FloCon 2016
12th Annual Open Forum for Large-Scale Network Analytics

Merging Network Configuration and Network Traffic Data in ISP-Level Analyses

Timothy J. Shimeall, Ph.D.

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0003171

Overview

The Network Data Flood

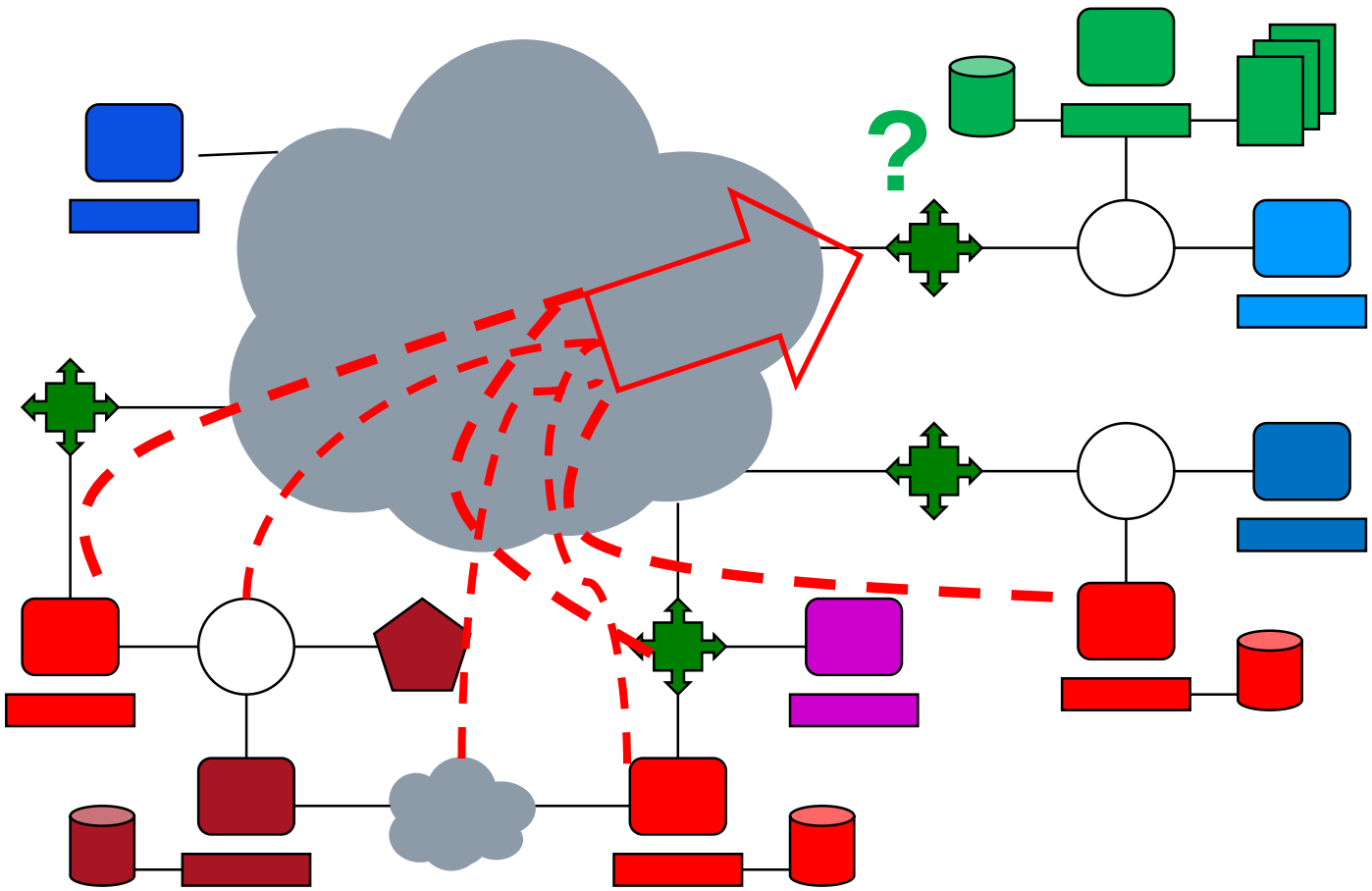
Analyst Needs

Merger Methods

Examples of Merger

Practical Tips

Network Data Flood



Network Configuration

- Host identification
- Host criticality
- Host configuration
- Vulnerability scan
- Vulnerability impact
- Subnet relations

Network Traffic

- Network Flows
- Packet captures
- Alerts
- Route information
- Address resolutions
- Service Logs

Analyst Needs

Network observation

- What behaviors are seen from hosts of configuration X?
- What configurations contribute to the volume of behavior Y?

Network orientation

- Which configurations have vulnerabilities scanned for during event Z?
- Which hosts are running the services exploited during event Z?

Network understanding

- How difficult is it to apply patch Q on this network?
- What issues would be involved in blocking service R on this network?

Network prediction

- What is likely to follow event Z due to our traffic and configuration?
- How likely are our customers to be affected by event Z?

Merger Methods

Config-first: Using configuration to drive network traffic analysis

Traffic-first: Using traffic to drive network configuration analysis

Deep-dive: Goals-Questions-Metrics

Sandwich: Iterate between traffic and configuration driving analysis

Examples of Merger

Assessing encryption

- Start with hosts configured as servers for encrypted services
- Filter packets/flows/logs for those servers to generate profiles
- Identify common users of services
- Filter for other network points of contact for those users
- Associate services and configuration associated with those points

Network attack impact

- Start with traffic indicators of attack
- Generate set of network hosts involved with indicators
- Associate services and configurations with hosts
- Filter for contacts
- Identify vulnerable configurations in contacts

Practical Tips

Watch for topology mismatches

Watch for NAT issues

Try the simple approach first

Generalize from working approaches

Do not try to solve the insolvable

Conclusion

Challenges

Methods exist

Don’t try to be too generic: you can extrapolate from what works

Need to take into account human and automated advantages

Contact Information

Timothy Shimeall

Senior Member of the Technical Staff

Telephone: +1 412.268.7611

Email: tjs@cert.org