University of Glasgow

School of Computing Science

60 YEARS OF COMPUTING AT GLASGOW

The Impact of Transport Header Encryption on Operation and Evolution of the Internet

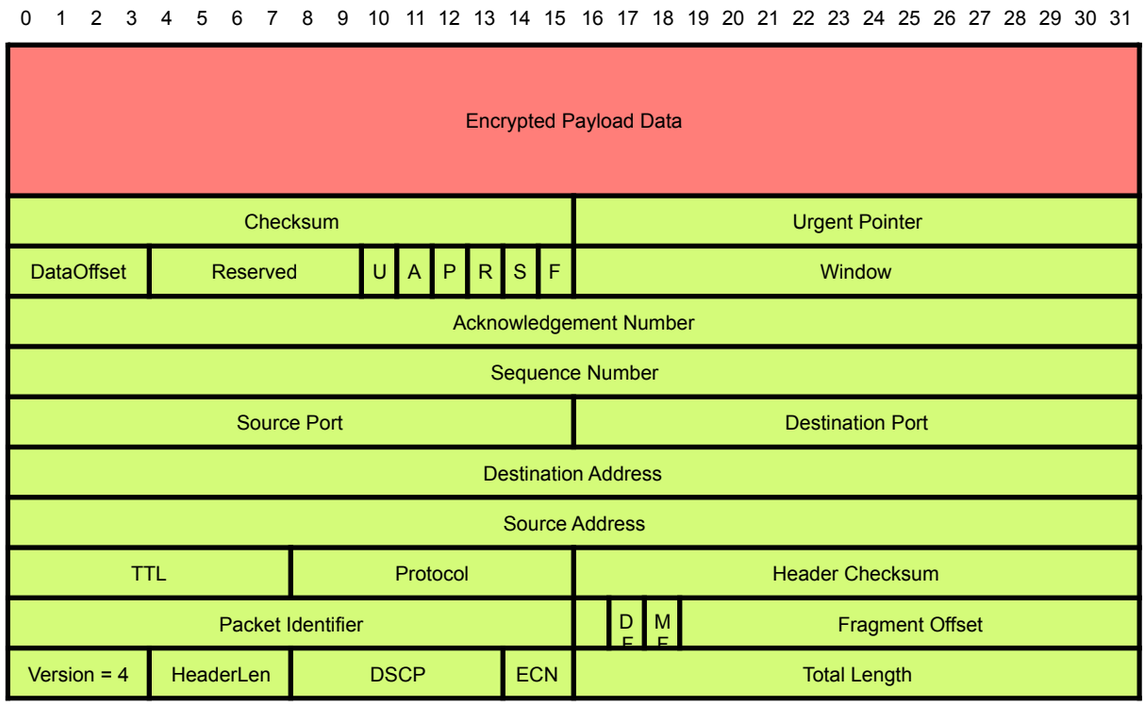
draft-fairhurst-tsvwg-transport-encrypt-04

Gorry Fairhurst – University of Aberdeen

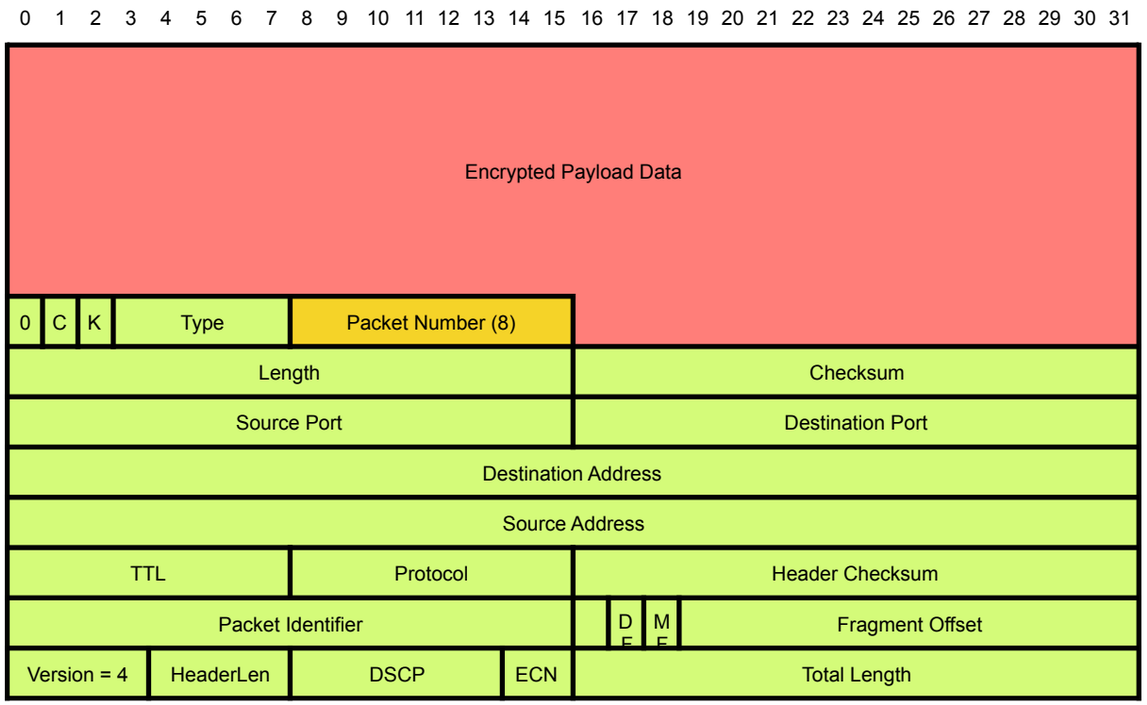
Colin Perkins – University of Glasgow

Presentation given to IETF TSVWG on 13 November 2017

Transport Header Encryption



TCP



QUIC

Increasing fraction of transport headers encrypted → reduces network visibility of transport progress (seq/ack numbers, window, flags)

QUIC an example – in principle everything above IP and ports could be encrypted

Benefits

- Reduces information leakage → enhances privacy
  - Harder to infer connection progress
  - Harder to infer RTT and timing variation
  - Prevents some spoofing/injection attacks against transport
- Preventing middlebox ossification → flexibility to change transport

- Benefits are widely reported

Costs

- Complicates network operations:
  - Network operations
  - Network trouble-shooting and diagnosis
  - Network traffic analysis
  - Open and verifiable network data
- Complicates protocol specification:
  - Understanding feature interactions
  - Supporting common specifications
  - Compliance with operational practice
  - Research and development

Costs

- Complicates network operations:
  - Network operations
  - Network trouble-shooting and diagnosis
  - Network traffic analysis
  - Open and verifiable network data
- Complicates protocol specification:
  - Understanding feature interactions
  - Supporting common specifications
  - Compliance with operational practice
  - Research and development

Observable transport headers → operators can analyse overall network performance

- help to detect anomalies
- inform capacity planning
- inform traffic engineering

Passive overview of the health of the network, care about overall behaviour, not per flow

Important for operations: transport encryption → work-arounds will be developed

- active traffic probes
- encapsulations to replace missing headers

Costs

- Complicates network operations:
  - Network operations
  - Network trouble-shooting and diagnosis
  - Network traffic analysis
  - Open and verifiable network data
- Complicates protocol specification:
  - Understanding feature interactions
  - Supporting common specifications
  - Compliance with operational practice
  - Research and development

Operators can't debug what they cannot observe

- Encrypted transport headers → flows subject to packet loss, other issues, indistinguishable from unaffected flows

Debugging will require active probes – intrusive, behaviour potentially differs from real traffic – or information from endpoints – not trustworthy?

Costs

- Complicates network operations:
  - Network operations
  - Network trouble-shooting and diagnosis
  - Network traffic analysis
  - Open and verifiable network data
- Complicates protocol specification:
  - Understanding feature interactions
  - Supporting common specifications
  - Compliance with operational practice
  - Research and development

Operators can't do traffic engineering or analysis if they cannot see the traffic

Costs

- Complicates network operations:
  - Network operations
  - Network trouble-shooting and diagnosis
  - Network traffic analysis
  - Open and verifiable network data
- Complicates protocol specification:
  - Understanding feature interactions
  - Supporting common specifications
  - Compliance with operational practice
  - Research and development

Encrypting transport headers limits open and verifiable data on transport behaviour

- Operators and researchers cannot tell if the transport is behaving as intended
- The community loses the data to inform future developments and to understand operational behaviour of transports → endpoint telemetry helps, but not necessarily trustworthy

Costs

- Complicates network operations:
  - Network operations
  - Network trouble-shooting and diagnosis
  - Network traffic analysis
  - Open and verifiable network data
- Complicates protocol specification:
  - Understanding feature interactions
  - Supporting common specifications
  - Compliance with operational practice
  - Research and development

Understanding transport mis-behaviour relies on being able to observe transport headers

- Essential for transport protocol research and protocol debugging by operators/vendors
- Needs to happen in the wild – testbeds don't *discover* feature interaction problems

Costs

- Complicates network operations:
  - Network operations
  - Network trouble-shooting and diagnosis
  - Network traffic analysis
  - Open and verifiable network data
- Complicates protocol specification:
  - Understanding feature interactions
  - Supporting common specifications
  - Compliance with operational practice
  - Research and development

Ecosystem fragmentation – faster innovation is desirable, point solutions are fragile

TCP works so well because it's open, and can be observed and improved by all

Pervasive encryption removes the checks-and-balances, and reduces incentives to conform to specifications, develop openly → problem for long-term health of standards ecosystem and network

Conclusions

- We are not against transport-level encryption – it offers important benefits – but also has costs for operations, protocol development, and standards
- We must seek balance – obstructing real operations needs will lead to work-arounds being deployed, and will likely not increase privacy

- Consider adopting as WG item, to encourage discussion of these issues

> "While PM is an attack, other forms of monitoring that might fit the definition of PM can be beneficial and not part of any attack, e.g., network management functions monitor packets or flows and anti-spam mechanisms need to see mail message content. Some monitoring can even be part of the mitigation for PM, for example, certificate transparency [RFC6962] involves monitoring Public Key Infrastructure in ways that could detect some PM attack techniques. However, there is clear potential for monitoring mechanisms to be abused for PM, so this tension needs careful consideration in protocol design. **Making networks unmanageable to mitigate PM is not an acceptable outcome**, but ignoring PM would go against the consensus documented here. **An appropriate balance will emerge over time as real instances of this tension are considered**."
>
> [RFC7258, "Pervasive Monitoring Is an Attack"]