DFRWS Forensics Challenge 2016

Michael McCarrin
Brian Greunke
Robert Beverly
Naval Postgraduate School
Rich History of Offering Timely Forensics Challenges to the Community...

<table>
<thead>
<tr>
<th>Year</th>
<th>Challenge</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>GPU Malware</td>
</tr>
<tr>
<td>2014</td>
<td>Mobile Malware</td>
</tr>
<tr>
<td>2013</td>
<td>Block Classifier</td>
</tr>
<tr>
<td>2012</td>
<td>Block Classifier</td>
</tr>
<tr>
<td>2011</td>
<td>Android Forensics</td>
</tr>
<tr>
<td>2010</td>
<td>Flash Memory Forensics</td>
</tr>
<tr>
<td>2009</td>
<td>Playstation Forensics</td>
</tr>
<tr>
<td>2008</td>
<td>Linux Memory Analysis</td>
</tr>
</tbody>
</table>

Thanks, Golden!
Forensics Challenge Goals

• Advance research in new and emerging areas of digital forensics
• Spur development of new (open) tools and techniques
• Emulate scenarios of forensic interest
• Engender cooperation within groups and competition between groups
Emerging Area: SDN

• Software Defined Networks (SDNs):
  – Move away from proprietary network operating systems (Cisco IOS, JunOS, etc)
  – Standards-based protocol (OpenFlow) and commodity hardware
  – Centralized controller, programmable network switches

• Promise:
  – Lower-costs
  – Multi-vendor
  – Enable innovation within network
State of SDN

• Implementations:
  – Software (e.g., Open vSwitch)
  – Hardware from all major vendors (HP, Cisco, etc), startups
  – Open software controllers (e.g., Pox, Nox, Floodlight, etc)

• Deployments:
  – Google (“OpenFlow has helped us improve backbone performance and reduce backbone complexity and cost”)
  – Amazon
  – Universities and enterprises
State of SDN

• Implementations:
  – Software (e.g., Open vSwitch)
  – Hardware from all major vendors (HP, Cisco, etc), startups
  – Open software controllers (e.g., Pox, Nox, Floodlight, etc)

• Deployments:
  – Google (“OpenFlow has helped us improve backbone performance and reduce backbone complexity and cost”)
  – Amazon
  – Universities and enterprises

Moral: SDNs are timely and relevant
2016 Challenge: SDN Forensics

- Only nascent work on SDN security
- No work on SDN forensics
- Let’s change that!
2016 Challenge: SDN Forensics

• *Potential* scenarios of interest:
  – Evidence of residual traffic flows on switch hardware
  – Investigate faults in SDN networks
  – Find attacks against controllers within network traffic
  – Reverse-engineer network and activity by observing traffic between controller and switch

• *Potential* data sources:
  – Traffic to/from controller
  – Switch memory dumps
  – Controller memory dumps
2016 Challenge: SDN Forensics

• We’re in the early stages of developing the 2016 challenge
• We welcome early feedback and input!
• Hope you’ll join us in 2016!
• Feedback / flames:

sdn-forensics@cmdand.org