Internet characterization through measurements

Steve Rich (srich@cisco.com)
Robert Broberg (rbroberg@cisco.com)
October 31, 2015
The Internet is going dark….  

• Soon to be ubiquitous encryption
• Malware detection and privacy
  • We want privacy
  • We don’t want theft or malicious behaviour
• Entropy
  • What does that mean for data transfer?
• Is there true entropy with current encryption?
  • Weak pnrng?
  • Can we determine ciphers?
  • Traffic analysis
  • Nx40G?
Cisco’s Advanced Security Research Group (ASRG)

- Security Research targeting issues 5, 10, 15 years out…..and 1, 3, 5
- Establishing programs in U.S, Europe and Asia
- Target Research institutes for multiplicative impact factor (pooling/collaboration)
- Engage universities/institutes/governments for joint research with impact
  - Cisco assigned liaison
  - Quarterly reviews to help guide academic research to relevant issues
  - Up to ~$250k target funding for ~1 to ~3 year program
  - Internships to allow for collaboration with real data
  - Strong publications and dissemination of research results are metrics for success
Areas of interest

- Advanced Cryptography
- Platform & Software Integrity
- Analytics and Privacy
- Threat Mitigation
- Integrated Circuit / Hardware Integrity; Design & Fabrication
<table>
<thead>
<tr>
<th>University</th>
<th>Lead PI</th>
<th>Title</th>
<th>Focus Area</th>
<th>ASRG RM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wake Forest</td>
<td>Errin Fulp</td>
<td>Evolutionary Cyber Defense for Resilient Computer Infrastructures</td>
<td>Threat Mitigation</td>
<td>Roger</td>
</tr>
<tr>
<td>Univ of PA</td>
<td>Nadia Heninger</td>
<td>Security Protocol Analysis Cluster Engineering</td>
<td>Analytics</td>
<td>Robert</td>
</tr>
<tr>
<td>Univ of Waterloo</td>
<td>Mark Aagaard</td>
<td>Fundamental Technologies for Ultralightweight Hardware Security Modules</td>
<td>Integrity</td>
<td>Roger</td>
</tr>
<tr>
<td>Indiana Univ</td>
<td>Jean Camp</td>
<td>The Trust Challenge of BGP</td>
<td>Integrity</td>
<td>Steve</td>
</tr>
<tr>
<td>Univ of Delaware</td>
<td>Chase Cotton</td>
<td>Threat Detection using Distributed Machine Learning and Shared Indicators of Compromise</td>
<td>Integrity</td>
<td>Robert</td>
</tr>
<tr>
<td>UC Berkeley</td>
<td>David Wagner</td>
<td>Secure Computing for Cloud and Enterprise: Machine Learning, Analytics, and Authentication</td>
<td>Analytics</td>
<td>Steve</td>
</tr>
<tr>
<td>INRIA</td>
<td>Mathieu Cunche</td>
<td>Privacy Preserving Mechanisms for Radio Based Location Analytics</td>
<td>Privacy</td>
<td>Steve</td>
</tr>
<tr>
<td>Virginia Tech</td>
<td>Patrick Schaumont</td>
<td>Remote Device Integrity by Physical Proofs</td>
<td>Integrity</td>
<td>Chris</td>
</tr>
</tbody>
</table>
Current solicitations for ASRG programs:

- **Integrity:**
  - [http://research.cisco.com/research-programs.html#rfp-2015092](http://research.cisco.com/research-programs.html#rfp-2015092)

- **Threat Mitigation:**
  - [http://research.cisco.com/research-programs.html#rfp-2015093](http://research.cisco.com/research-programs.html#rfp-2015093)

- **Anonymity and Privacy:**
  - [http://research.cisco.com/research-programs.html#rfp-2015094](http://research.cisco.com/research-programs.html#rfp-2015094)

- **Threat Defense and Distributed Computation and Trusted Computing**
  - [http://research.cisco.com/research-programs.html#rfp-2013081](http://research.cisco.com/research-programs.html#rfp-2013081)

- **Integrated Circuit / Hardware Integrity; Design & Fabrication**
  - [http://research.cisco.com/research-programs.html#rfp-2015095](http://research.cisco.com/research-programs.html#rfp-2015095)
Thank you.