CONSIDERATIONS ON

APPLICATION – NETWORK COLLABORATION USING PATH SIGNALS

DRAFT-ARKKO-PATH-SIGNALS-COLLABORATION

IAB OPEN SESSION, IETF-111, JULY 2021

JARI ARKKO, MIRJA KÜHLEWIND, TOMMY PAULY, TED HARDIE

PATH SIGNALS

Path signals are signals to or from on-path elements

- Past signals were often implicit, e.g., derived from in-clear end-to-end information such as transport protocols data that happened to be available
- This results in negative effects:
  - Ossification
  - Systemic incentives against more secure protocols
  - Basing behavior on information that may be incomplete / wrong
  - Creating an expectation that network elements can see rich data about flows

PATH SIGNALS

But there's good news:

- Increased use of encryption has changed this for the better
- Encryption is also an opportunity to redesign path signal cooperation to be explicit and secure

Some existing guidance:

- RFC 8558 recommendations: build for confidential operation and use explicitly designed mechanisms for sharing data (if needed)
- Draft-irtf-panrg-what-not-to-do guidelines & documentation of failures

GUIDING PRINCIPLE	WHAT	EXAMPLES
Intentional distribution	Per RFC 8558	Bad: middlebox reads TCP options Good: ECN
Minimal set of entities	Limit exchange to those with need to know	Bad: cleartext DNS query Good: encrypted query
Minimum information	The info that is needed for the task	Bad: user's or application's identity Good: describing sender's QoS preferences
Consent of parties	Sender, recipient, and ultimately user willingness	Bad: must disclose user id, or must process hop-by-hop header Good: Application decides
Securing the signals	Does the information need to be protected? Do the parties need to be authenticated?	Sharing simple data (e.g., ECN bits) Sharing sensitive data (e.g., DNS) Authentication may not imply trust

AREAS FOR FURTHER RESEARCH

The following topics have traditionally been difficult, and more work is needed:

- Business arrangements
  - E.g., expectation of paying for a service is core to many QoS designs and a big reason why various proposals have failed
- Secure communications with path elements
- Could path signals help combat denial-of-service attacks?
- Protecting information held by network or servers
  - Going beyond communications security (e.g., Oblivious-X, enclaves)
- Sharing information from networks to applications
  - E.g., mobile networks know a lot about network capacity, but can that info be safely shared?