

*A summary of security-related network
measurements.*

David Malone
Maynooth University.

2017-09-11 15:15:00

Network Measurement Results

- Internet Measurement Conference (IMC),
- Passive and Active Measurement Conference (PAM),
- Traffic Measurement and Analysis (TMA),
- Also at SIGCOMM, Usenix Security, IEEE SS&P, NDSS, ...

Packet Processing Frameworks

- BPF
 - old, useful and new uses in Linux.
- PF_RING
 - faster packet capture,
 - reduces copies,
 - better multithreading, queueing, hashing, ...
- DPDK/netmap
 - full packet processing in userland,
 - can write switches/firewalls/IDSes/...,
 - used to accelerate various tools.

Form the basis for tcpdump, tshark, wireshark, ...

Some interesting extensions for other technology (e.g. radiotap for WiFi, usbdump for USB).

Scanning Tools

- nmap
- nc
- zmap
 - Bit like nmap,
 - Focused on fast large-scale scanning,
 - Did a 65536 host network in 10s,
 - Whole IPv4 Internet in 5min (10Gbps + PF_RING)
 - Family of tools for:
 - zgrab for banner grabbing,
 - zdns for looking up DNS,
 - zcrypto/zlint/zcertificate for TLS/cert analysis.
 - Even a search engine <https://censys.io>
- Some more advanced tools like scamper.

Measurement Infrastructure

- Looking glasses,
- Passive Network Telescopes
 - Unused but routed address space,
 - Look for direct attacks or reflected spoofed traffic,
 - e.g. UCSD (CAIDA) or Team Cymru Darknet.
 - Often used to monitor DDoS events.
- RIPE Atlas,
 - (10,000) Small computer hosted in network,
 - Does pings/DNS lookups/... ,
 - Allows user-defined measurements,
 - Encourages researchers to get involved.
- CAIDA ARC,
 - Currently Raspberry Pi hosted by researchers,
 - Used for topology measurement, DNS measurements, ...
 - Allows ping/traceroute interface for researchers.
- Facebook ads.

IPv6

- Google sees about 20% users using IPv6,
- Ireland at about 10%
- Interest in mapping usage
- Log files and traceroutes,
- Akami mapping users,
- Now interest in target generation (DNS walking, ...),
- How to map open relays, proxies, resolvers, ...
- How to identify IPv4/IPv6 pairs,
- Also interest in new protocol features (e.g. extension headers).

Some studies of address scarcity and markets forming for IPv4.

Routing

- Longstanding problem of measuring topology,
- Some research on whose AS can see your packets,
- Who is allowing spoofing (egress filtering)?
- BGP studies of flapping, AS reputation, hijacking,
- Some great databases of historical data,
- Starting studies of RPKI.

Related: DDoS measurement/mitigation, geolocation, ...

Vaguely related: Spotting large scale network scans.

DNSSEC

- How deployed is DNSSEC?
 - Server side: who signs, what algorithms, ...?
 - Client side: who verifies?
- Deployment challenges.
 - EDNS0 extensions for large responses.
 - Switching to TCP.
- Effectiveness of NSEC.
- Measuring key rollover.

Other DNS activity: detecting alternative roots, performance/robustness of anycast, ...

TLS/SSL

- Deployment levels have always been well monitored.
- Performance has also been of interest.
- Health of certificate system:
 - certificate transparency,
 - certificate validity (65% have problems),
- Fascinating attacks on keys:
 - Debian RNG bug.
 - $\gcd(N_1, N_2)$ for RSA.
 - Resulting patching behavior.
- Implementation problems
 - long session caching,
 - long Diffie-Hellman lifetimes,
 - clients presenting TLS certificates.

Network Censorship

- Understanding the Great Firewall of China,
- Measuring Internet disconnection around specific events,
- Finding websites or pages that are blocked,
- Finding content and keywords that are blocked.
- People hiding protocols on wrong port/with TLS/with Tor.

There's a whole side subject or Tor deanonymisation.
Has raised ethical issues.

Modern Mobile/App/Web Infrastructure

- What are mobile operators middle boxes up to?
- How trackable are you with TLS on?
- How can we find personally identifying information?
- How do apps behave?
 - How many are built evil?
 - How many apps/frameworks are calling home?
- Are tracker blockers/ad blockers/cookie directives any good?

Interesting High Level Measurements

- Deanonimisation of bitcoin transactions.
- Analysis of propaganda/fake news bots.
- Detecting and characterising doxing.
- Who gets to see your e-mail?
- What happens to stolen e-mail creds?