Session 5

Compounding Trends Toward Invisibility of Infrastructure

Encryption / Protocols

Specific type of invisibility? [1/3]

- The process of securing existing protocols (e.g., HTTPS)
- The emergence of new protocols, developed with encryption by design (e.g., QUIC)
- (odd one out) Lack of information about infrastructure decisions (e.g., what’s behind a SERVFAIL?)

Specific type of invisibility? [2/3]

Resultingly:

- “Previously known” data is hidden
- Potential to dpi is lost/lowered
  - Threat detection (e.g., malware, higher-layer attacks, …)
  - Traffic engineering
  - Exposure to data exfiltration
- *<Your measurement concern here>*

Specific type of invisibility? [3/3]

A compounding issue:

- *Shifting* client-to-infrastructure interaction to elsewhere (ISP/Cloud)

Taking DoH/DoT as example:

- Centralized DNS (management & security of dependent infrastructure becomes harder)
- Controls can be bypassed (phishing sites, etc.)

VPN is also an interesting case

Broader impact

- “Encryption is needed to protect privacy” (classic argument)
- The trick is: protecting privacy while still enabling legitimate measurement and security-focused uses
- Performance may be affected
  - and cascading perception of performance

Specific solutions to invisibility? [1/2]

- Voluntary participation in research data collection (e.g., via opt-in proxy)
- “Enterprise-mandated” participation
  - e.g., block certain traffic (not always applicable)
- Moving (or adding) VPs to points where things are (still) visible
  - e.g., move above recursive (again, may n/a)

Specific solutions to invisibility? [2/2]

- Adapt protocols to extract information without breaking privacy goals (e.g., QUIC spin bit)
- RFC8914 Extended DNS Error Codes (what’s behind that SERVFAIL?)
- Small letters (e.g., Quad9)

Role of govt.

- Obviously, some monitor network traffic for law enforcement and intelligence gathering
- Others (agencies) may seek access to network traffic for policy assessment / enforcement (e.g., FCC in the US)
- NIST and ENISA often play a role in standardizing ciphers for protocols
- Some block traffic traffic altogether (e.g., China)
  - This may, in some ways, hamper market forces (in specific areas)

Research questions that require measurement/data

- Skipping several (covered in previous summaries)
- Is performance negatively affected by the centralization of services?
- Do protocols/services actually provide privacy, or create additional side channels? (e.g., CT lookups)

What can the NSF do?

- Convene an entire workshop specifically on this topic (yes, really!)
- Facilitate data access discussions with large providers
- Identify network monitoring as a specific focus area for a targeted funding program