Nfsight: Netflow-based Network Awareness

Michel Cukier (with R. Berthier (UIUC), M. Hiltunen (AT&T), D. Kormann (AT&T), and G. Vesonder (AT&T))

ISR @25 — The Institute for Systems Research — A. James Clark School of Engineering

Goals

- Gaining situational awareness on large networks:
  - What servers are deployed?
  - Are there rogue services?
- Visualizing network traffic at various granularities

Contributions

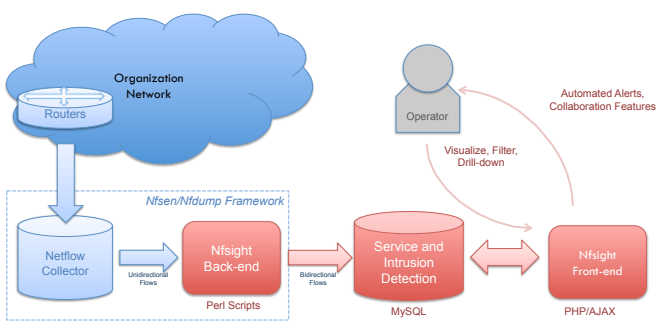
- Netflow-based client/server detection
  - Heuristics and Bayesian inference are used to generate bidirectional flows from Netflow
- Lightweight and easy to deploy
  - Back-end as plugin for Nfsen/ Nfdump
  - Web-based front-end developed in PHP and Javascript
- Anomaly detection and automated alerts

Intrusion Detection

- Nfsight enables operators to write anomaly detection signatures and be alerted by email
- Signatures are based on data fields from graphlet structures stored for each IP

Detect TCP Scanning Behavior	Protocol == TCP AND unique_dst_IP > 100 AND #failed_connections > 80

Architecture



Dr. Cukier's Research

- Goal: quantification of computer security
- Empirical studies using all security related data collected on the UMD network
- Research projects examples:
  - Profiling attacker behavior following SSH compromises
  - Analyzing Intrusion Prevention System Event Data
  - Honeypot Architecture for Network Threats Quantification
- PI of NSF REU Site on computer security (collaboration with Women in Engineering)
- Funded by NSF, DARPA, AT&T, Raytheon

Client/Server Detection

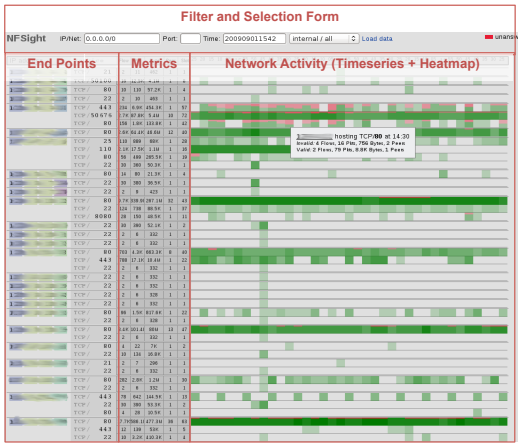
Bidirectional Flows (Netflows paired-up by IP/port)

Heuristic ID	Features and Formula Used	Output
Heuristic 0	Timestamp of request < Timestamp of reply	[0, 1]
Heuristic 1	Src port > Dst port	{0, 0.5, 1}
Heuristic 2	Src port > 1024 > Dst port	{0, 0.5, 1}
Heuristic 3	Port in /etc/services	{0, 0.5, 1}
Heuristic 4	# ports related	[0, 1]
Heuristic 5	# IP related	[0, 1]
Heuristic 6	# Tuples related	[0, 1]

Decisions combined with Bayesian infer.

IP Address	Proto.	Port	Type	Bayesian Probability
10.0.123.1	TCP	22	Server	98%
		80	Server	92%
10.0.123.8	TCP	25	Server	97%
		143	Server	98%
192.168.1.34	TCP	80	Client	75%
		443	Client	87%
192.168.4.56	TCP	6667	Server	95%
	UDP	22456	Client	62%

Visualization Front-end



Top 20 Scanned Services:

service	sources	Flow	Pkts	byte	Peer/5min
TCP/25	2617	75.6K	159.6K	8.3M	8
TCP/5900	706	213.5K	400.1K	20.3M	12
TCP/80	172	811.2K	1.1M	49.8M	652
TCP/443	113	62.6K	111.4K	5.4M	72
TCP/23	70	16.6K	44.3K	2.1M	24
TCP/22	46	801.9K	1.1M	62.9M	1.6K
TCP/3072	38	5.8K	7.6K	356.1K	39
TCP/1024	38	5.7K	7.4K	346.5K	38
TCP/1433	37	1.4M	1.5M	61.3M	15K
TCP/3389	32	307.3K	332K	16.7M	3K
TCP/8080	18	211.5K	325.4K	14.7M	372
TCP/9415	18	429.1K	498.7K	21M	2.8K
TCP/3128	17	244.2K	396K	17M	397
TCP/465	15	412	609	27.7K	6
TCP/1080	12	591.8K	603K	24.4M	3.7K
TCP/8296	9	487	573	23.1K	8
TCP/38981	9	926	1.1K	44K	11
TCP/53329	9	513	592	23.9K	9
TCP/63580	9	450	536	21.6K	8
TCP/8000	9	1M	1M	41.9M	10.8K

Detection of Scanning Activity: