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

draft-fairhurst-tsvwg-transport-encrypt

Gorry Fairhurst – University of Aberdeen (MAMI)

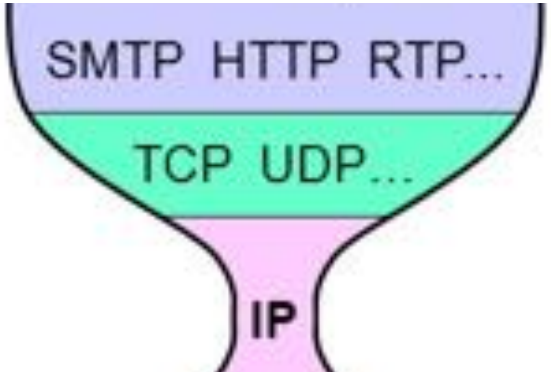
Colin Perkins – University of Glasgow

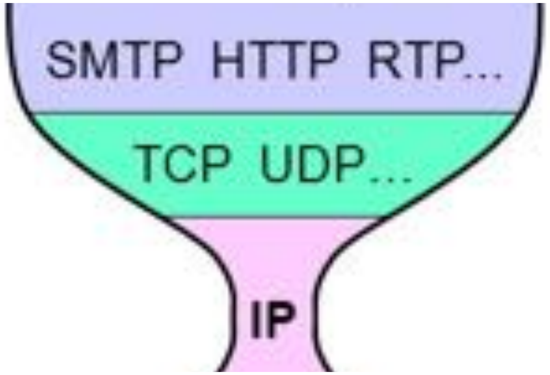
mami

measurement and architecture for a middleboxed internet

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688421.The opinions expressed and arguments employed reflect only the authors' view. The European Commission is not responsible for any use that may be made of that information..

My view of transport



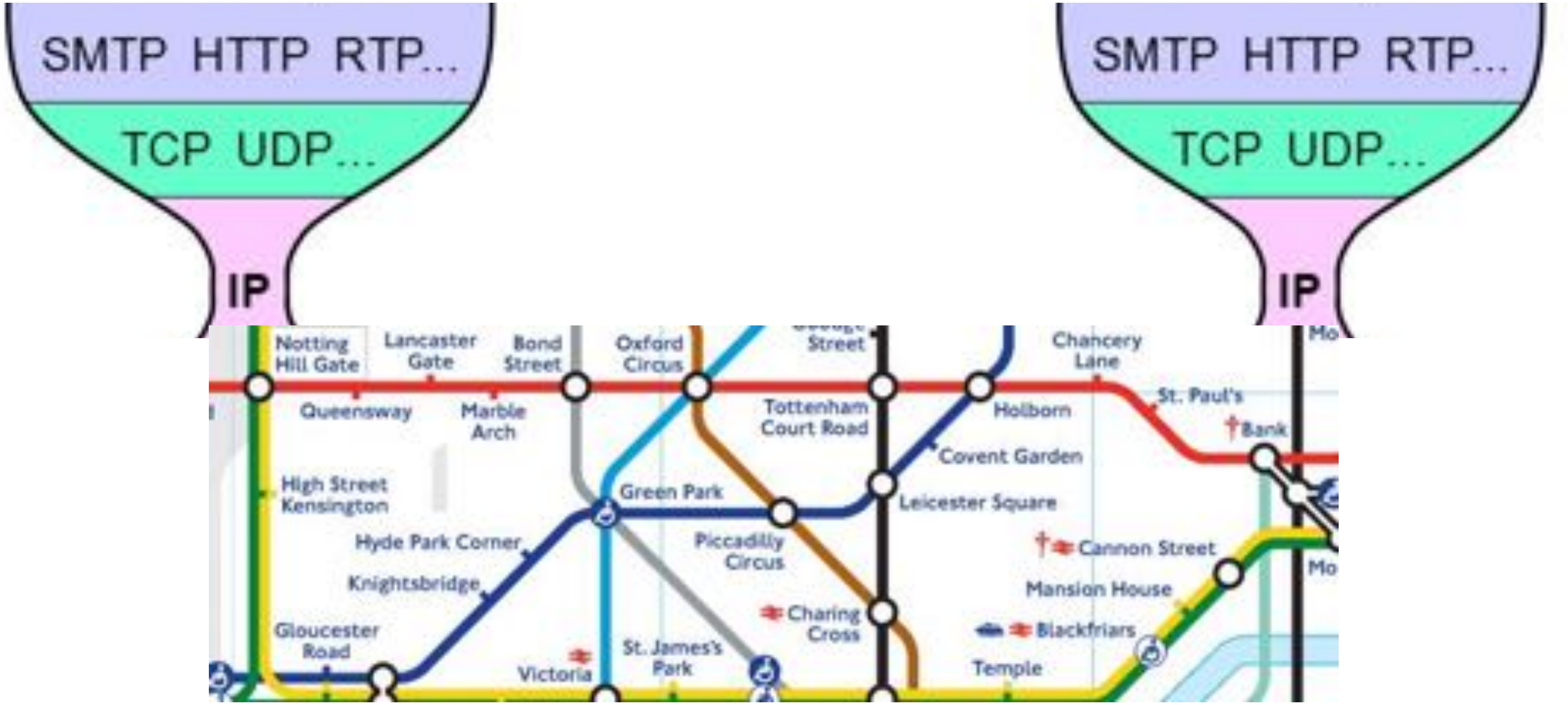


Packets move across the network

End-to-End functions to ***move*** data

End-to-End ***negotiation*** of features

My view of transport



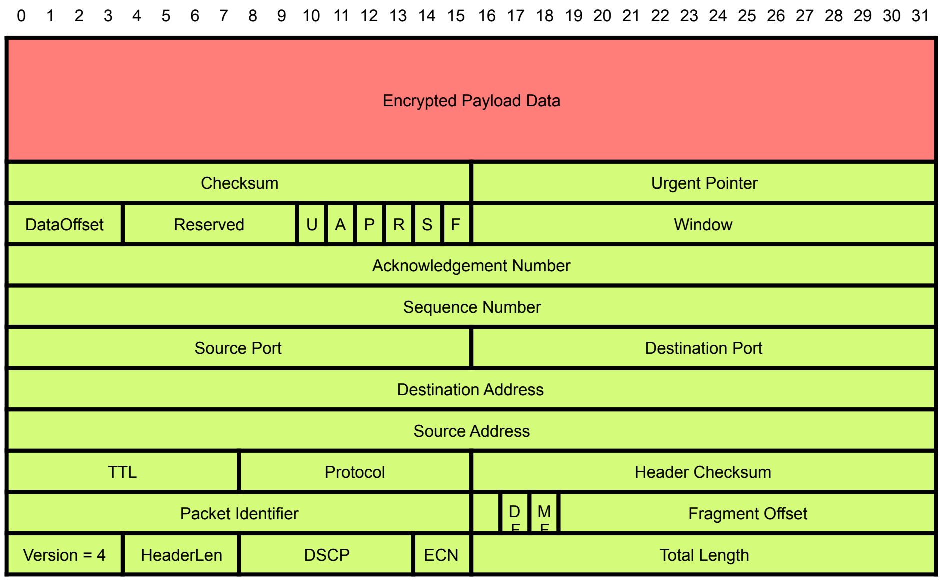
End-to-End functions to ***move*** data

End-to-End ***negotiation*** of features

Adaption to the network path

Making this ***work well***

Transport Header Encryption



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Encrypted Payload Data

Checksum | Urgent Pointer

DataOffset | Reserved | U | A | P | R | S | F | Window

Acknowledgement Number

Sequence Number

Source Port | Destination Port

Destination Address

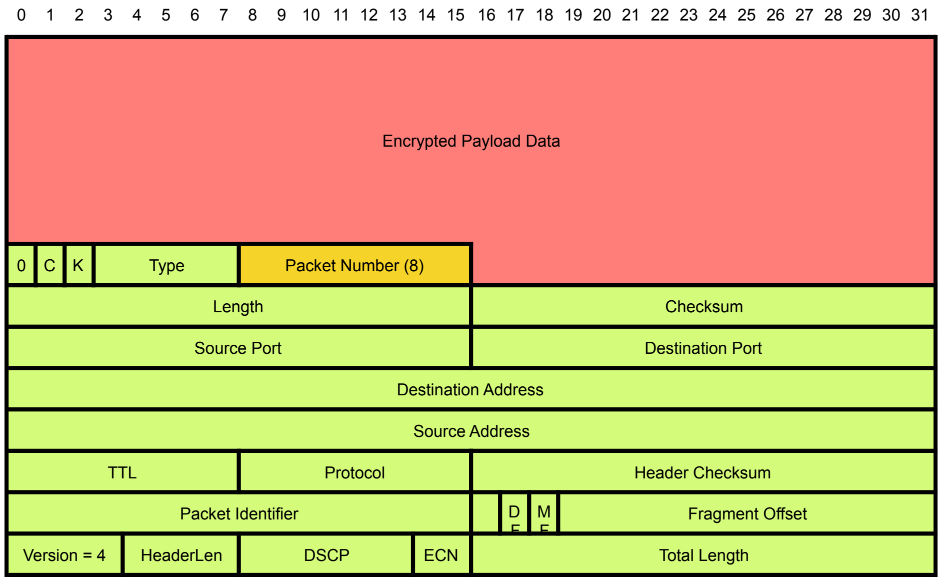
Source Address

TTL | Protocol | Header Checksum

Packet Identifier | DF | MF | Fragment Offset

Version = 4 | HeaderLen | DSCP | ECN | Total Length

TCP Transport Header



0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Encrypted Payload Data

0 | C | K | Type | Packet Number (8)

Length | Checksum

Source Port | Destination Port

Destination Address

Source Address

TTL | Protocol | Header Checksum

Packet Identifier | DF | MF | Fragment Offset

Version = 4 | HeaderLen | DSCP | ECN | Total Length

QUIC Transport Header

In principle, everything above IP and ports ***could*** be encrypted

Eliminates network visibility of the transport headers

An increasing fraction of transport headers ***is being*** encrypted

Benefits of Header Encryption

Reduces information leakage

→ ***enhances privacy***

Harder to infer connection progress/operation

Harder to infer the user or application using the network

Avoids assumptions about the needs of traffic being carried

Prevents middlebox ossification

→ ***flexibility to change transport***

Avoids some spoofing/injection attacks against transport

Benefits are widely reported

Costs of pervasive encryption

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

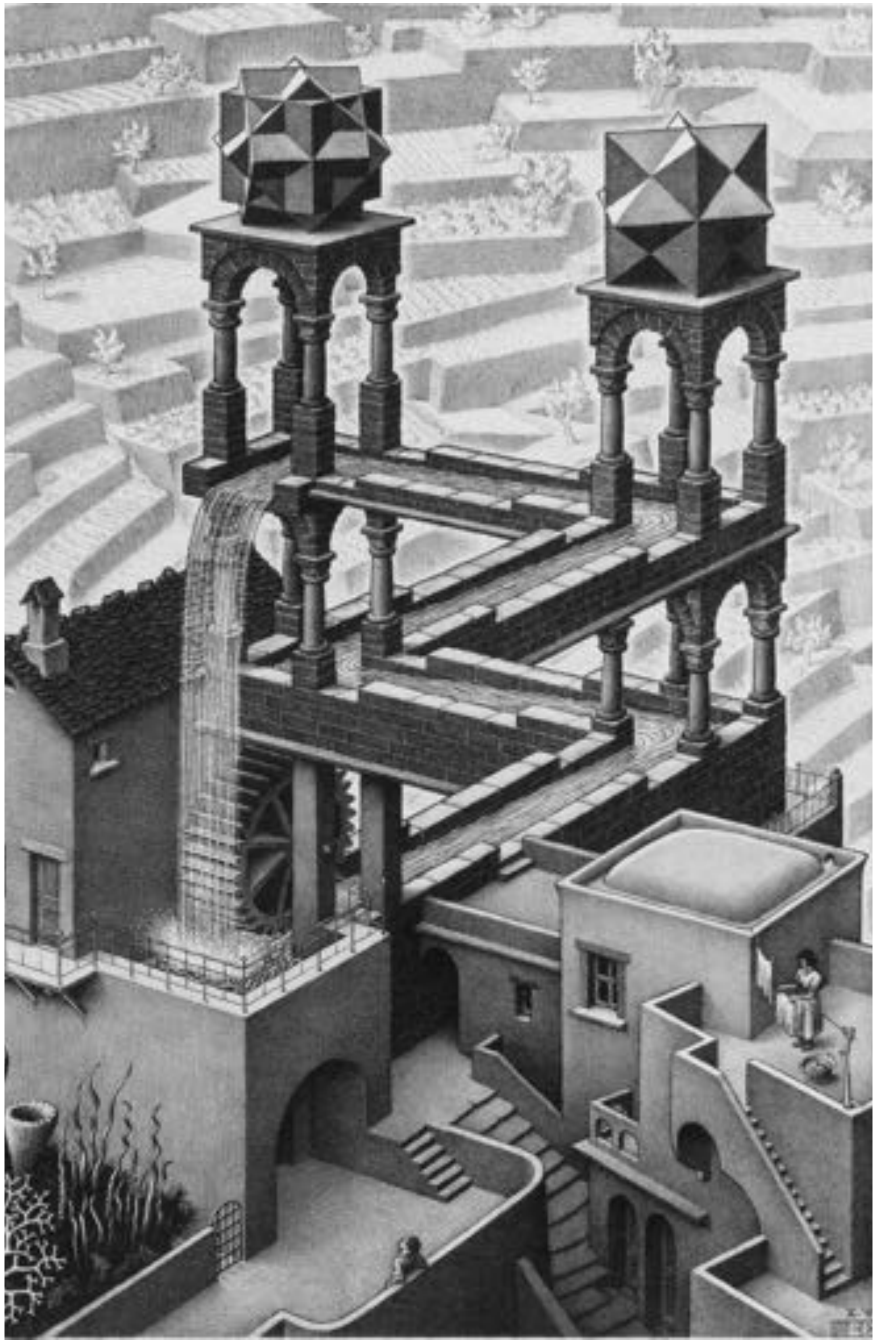
Compliance with operational practice

Research and development

Perspective Matters

Q1: How are Transport headers being used now?

Q2: What is the best recommended practice for encrypting transport headers?



M.C. Escher, Waterfall, 1961, lithograph

Next Steps

Transport-level encryption offers important benefits – but also has costs for operations, and protocol development

This may be problems for long-term health of standards ecosystem and research support for network protocols

Obstructing operational needs will lead to deploying (multiple) work-arounds, and likely will not increase privacy or consistency

The IETF needs to understand the tradeoffs and seek a balance

Costs of pervasive encryption

Complicates network operations:

Network operations

Network trouble-shoo

Network traffic analys

Open and verifiable r

Complicates protoco

Understanding featu

Supporting common

Compliance with ope

Research and development

Operators can currently analyse performance by observing transport headers:

- help to detect anomalies
- inform capacity planning
- inform traffic engineering
- provide an overview of network health

Other tools needed for encrypted traffic:

- encapsulations to replace missing headers
- active probes, etc

Costs of pervasive encryption

Complicates network operations:

Network operations

Network trouble-shooting and diagnosis

Network traffic analy

Open and verifiable

Complicates protoc

Understanding featu

Supporting commor

Compliance with op

Research and development

Can’t **debug** what cannot be observed

- flows subject to loss, jitter, etc, are indistinguishable from unaffected flows

→ Debugging encrypted traffic requires either:

- active probes: both intrusive and behaviour potentially differs from real traffic
- information from endpoints

Costs of pervasive encryption

Complicates network operations:

Network operations

Network trouble-shooting and diagnosis

Network traffic analysis

Open and verifiable ne

Can’t do **traffic engineering** or **analysis**
if they cannot see the traffic

Complicates protocol specification:

Understanding feature interactions

Supporting common specifications

Compliance with operational practice

Research and development

Costs of pervasive encryption

Complicates network operations:

Network operations

Network trouble-shooting and diagnosis

Network traffic analysis

Open and verifiable network data

Complicates protocol

Understanding feature

Supporting common s

Compliance with operational practice

Research and development

Limits **open and verifiable** data on behaviour

- Loss of data to understand operational behaviour of transports
- Can’t tell if transport ***behaves as intended***

Costs of pervasive encryption

Complicates network operations:

Network operations

Network trouble-shoo

Network traffic analys

Open and verifiable n

Hinders understanding of **interactions** between transport, applications and networks

- Measurements **need to be in the wild**
  → testbeds don't discover feature interaction problems, anomalies, etc

Complicates protocol specification:

Understanding feature interactions

Supporting common specifications

Compliance with operational practice

Research and development

Costs of pervasive encryption

Complicates network operations:

Network operations

Network trouble-shooting and diagnosis

Network traffic analysis

Open and verifiable ne

Complicates protocol s

Understanding feature

Supporting common specifications

Compliance with operational practice

Research and development

Hard to confirm conformance

- Tools need ***to evolve track each version***
- Reduces incentives to conform
  → endpoint telemetry helps, but not necessarily trustworthy

Costs of pervasive encryption

Complicates network operations:

Network operations

Network trouble-shooting and diagnosis

Network traffic analysis

Open and verifiable ne

Complicates protocol s

Understanding feature

Supporting common sp

Compliance with opera

Research and development

Danger of ecosystem fragmentation:

- While faster innovation is desirable, point solutions are ***fragile***
- ***loss of data*** to inform future developments and understand operational behaviour
- ***removes the checks-and balances***

Pervasive Monitoring

While Pervasive Monitoring “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”]