The Impact of Transport Header Encryption on Operation and Evolution of the Internet
draft-fairhurst-tsvwg-transport-encrypt-04

Gorry Fairhurst, Colin Perkins
Transport

• Transports *discover and adapt* to the properties of the current Internet path:
  • adapting to changes in path characteristics
  • avoiding unwanted side effects of congestion, PMTU, etc
  • avoiding impact on other flows sharing a part of the path
  • avoiding congestion collapse

• Design of current methods have benefited from measurement and insights of the operations community to understand trade-offs
Encryption

Once most Internet packets looked like this:

Soon they could all look like this:

E-2-E Transport
Encrypt
UDP
Network

RFC 793, 1981

2017: Does this matter?
Transport Header Encryption

- Encryption is not new... IPSEC, VPNs, TOR, etc
- But, a growing trend for various reasons, e.g.:
  - Encryption can overcome ossification, allowing deployment of new transports with new mechanisms
  - Encryption helps protect privacy
  - Encryption transfers *more control* to “origin” servers
- So, what other impacts are there if *more* traffic is encrypted?
Support for Network Operations

Why would operators want to look at transport headers?
Support for Network Operations

Why would operators want to look at transport headers?

- **Volume and Type of Traffic**: to Plan and Provision Networks
  - Characterising traffic (& compliance to SLA)
  - Characterising “unknown” traffic
Support for Network Operations

Why would operators want to look at transport headers?

- **Volume and Type of Traffic:** to Plan and Provision Networks
  - Characterising traffic (& compliance to SLA)
  - Characterising "unknown" traffic
- **Dynamics of Traffic:** for service performance measurement
  - Locating configuration/equipment faults
  - Understanding scale of impact for a new feature, app, etc.
Support for Network Operations

Why would operators want to look at transport headers?

- **Volume and Type of Traffic:** to Plan and Provision Networks
  - Characterising traffic (& compliance to SLA)
  - Characterising “unknown” traffic
- **Dynamics of Traffic:** for service performance measurement
  - Locating configuration/equipment faults
  - Understanding scale of impact for a new feature, app, etc.
- **Protocol Interactions:** for Diagnostics and troubleshooting
  - Could be as simple as helping locate customer performance issues, but if an operator does not see the packets, they are unlikely to help!
Can pervasive encryption impede R&D?
Can pervasive encryption impede R&D?

- Transport protocols are both complicated to design and complex to deploy
Can pervasive encryption impede R&D?

• Transport protocols are both **complicated to design** and **complex to deploy**

• Measurements are needed:
  • To understand what is currently being used and with what effect?
  • Most useful where packets can be correlated with problems/interactions (loss, queues, etc)
  • Encryption hides the actual used protocol mechanism
Can pervasive encryption impede R&D?

- Transport protocols are both *complicated to design* and *complex to deploy*
- Measurements are needed:
  - To understand what is currently being used and with what effect?
  - Most useful where packets can be correlated with problems/interactions (loss, queues, etc)
  - Encryption hides the actual used protocol mechanism
- Individual mechanisms need to be evaluated while considering other mechanisms, across a range of network topologies
  - Broadness of deployability is the key challenge
  - Often has been the focus of research/academic contributors (e.g., IRTF ICCRG, and research publications)
Next Steps

• How does the IETF provide incentives to ensure good practice that benefits the wide diversity of requirements for the Internet community as a whole?

• HELP!!!! We are looking for people to read and help understand the implications
  • Please read: draft-fairhurst-tsvwg-transport-encrypt

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688421.