Conference Program

Agenda last updated 10 June 2013. Please note that the program is subject to change.

Please note that some special interest groups are invite-only.

To view an abstract, please click on titles that have the [+] indication to expand. Speaker bios will be posted soon.

Print Version Available

Saturday, 15 June 2013

1000-1630 Education & Training Committee Meeting (Open to non-members)
London 1 - Level 1

Sunday, 16 June 2013

1000-1330 Education & Training Committee Meeting (Open to non-members)
London 1 - Level 1

1400-1800 Registration
Hong Kong - Level 2

1830-2000 Registration (During Reception)
Spa/Pool Level - Conrad Terrace Pool

1500-1600 2013 Session Chairs Meeting
Willow I - Level 3

1830-1900 Newbie Reception w/ FIRST Steering Committee & Membership Committee
Spa/Pool Level - Conrad Terrace Pool
FIRST Newbies (non-members) & First Time Attendees (members and non-members) are cordially invited to mix and mingle with each other and the FIRST Steering Committee & Member Committee. Beverages and appetizers will be served - find all the unique food & beverage stations spread out alongside the pool and walking paths!

1900-2100 Ice Breaker Reception sponsored by Solera Networks
Spa/Pool Level - Conrad Terrace Pool
All attendees are encouraged to attend this kick-off networking event.

Monday, 17 June 2013

0730-1700 Registration
Hong Kong - Level 2

0730-0900 CVSS v3 Special Interest Group (SIG) - click here for details.
London 1 - Level 1 | Invite-only

0730-0830 Morning Coffee & Tea Service
Prefunction - Level 4
Breakfast is included in the Conrad Bangkok lodging rate in the hotel restaurant. This coffee & tea service is specifically for attendees not staying in the Conrad and who plan to arrive early.

0830-0900 Conference Opening & Welcome Remarks
Grand Ballroom - Level 4
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Location</th>
<th>Speakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>0900-0930</td>
<td>Opening Remarks by Her Excellency Ms. Yingluck Shinawatra</td>
<td>Grand Ballroom</td>
<td>Prime Minister of the Kingdom of Thailand</td>
</tr>
<tr>
<td>0930-1030</td>
<td>Keynote Presentation: INTERPOL Global Complex for Innovation--Facilitating international police cooperation to combat cybercrime</td>
<td>Grand Ballroom</td>
<td>James Pang, Assistant Director for Digital Crime Investigation Support, INTERPOL</td>
</tr>
<tr>
<td>1030-1100</td>
<td>Coffee &amp; Networking Break</td>
<td>Prefunction</td>
<td></td>
</tr>
<tr>
<td>1100-1200</td>
<td>Plenary: Big Data, Big Breaches, Big Headaches</td>
<td>Grand Ballroom</td>
<td>Scott McIntyre, Senior Technology Architecture Specialist, Telstra, AU</td>
</tr>
<tr>
<td>1200-1330</td>
<td>Lunch (2 locations)</td>
<td>Cafe @2 - Level 2</td>
<td>Kisaara Restaurant - Level 3</td>
</tr>
<tr>
<td>1335-1420</td>
<td>Chasing the Fox: A closer look at an APT malware</td>
<td>Grand Ballroom</td>
<td>Andreas Schuster, Deutsche Telekom AG</td>
</tr>
<tr>
<td>1425-1510</td>
<td>Proactive Forensics of Web Application Attacks—A Step by Step Guide</td>
<td>Grand Ballroom</td>
<td>Shlomi Ben-Hur, Shay Chen, Hacktics ASC, Ernst &amp; Young, LLP, IL</td>
</tr>
<tr>
<td>1510-1545</td>
<td>Coffee &amp; Networking Break</td>
<td>Prefunction</td>
<td></td>
</tr>
<tr>
<td>1640-1725</td>
<td>Mining Billion Nodes Malicious Network Behavior in Practice—Chinese Taipei Perspective</td>
<td>Grand Ballroom</td>
<td>Ching-Hao Mao, Institute for Information Industry, TPE</td>
</tr>
<tr>
<td>1730-1830</td>
<td>Lightning Talks - Day 1</td>
<td>Grand Ballroom</td>
<td></td>
</tr>
</tbody>
</table>

**Tuesday, 18 June 2013**

**QUESTIONS?**

Do you have specific questions? Please send inquiries to first-2013@first.org.

Direct line to conference office: +1 312 646 1013

Direct mailing address to conference office: FIRST Conference Office 219 W. Chicago Avenue, Suite 300 Chicago, Illinois 60654

**CONNECT WITH US**

- FIRST News!
- FIRST Podcasts!
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>0730-1700</td>
<td>Registration</td>
<td>Hong Kong - Level 2</td>
</tr>
<tr>
<td>0730-0900</td>
<td>CVSS v3 Special Interest Group (SIG) - [click here for details.]</td>
<td>London 1 - Level 1</td>
</tr>
<tr>
<td>0800-0900</td>
<td>Morning Coffee &amp; Tea Service</td>
<td>Prefunction - Level 4</td>
</tr>
<tr>
<td>0900-0930</td>
<td>Opening Remarks</td>
<td>Grand Ballroom - Level 4</td>
</tr>
<tr>
<td>0930-1030</td>
<td>Keynote: Economic Products and By-products of Open, Shared, Real Time Sinkholes--Lessons From GhostClick and Conficker [*]</td>
<td>Grand Ballroom - Level 4</td>
</tr>
<tr>
<td>1030-1100</td>
<td>Coffee &amp; Networking Break</td>
<td>Prefunction - Level 4</td>
</tr>
<tr>
<td>1100-1200</td>
<td>FIRST Session: FIRST Financials Review</td>
<td>Grand Ballroom - Level 4</td>
</tr>
<tr>
<td>1200-1340</td>
<td>FIRST Breakout</td>
<td>Prefunction - Level 4 and 2</td>
</tr>
<tr>
<td>1335-1420</td>
<td>Virut Botnet Takedown [*]</td>
<td>Grand Ballroom 1&amp;2 - Level 4</td>
</tr>
<tr>
<td>1425-1510</td>
<td>BlackHole, the hidden stuff beyond the spotlight [*]</td>
<td>Beverly Hills Ballroom - Level 2</td>
</tr>
<tr>
<td>1500-1700</td>
<td>Net Infrastructure BoF (open)</td>
<td>London 1 - Level 1</td>
</tr>
<tr>
<td>1515-1545</td>
<td>Coffee &amp; Networking Break</td>
<td>Prefunction - Level 4 and 2</td>
</tr>
<tr>
<td>1550-1635</td>
<td>Nfsen + Hadoop [*]</td>
<td>Grand Ballroom 1&amp;2 - Level 4</td>
</tr>
<tr>
<td>1640-1725</td>
<td>Analysis of DNS data from Chinese Telecom Operators [*]</td>
<td>Beverly Hills Ballroom - Level 2</td>
</tr>
<tr>
<td>1730-1800</td>
<td>Lightning Talks - Day 2</td>
<td>Grand Ballroom 1&amp;2 - Level 4</td>
</tr>
<tr>
<td>1730-1900</td>
<td>CVSS v3 Training BoF (open)</td>
<td>Beverly Hills Ballroom - Level 2</td>
</tr>
</tbody>
</table>

**Breakouts**

**Deep Technical Dives**

- **Grand Ballroom 1&2 - Level 4**
  - Virut Botnet Takedown [*]
  - BlackHole, the hidden stuff beyond the spotlight [*]

**Technical Foundations**

- **New York Ballroom - Level 2**
  - Tracing Botnet in Chinese Taipei [*]
  - Lessons Learned in Automating Threat Intelligence Sharing with Open IOC [*]

**Policy & Management**

- **Beverly Hills Ballroom - Level 2**
  - Declared Level of Response as a Voluntary CERT Community Cooperation Model in Incident Handling [*]
  - CERT Certification - A certification scheme for CERTs/CSIRTs using the SIM3 maturity model [*]

**Special Interest Groups (SIG)**

- **CVSS v3 Training BoF (open)**

**Sign-up**

- **Registration**
  - Hong Kong - Level 2
  - Database with details about the conference.
Wednesday, 19 June 2013

0800-1400  Registration  Hong Kong - Level 2

0800-0900  CVSS v3 Conference Update  Grand Ballroom - Level 4 | Open to All Attendees

Seth Hanford  Cisco Systems, US

0800-0900  Morning Coffee & Tea Service  Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4

Breakfast is included in the Conrad Bangkok lodging rate in the hotel restaurant. This coffee & tea service is specifically for attendees not staying in the Conrad and who plan to arrive early.

0800-0945  Deep Technical Dives

Detecting Malware infections through DNS live monitoring [*]

Hector Ortiz  Swisscomm, CH

0900-0945  Technical Foundations

Winning the Game with the Right Playbook [*]

Jeff Bollinger
Brandon Enright
Matthew Valites  Cisco Systems, US

0950-1035  Incubations: Cyber Espionage Operators and Their Tools [*]

Brandon Dixon  Verisign, US

1000-1045  Policy & Management

When security incidents drive an incumbent ISP to change its security strategy 180 degrees [*]

Martijn van der Heide  KPN-CERT, NL

1040-1140  Re-writing the CSIRT Playbook BoF  London 1 - Level 1

1040-1110  Coffee & Networking Break with Exhibits  Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4

1115-1205  Breakouts

Journeys Through Unallocated Space [*]

Timothy Slaybaugh  General Dynamics - AIS, US

1200-1330  Lunch (2 locations)  Cafe @2 - Level 2

Liu Restaurant - Level 3

1300-1600  Special Interest Group (SIG) - click here for details.  London 1 - Level 1

1300-1600  Vendor Special Interest Group (SIG) - click here for details.  London 1 - Level 1

1335-1420  Deep Technical Dives

Zeus Gameover - P2P Spyware at Work [*]

Tomasz Bukowski  NASK/CERT Polska, PL

1425-1510  Technical Foundations

The Case for NetFlow for Law Enforcement [*]

Richard Nolan
Kristopher Rush  SEI, CERT/CC, US

1510-1530  Coffee & Networking Break  Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4

1600-1630  Vendor Special Interest Group (SIG) - click here for details.  London 1 - Level 1

1630-2200  Conference Reception & Banquet Dinner  Location & event details will be announced onsite!
### THURSDAY, 20 JUNE 2013

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0800-1600</td>
<td><strong>Registration</strong>&lt;br&gt;Hong Kong - Level 2</td>
</tr>
<tr>
<td>0800-0900</td>
<td><strong>Morning Coffee &amp; Tea Service</strong>&lt;br&gt;Grand Ballroom Prefunction &amp; Grand Ballroom 3 - Level 4</td>
</tr>
<tr>
<td></td>
<td>Breakfast is included in the Conrad Bangkok lodging rate in the hotel restaurant. This coffee &amp; tea service is specifically for attendees not staying in the Conrad and who plan to arrive early.</td>
</tr>
</tbody>
</table>

**BREAKOUTS**

<table>
<thead>
<tr>
<th>Time</th>
<th>Session Type</th>
<th>Room</th>
<th>Speakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>0900-0945</td>
<td><strong>Conducting Technical Incident Investigations on Apple iOS Devices [*]</strong></td>
<td>Grand Ballroom 1 &amp; 2 - Level 4</td>
<td>Kenneth van Wyk&lt;br&gt;KRVW Associates, LLC, US&lt;br&gt;Snorre Fagerland&lt;br&gt;Norman AS, NO</td>
</tr>
<tr>
<td>0950-1035</td>
<td><strong>Monitoring DDoS Botnets in the Wild to Understand Behavior and Collect Intel [*]</strong></td>
<td>Grand Ballroom 1 &amp; 2 - Level 4</td>
<td>Shahan Sudusinghe&lt;br&gt;Verisign, US&lt;br&gt;Yusuke Gunji&lt;br&gt;Rakuten, Inc, JP</td>
</tr>
<tr>
<td>1040-1110</td>
<td><strong>Coffee &amp; Networking Break with Exhibits</strong>&lt;br&gt;Grand Ballroom Prefunction &amp; Grand Ballroom 3 - Level 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1115-1205</td>
<td><strong>A Sampling of Internetwork Security Issues Involving IPv6 [*]</strong></td>
<td>Grand Ballroom 1 &amp; 2 - Level 4</td>
<td>John Kristoff&lt;br&gt;Team Cymru, US&lt;br&gt;Arturo Servin&lt;br&gt;LACNIC, UY</td>
</tr>
<tr>
<td>1210-1330</td>
<td><strong>Lunch (2 locations)</strong></td>
<td>Café @2 - Level 2&lt;br&gt;Kisara Restaurant - Level 3</td>
<td></td>
</tr>
<tr>
<td>1335-1420</td>
<td><strong>Malware Analysis Case Study [*]</strong></td>
<td>Grand Ballroom 1 &amp; 2 - Level 4</td>
<td>Yuii Kubo&lt;br&gt;Teiichi Torikai&lt;br&gt;National Police Agency, JP&lt;br&gt;Fath Halats&lt;br&gt;Center for Interdisciplinary Studies in Security and Privacy New York University Abu Dhabi, TR</td>
</tr>
<tr>
<td>1425-1510</td>
<td><strong>Intelligent Defence: deriving malicious intent using domain registrar information [*]</strong></td>
<td>Grand Ballroom 1 &amp; 2 - Level 4</td>
<td>Michael Jordon&lt;br&gt;Context, UK&lt;br&gt;The Mayans were right! A new age of data breaches [*]**</td>
</tr>
<tr>
<td>1515-1600</td>
<td><strong>Coffee &amp; Networking Break with Exhibits</strong>&lt;br&gt;Grand Ballroom Prefunction &amp; Grand Ballroom 3 - Level 4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Friday, 21 June 2013**

<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0800-1400</td>
<td><strong>Registration</strong>&lt;br&gt;Hong Kong - Level 2</td>
</tr>
<tr>
<td>0800-0900</td>
<td><strong>Morning Coffee &amp; Tea Service</strong>&lt;br&gt;Grand Ballroom 1 &amp; 2 - Level 4</td>
</tr>
</tbody>
</table>

---

**AGM Registration will be located outside of the doors.**

Members-only meeting. Please be on time and have a valid government issued photo ID for entry into meeting room. No exception. Coffee break for members will be served in the meeting room.
## Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4

Breakfast is included in the Conrad Bangkok lodging rate in the hotel restaurant. This coffee & tea service is specifically for attendees not staying in the Conrad and who plan to arrive early.

### 0830-0900 Opening Remarks

**Grand Ballroom - Level 4**

**Chris Gibson**  
Chair, FIRST.Org  
Director, Citi, UK

### BREAKOUTS

#### DEEP TECHNICAL DIVES

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Venue</th>
<th>Speakers</th>
</tr>
</thead>
</table>
| 0900-0945 | Memory Analysis Update - Volatility v2.3 [*] | Grand Ballroom 1&2 - Level 4 | Andreas Schuster  
Deutsche Telekom, AG |
| 0950-1035 | Memory Analysis Update | Grand Ballroom 1&2 - Level 4 | Pavel Kácha  
CESNET, CZ |

#### TECHNICAL FOUNDATIONS

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Venue</th>
<th>Speakers</th>
</tr>
</thead>
</table>
| 0900-0945 | Sharing by Wim [*] | New York Ballroom - Level 2 | Willem Biemolt  
SURFnet/SURFoer, NL |
| 0950-1035 | WARDEN: realtime sharing of detected threats between CSIRT teams [*] | Beverly Hills Ballroom - Level 2 | Michael Lotas  
General Dynamics Fidelis Cybersecurity Solutions, US |

#### POLICY & MANAGEMENT

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Venue</th>
<th>Speakers</th>
</tr>
</thead>
</table>
| 0900-0945 | A Glimpse Into the Future: The Evolution of Cybercrime in the Next Decade [*] | Beverly Hills Ballroom - Level 2 | Ziv Mador  
Trustwave, US |
| 0950-1035 | The Art of Cyber Warfare [*] | Beverly Hills Ballroom - Level 2 | Bisyron Wahyudi  
ID-SIRTII, ID |

#### 1000-1110 Coffee & Networking Break with Exhibits

**Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4**

#### 1115-1205 Improving Cybersecurity Capabilities of Critical Infrastructures - Findings in Assessing ICS [*]

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Venue</th>
<th>Speakers</th>
</tr>
</thead>
</table>
| 1115-1205 | Improving Cybersecurity Capabilities of Critical Infrastructures - Findings in Assessing ICS [*] | New York Ballroom - Level 2 | Lauri Korts-Pärn  
Masako Someya  
Cyber Defense Institute, Inc., JP |
| 1115-1205 | National CSIRT Community to Protect Key Strategic Resources and Critical Information Infrastructures [*] | Beverly Hills Ballroom - Level 2 | Bisyron Wahyudi  
ID-SIRTII, ID |

### 1210-1330 Lunch (2 locations)

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Venue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1210-1330</td>
<td>Lunch (2 locations)</td>
<td>Cafe @2 - Level 2, Diplomat Bar - Lobby Level</td>
</tr>
</tbody>
</table>

### 1335-1400 Closing Remarks, Security Challenge Winners & Raffles

**Grand Ballroom 1&2 - Level 4**

### 1300-1430 Closing Coffee & Networking Break

**Grand Ballroom Prefunction & Grand Ballroom 3 - Level 4**

---

© 2012-2013 FIRST.Org, Inc. Questions? Please contact us at first-2013@first.org

Press Policy | Network Privacy Statement & Conference Monitoring | FIRST Board of Directors | Contact the FIRST Secretariat

Site powered by CAPS, LLC