early Warning System* Martin Bierwirth Andre Vorbach Federal Office for Information Security (BSI, Germany), DE
12:00-13:30	**Lunch – 3F Genji South & East**		
13:30-14:30	**Track I: Technical** **5F Kokin Naka**	**Track II: Management** **3F Genji West & North**	**Track III: Incident Response** **5F Kokin Naka**
13:30-14:00	*New Developments on Brazilian Phishing Malware* Jacomo Piccolini ESR/RNP, BR	*The Essential Role of the CSIRT in Secure Software Development* Kenneth Van Wyk KRvW Associates, LLC, US	*Anti-bot Countermeasures in Japan* Chris Horsley Takashi Manabe JPCERT/CC, JP
14:00-14:30	*New Developments on Brazilian Phishing Malware* (continued)	*The Essential Role of the CSIRT in Secure Software Development* (continued)	
14:30-15:00	**Closing Remarks – 3F Genji West & North** Derrick Scholl, Chair, FIRST, US		

Notes

PROGRAM COMMITTEE & STAFF

What Is FIRST?

FIRST is the Forum of Incident Response and Security Teams. The idea of FIRST goes back until 1989, only one year after the first CERT was created after the infamous Internet worm. Back then incidents already were impacting not only one closed user group or organization, but any number of networks interconnected by the Internet.

It was clear from then on that information exchange and cooperation on issues of mutual interest like new vulnerabilities or wide ranging attacks - especially on core system like the DNS servers or the Internet as a critical infrastructure itself - were the key issues for security and incident response teams.

Since 1990, when FIRST was founded, its members have resolved an almost continuous stream of security-related attacks and incidents including handling thousands of security vulnerabilities affecting nearly all of the millions of computer systems and networks throughout the world connected by the ever growing Internet.

FIRST brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors.

Vision

FIRST is a premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents by providing access to best practices, tools, and trusted communication with member teams.

Mission Statement

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

Interested in Joining?

Please leave your business card or e-mail address and phone number at the 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.

2009 Program Chair

Mick Creane	BT

2009 Program Committee

Jeff Boerio	Intel
Ranil Dassanayaka	HP Consulting
Gert Florijn	ABN Amro
Miroslaw Maj	NASK/CERT Polska
Mark-David McLaughlin	Cisco Systems
Reneaué Railton	Cisco Systems
Jon Ramsey	SecureWorks
Gavin Reid	Cisco Systems
Bharat Thakrar	BT
Marco Thorbruegge	ENISA
Yonglin Zhou	CNCERT/CC
Belhassen Zouari	ANSI

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

Corporate Executive Programme (CEP)

In June 2005, the Board and membership of FIRST agreed to fund and establish a unique Corporate Executive Programme (CEP).

Security issues reach far beyond IT to impact an entire organization: Marketing, Sales, Human Resources, Finance, Logistics and more. The Corporate Executive Programme is the ONLY forum to unite cross-functional senior executives from across all business lines, including public and private sectors, to address enterprise-wide risk strategically, openly and condifentially. CEP membership has grown to include top level executives from the world's largest organizations including among others, Intel, HSBC, EADS, Diageo and Mitsubishi UFJ.

For more information, visit: *http://www.globalcep.com.*

FIRST Symposia

One of the benefits FIRST offers to its members is a series of regional technical programs. These are three-day programs - two days of presentations and one day of small "hands-on" breakout sessions. In conjunction with these programs, FIRST provides meeting opportunities for Special Interest Groups (SIGs) and the Steering Committee. In some locations FIRST may conduct a joint program with regional CSIRTs.

For more information, visit: *http://www.first.org.*

FIRST Technical Colloquia (TC)

FIRST Technical Colloquia provide a discussion form for FIRST member teams to share information about vulnerabilities, incidents, tools and all other issues that affect the operation of incident response and security teams. These colloquia are hosted by members and take place 2-3 times a year.

For more information, visit: *http://www.first.org.*

FIRST Train the Trainers Workshop (T3)

Thanks to the TRANSITS (Training of Network Security Incident Teams Staff) project, FIRST has been successfully running the Train the Trainers workshop. The T3 workshop consists of two full-day training sessions in CSIRT issues for potential instructors of TRANSITS. The purpose of the workshop is to provide the TRANSITS material to potential trainers in these areas, help them to familiarize with the contents, and give them the tools to deliver the training course themselves in their region.

For more information, visit: *http://www.first.org.*

What would you like FIRST to address?

Are we covering all the areas that you believe we should be? Are there any areas or subjects that you believe FIRST as an organization should be addressing?

Let us know at first-sec@first.org!

Acessing Conference Presentations

1.) Navigate to: https://reg.first.org/papers.
2.) Login with the following credentials:

Username:	attendee
Password:	FIRST

Presentations are sorted by speaker last name. Locate the speaker and presentation you would like to download, right-click on the PDF icon* and save to file.

*If there is no PDF icon available, the presenter has either no slide deck, or has not yet made their presentation available.

All final presentations will be collected following conference close and will be available to download on the Member side of www.first.org. If you are unable to locate a presentation, please feel free to send mail to first-2009@first.org.

Lost & Found

If you see items laying around, please bring them to the registration desk.

The conference staff will hold lost items until the conference close on Friday, July 3rd. Items that have not been claimed will be discarded or donated.

21st Annual FIRST Conference
KYOTO June 28-July 3, 2009

Conference Policies

Please note the following policies will be in effect during the conference. We ask for your compliance with 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 his/her 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 Phones & Photography

A reminder to kindly turn off or silence mobile phones during the presentations and sessions. Also, picture taking is not allowed at the FIRST conference. If the policy is violated, the offender will be issued a warning. Any second offense may result in dismissal (non-refundable) from the conference.

Streaming

Attendees are prohibited from making audio or video recordings of any conference event or of attendees during the conference without the express written consent of the FIRST Steering Committee who will coordinate with any parties being recorded.

This year, FIRST will be streaming certain presentations with the advance approval of the presenters. All recordings will be available to FIRST members by the end of July 2009 via the FIRST website (certificate required). A select number of keynote recordings or portions of a recording may be available to the public. Recordings for FIRST membership only may not be distributed or shared among non-Team members of FIRST. However, FIRST will develop 5-10 minute approved recordings for recruitment and public relations purposes only. If you have any questions about the FIRST Information Sharing policy, please contact the Secretariat at first-sec@first.org.

FIRST
Improving Security Together

JUNE 13-18, 2010
INTERCONTINENTAL MIAMI
MIAMI, FLORIDA USA

PAST THE FADED PERIMETER

Threat & Incident Response

WWW.FIRST.ORG/CONFERENCE/2010

22nd ANNUAL
FIRST
CONFERENCE
MIAMI

JUNE 13-18, 2010

21st Annual FIRST Conference
KYOTO June 28-July 3, 2009

SPONSORED BY FIRST Improving Security Together

HOSTED BY JPCERT CC®

IN COOPERATION WITH BT

PLATINUM SPONSORS

CERT Software Engineering Institute Carnegie Mellon

FIRST Japan Teams

IPA® INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

GOLD SPONSORS

NRI SECURE TECHNOLOGIES

NTT

IIJ Internet Initiative Japan

Microsoft®

SUPPORTING SPONSORS

CISCO™

We are the future. NTT Smart Connect

OIPC ICPO INTERPOL

Sun microsystems®

Secunia Stay Secure

HITACHI

Google™

BFK edv-consulting GmbH www.bfk.de

O'REILLY®

netsecpodcast.com THE NETWORK SECURITY PODCAST

Event	**Law Enforcement Special Interest Group session on cyber security**
Date(s)	**29 June 2009**
Place	**Kyoto, Japan**

DRAFT PROGRAMME

SUNDAY, 28 JUNE 2009

Time	Agenda item	Subject	Speakers
19:00	Ice Breaker Reception – 3F Genji West & North – Sponsored by INTERPOL		

MONDAY, 29 JUNE 2009

Time	Agenda item	Subject	Speakers
08:45	Conference Opening – 3F GengiWest & North		
	08:45 to 09:00 | Opening remarks: Derrick Scholl, FIRST Chair, US 09:00 to 13:30 | Keynote: Suguru Yamaguchi, Information Security Management and Economic Crisis, Cabinet Office, Japan LE SIG participants are kindly invited to attend.		
10:30 to 11:00	Networking Break – 3F Genji Waiting Room and 5F Taketori + Foyer		
12:00	Lunch – 3F Genji West & North		
13:30	1	Opening/ Introduction	Chair
13:50	2	The technical assistance CERTs can provide to LE	Matthew McGlashan AuCERT
14:10	3	Presentation from FBI	Christopher Geary US Federal Bureau of Investigation
14:30	4	Crime in 2009 are focused on carding	Ryan Connelly Team Cymru
14:50	5	Cyber attacks against INTERPOL	Vincent Danjean, INTERPOL
15:10	6	Example of Technical Analysis	Yoichi Kumota NPA Japan
15:30	Networking Break – 3F Genji Waiting Room and 5F Taketori + Foyer		
15:50	7	Cybercrime and the Underground, an Industry Perspective	Ramses Martinez VeriSign
16:10	8	Recent observations on malicious hosting service providers	Kauto Huopio CERT-FI
16:30	9	Best practice - Evidence collection	Tom Mullen CISSP BT Group
16:50	10	CERT-Bund and the BSI	André Vorbach Federal Office for Information Security (BSI), CERT-Bund
17:10	11	General Discussion	ALL
17:30	Closing remarks - END		

Windows Memory Forensics with Volatility

- Important Information for Attendees -

Agenda

1. Refresher
   a. Why memory analysis?
   b. Memory acquisition primer
   c. Memory image file formats
   d. Concepts of virtual and physical memory
   e. Windows kernel objects
   f. Windows memory pools
   g. Object enumeration techniques
   h. Examination techniques
2. Volatility memory analysis framework
   a. Overview
   b. Architecture
   c. Using built-in commands
3. Programming Volatility
   a. Address spaces
   b. Objects
   c. Your first plugin
   d. Building blocks (common problems and solutions)

Who should attend?

The course addresses forensic examiners and incident responders who already know about the basics of Windows memory analysis and who have used tools like a kernel debugger, PTFinder and Volatility in the past.

The course builds on the classes held by Pär Österberg-Medina and Andreas Schuster at previous FIRST conferences. Attendees should be familiar with the literature (see “Recommended reading” below) and expect a steep learning curve.

The main part of the course will deal with the architecture of the Volatility memory analysis framework. A basic analysis and programming environment will be provided as a Linux virtual machine. Attendees should know how to navigate a UNIX shell (bash) and how to edit a text file. Also, attendees should know how to program and debug Python 2.6 scripts.

Recommended reading

- Pär Österberg-Medina: Detecting Intrusions - The latest forensics tools and techniques to identify Windows malware infections http://members.first.org/conference/2008/papers/medina-osterberg-par-slides.pdf
- Harlan Carvey: Windows Forensic Analysis, Chapter 3: Windows Memory Analysis. http://www.elsevierdirect.com/product.jsp?isbn=9781597491563
- Aquilina, Casey and Malin: Malware Forensics, Chapter 3: Analyzing Physical and Process Memory Dumps for Malware Artifacts. http://www.elsevierdirect.com/product.jsp?isbn=9781597492683
- Andreas Schuster: Searching for Processes and Threads in Microsoft Windows Memory Dumps. http://computer.forensikblog.de/files/talks/DFRWS2006-Searching_for-Processes_and_Threads.pdf
- Andreas Schuster: Pool Allocations as an Information Source in Windows Memory Forensics http://computer.forensikblog.de/files/talks/IMF2006-PoolAllocations-paper.pdf
- Mark Lutz: Python pocket reference. O'Reilly 2005 http://oreilly.com/catalog/9780596009403/
- Richard Gruet: Python Quick Reference. http://rgruet.free.fr/#QuickRef

Hardware/Software prerequisites

Attendees are expected to bring their own Laptop.

- Minimum hardware requirements:
  - CPU 1.5 GHz
  - 1 GB RAM
  - 6 GB of free disk space
  - DVD drive
- Software:
  - Either VMware Player (free) Version 6.5.2
    or VMWare Workstation 6.5.2 (commercial, 30days trial version available)
    from http://www.vmware.com/
  - Any archiver for your host OS that can unpack ZIP archives, e.g. file roller, WinZip

Don't forget to bring power adaptors, extension cords, an USB hub, OS and driver installation media, your latest backup and whatever else might be helpful in an impromptu work environment.

Contact

Don't hesitate to contact me; I welcome your suggestions and questions.

Andreas Schuster
a.schuster@yendor.net
http://computer.forensikblog.de/en/