DFRWS Forensics Challenge 2016

Michael McCarrin
Brian Greunke
Robert Beverly
Naval Postgraduate School

DFRWS
DIGITAL FORENSIC RESEARCH WORKSHOP

Rich History of Offering Timely Forensics Challenges to the Community…

Year	Challenge
2015	GPU Malware
2014	Mobile Malware
2013	Block Classifier
2012	Block Classifier
2011	Android Forensics
2010	Flash Memory Forensics
2009	Playstation Forensics
2008	Linux Memory Analysis

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@cmand.org

DFRWS
DIGITAL FORENSIC RESEARCH WORKSHOP