Future of IDS

Considerations for keeping up with increasing network growth.
Bio

Harry Hoffman
Director, Security & Resilience
Massachusetts Institute of Technology
Current Networks and Instrumentation
Drawbacks
From 1G to 100GB...
Challenges
Scaling up
Virtual Infrastructures
Dealing with the “Cloud"
High Speed Deployments
*Enterprise Management Associates, Oct 2013
Network Growth - Predictions

100G will account for over half of all bandwidth deployed in carrier networks in 2014, growing rapidly through 2018.

- 10G
- 40G
- 100G

Transmission Capacity in Petabits per Second

Future of IDS - Harry Hoffman
Network Growth - Sales

40GbE/100GbE Transceiver Sales

Source: LightCounting

Future of IDS - Harry Hoffman
Questions

* How many of you have 10G core networks?

* How many have 10G interconnects to external providers (Internet2, Amazon, etc.)?

* Multiple Internet connections for redundancy?
Current Network Architecture
Simple SPAN port
R(emote) SPAN port
Challenges

* Potential oversubscription
* Delays in data and timing
* Bad packets not forwarded
* Resources consumption
Growing beyond SPAN ports
100G Considerations

- **Cost**
  - Sensor hardware
  - Network gear expense
  - Tap/aggregation products
  - 2x optics on each side
- **Bursting traffic**
- **Resource exhaustion**
  - Loss at writing alerts/logs
100G Considerations

* No Single Product to handle 100G (or 40G)
* Vendor Products
  * RSA Security Analytics – 10G
  * Cisco Sourcefire – 40G
  * Fireeye – 10G
  * Broala – 10G (ETA?)
Challenges

* Capture all the packets
* Write them somewhere (at least temporarily)
* Analyze the stream
* Understand the protocols and applications
* Process in a timely manner
* Encryption
* IPv6 (sigh...)
Capture Points

* Network
* Host
* Virtual Infrastructure
* Cloud
* Export from network gear
Ensure you see everything!

“What!? ONLY PACKET STEERED TO US ARE BELONG TO US?”

BRAD HEDLUND .com
Capture all the Packets

1Gbps – per/hour per/day

TOTAL: 450,0 GB
BYTES: 450000000000

Compare the filesize/throughput to common sizes:

TOTAL: 10,8 TB
BYTES: 108000000000

Compare the filesize/throughput to common sizes:
High speed packet capture

- Requires use of purpose designed hardware
- Usually coupled with software
- Limited options
Products – Security Analytics
Products - Devices
Existing Solutions
Divide and conquer
Gigamon – Maps
Encryption Challenges

- Attack patterns may not show up in logs
- NAT addresses behind SSL load-balancers
- IPSs unable to act upon the data stream
Encryption - Passive

![Diagram showing encryption processes involving non-SSL, encrypted SSL, and decrypted SSL channels.](image URL)
Encryption - Inline
Network Flows
Flow Benefits

* Baseline Traffic per network
* Scalability
* OS Fingerprinting
* DDoS/Work/Botnet detection
* Data transfer analysis
  * By size
* Tie in user authentications (external systems)
Flow data

- Time
- Duration
- IP Addresses
- Protocols
- Ports
- TOS
- TTL
- Bytes
- Ethernet Addresses
- Tunnels (GRE, IP/IP, etc)
- IPv6
- NAT
- RTT
- Jitter
Supplemental Decision Making

- Bad actors
  - IP
  - ASN
  - Email
  - File Hashes

Future of IDS - Harry Hoffman
Distributed Threat Feeds

Future of IDS - Harry Hoffman
Virtual Environments
VMWare Instrumentation

Future of IDS - Harry Hoffman
Virtual Tapping

Future of IDS - Harry Hoffman
Cloud Environments
Virtual Private Cloud
Old higher-ed mantra...
Each host must be able to protect itself
**NEXT GENERATION ENDPOINT SECURITY**

**YESTERDAY**

- **‘DEDICATED EQUIPMENT’**
  - Example: either hardware or software deployed on premise

- **‘POINT SOLUTIONS’**
  - Example: AV, Micro-virtualization, Virtual detonation, HIPS, Whitelisting, etc.

- **INDICATOR-OF COMPROMISE**
  - Example: outdated profiles and artifacts of known exploits and vulnerabilities

- **‘POINT-IN-TIME’**
  - Example: retrospective approach reliant on scans & sweeps

**TODAY**

- **‘CLOUD’**
  - ✓✓

- **‘INTEGRATED SOLUTION’**
  - ✓✓

- **‘INDICATOR-OF-ATTACK’**
  - ✓✓

- **‘REAL-TIME’**
  - ✓✓

- **‘ATTRIBUTION & CONTEXT’**
  - ✓✓

**TODAY**

- **‘DEDICATED EQUIPMENT’**
  - Example: either hardware or software deployed on premise

- **‘POINT SOLUTIONS’**
  - Example: AV, Micro-virtualization, Virtual detonation, HIPS, Whitelisting, etc.

- **INDICATOR-OF COMPROMISE**
  - Example: outdated profiles and artifacts of known exploits and vulnerabilities

- **‘POINT-IN-TIME’**
  - Example: retrospective approach reliant on scans & sweeps

- **‘ATTRIBUTION & CONTEXT’**
  - Example: focused on malware & exploits

**TODAY**

- **‘CLOUD’**
  - ✓✓

- **‘INTEGRATED SOLUTION’**
  - ✓✓

- **‘INDICATOR-OF-ATTACK’**
  - ✓✓

- **‘REAL-TIME’**
  - ✓✓

- **‘ATTRIBUTION & CONTEXT’**
  - ✓✓
Endpoints - CrowdStrike
Products for Everything
Cisco ASA - FirePower
Virtual Tapping
SDV – Software Defined Visibility

Future of IDS - Harry Hoffman
What do you think is next?
Thank you...
Questions?