WP3: Middlebox Cooperation

Gorry Fairhurst WP3 Lead

2nd Technical review

3rd October 2017

Research and Innovation Action **688421**

Call: H2020-ICT-2015: Integrating experiments and facilities in FIRE+

mami

measurement and architecture for a middleboxed internet

measurement | architecture | experimentation

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..

Objectives from DoW

- Definition of **use cases and requirements** for an architecture for Middlebox Cooperation Protocol (MCP)
- **Design, implementation, and initial testing** of the **MCP** to provide an information exchange between end hosts and middleboxes
- Design of a **flexible transport stack (FTL)** to complement the MCP, restoring connectivity over the Internet
- **Threat and trust analysis** of the developed protocols, protocol extensions and transport layer mechanisms as a basis for Internet-scale deployment

WP3 Tasks Overview

T3.1: Use Case Analysis and Requirement Definition (M1 - M6)

T3.2: Design of the MCP (M7 - M24)

T3.3: Design of a flexible cooperative transport layer (M7 - M36)

T3.4: Implementation and Testing (M9 - M36)

T3.5: Threat and Trust Analysis for Middlebox Cooperation (M1 - M36)

May include a GANTT chart snippet here

Overview - Who did what?

Partner	Task 3.1 Use Cases	Task 3.2 MCP Design	Task 3.3 FTL Design	Task 3.4 Implementation and Testing	Task 3.5 Threat and Trust Analysis
ETH	✓	✓	✓	✓	
TID	✓	✓			✓
UoA		✓	✓		
ZHAW	✓			✓	✓
ALU (Nokia)	✓		✓	✓	✓

Objectives

- Definition of **use cases and requirements** for an architecture for Middlebox Cooperation Protocol (MCP)
- **Design, implementation, and initial testing** of the **MCP** to provide an information exchange between end hosts and middleboxes
- Design of a **flexible transport stack (FTL)** to complement the MCP, restoring connectivity over the Internet
- **Threat and trust analysis** of the developed protocols, protocol extensions and transport layer mechanisms as a basis for Internet-scale deployment

Deliverables Summary

D3.1	**Use Case Analysis and Requirements**
D3.2	**Design of the MCP**
D3.3	**Design of a flexible cooperative transport layer**

WP3 activities in the reporting period

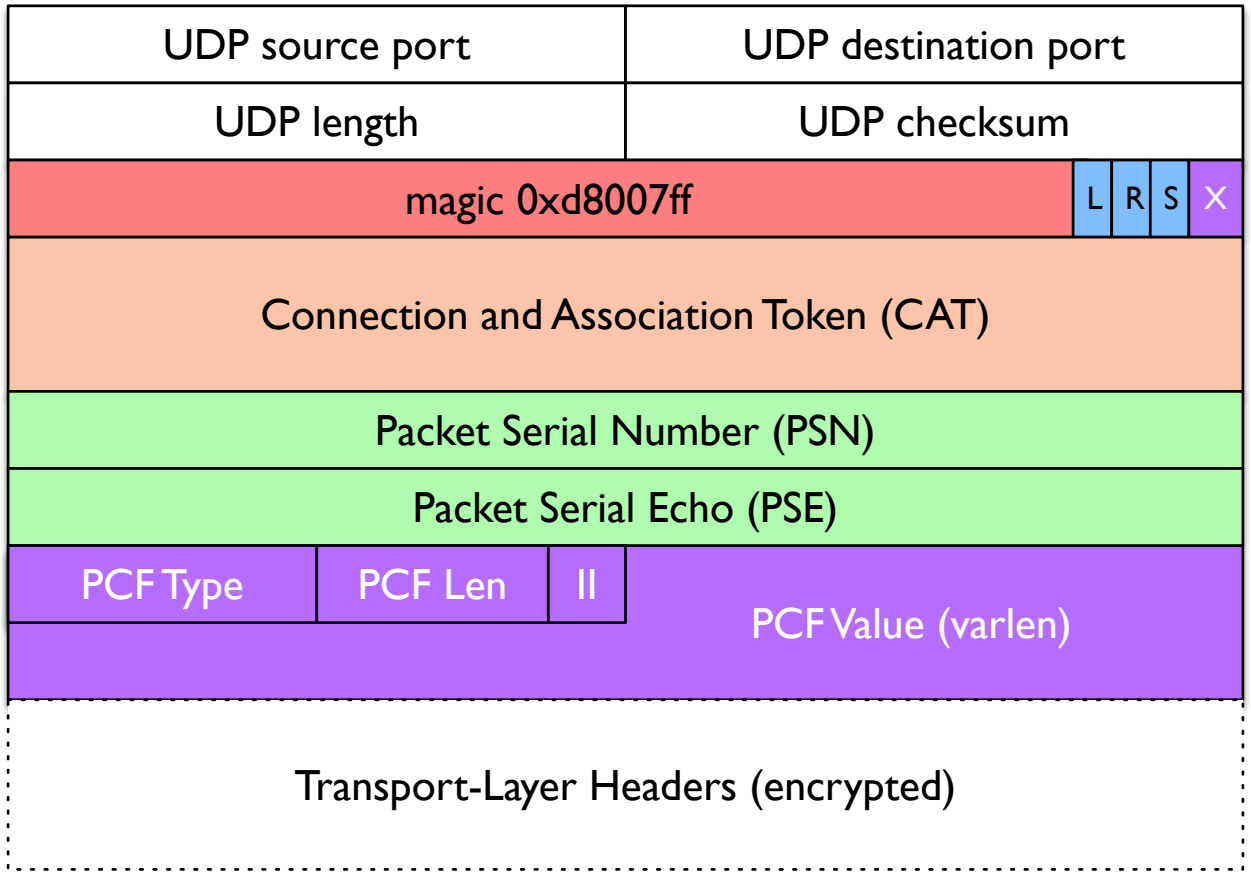
- Endpoint and **Middlebox Cooperation Protocol** (MCP)
  - Implementation of protocols and protocol extensions
- A New **Transport API**
- **Flexible Transport Layer** (FTL)
  - Implementation of protocols and protocol extensions
- **Security Analysis** and **Manageability**

Middlebox Cooperation Concept

- An endpoint should be able to explicitly expose any signals used by on-path devices.
- An endpoint should be able to request signals from devices on the path.
- An on-path device should not be able to forge, change, or remove a signal sent by an endpoint.
- The endpoint should control signaling.
- It should be possible for an endpoint to request and receive signals from a pre- viously unknown on-path device.
- There should be no significant surface for amplification attacks.

PLUS

D3.2 includes a consistent spec for middlebox cooperation



PLUS in IETF

Initial specification contributed to IETF PLUS design:

draft-trammell-spud-req (expired)

draft-trammell-plus-abstract-mech (expired)

draft-trammell-plus-statefulness (expired)

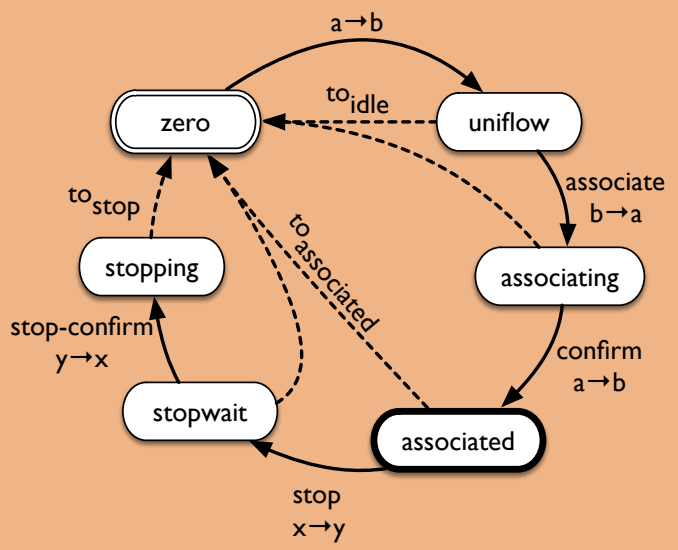
draft-trammell-plus-spec (expired)

PLUS work stagnated in the IETF

Concerns that a generic metadata exposure protocol could be used to force metadata injection on endpoints

We do not expect deployment of PLUS as specified in D3.2

PLUS state machine



TEXT ON HOW THIS FINISHED

QUIC in IETF

Google proposed a new protocol web transport (**QUIC**)

Work adopted as an IETF activity in 2017

All energy in transport/web space going into QUIC, which will actually deploy at scale in the near term (2019)

PLUS and QUIC in MAMI

MAMI adopted a broader focus on middlebox cooperation

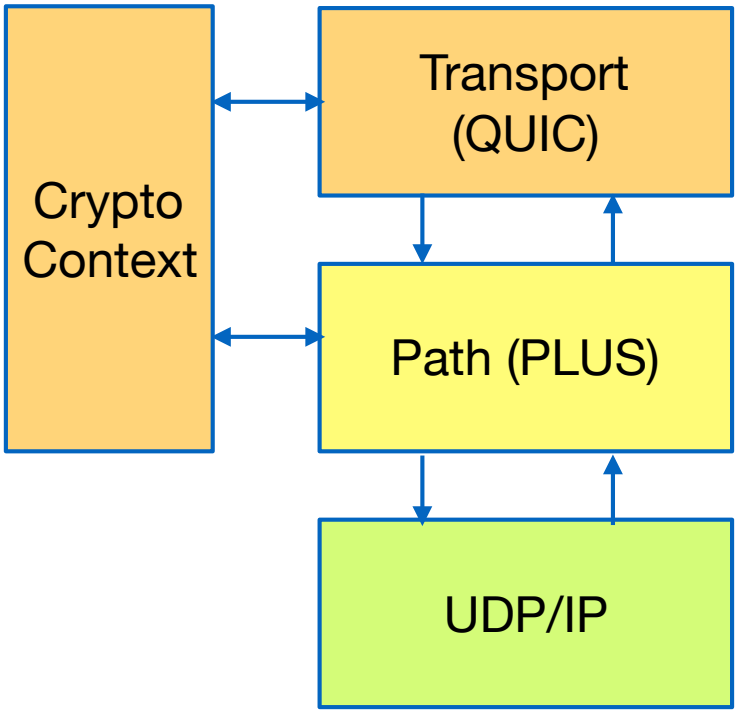
MAMI has shown concepts can be applied to other protocols

- Mechanisms using UDP
- Exploring mechanisms with QUIC

IETF applicability and manageability documents for QUIC

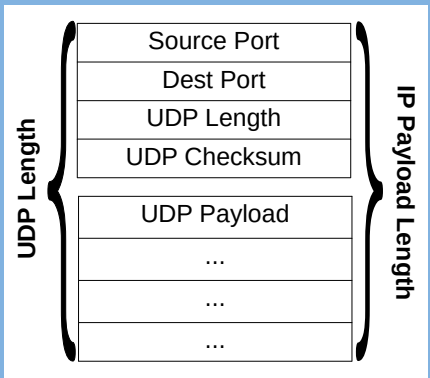
- draft-ietf-quic-manageability *(expected to be published 2019)*
- draft-ietf-quic-applicability *(expected to be published 2019)*
- *draft-trammell-quic-spin* (Consensus to be incorporated in QUIC)
- draft-trammell-wire-image (Progressing as draft-iab-wire-image)
- draft-trammell-privsec-defeating-tcpip-meta (expired)

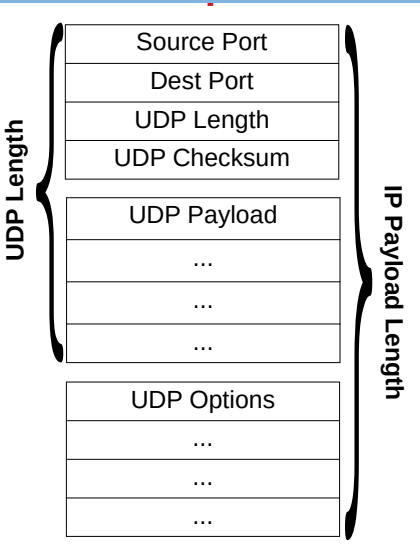
PLUS Reference Implementation
~~QUIC~~ GUIC

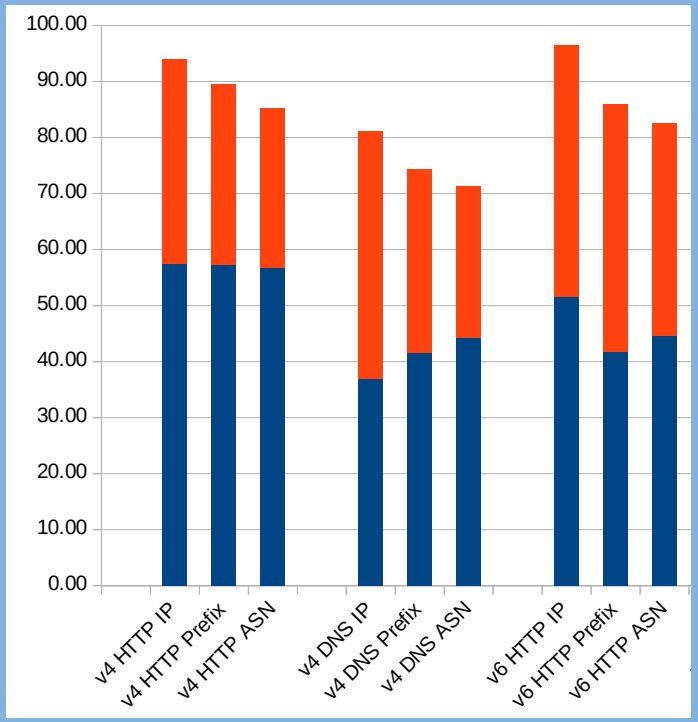


- QUIC spec expected Nov 2019
- Google's QUIC (GUIC) is the best we had for experimentation
- MAMI completed a software implementation in fd.io
- fd.io testbed built
- Experimentation in WP2

A Transport Stack with UDP Options



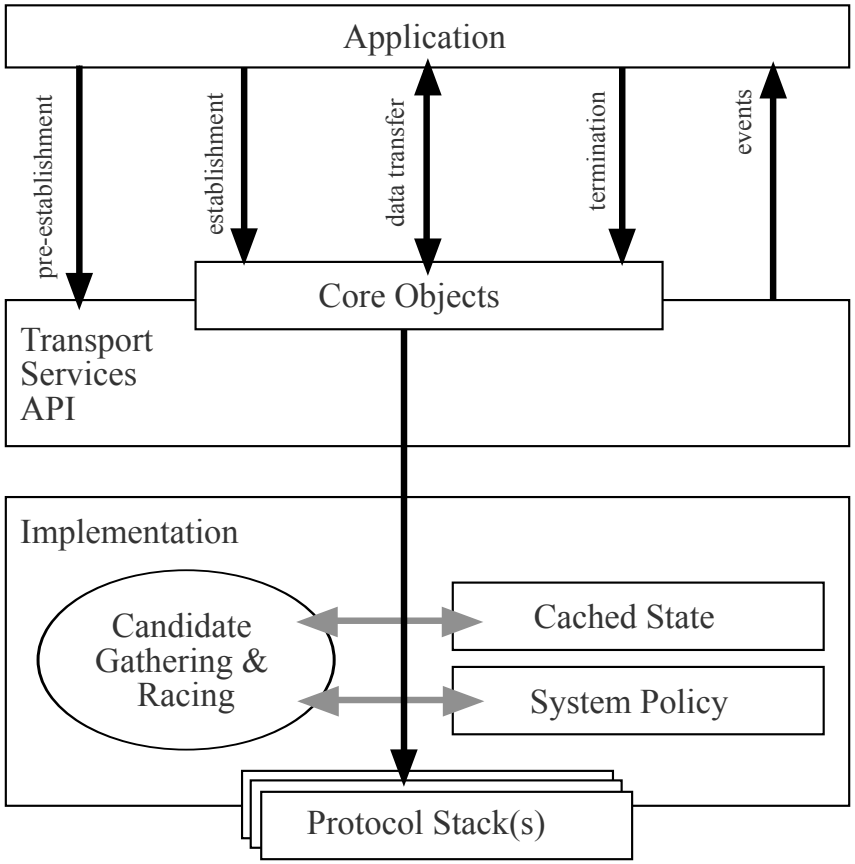




- UDP-O provides a way to add meta-information to UDP flows
- Open source reference implementation on the FreeBSD
- draft-fairhurst-udp-options-cco

CCO

Standards-based Abstract Interface for Transport Services (TAPS)



Definition of ***unified*** (abstract) API independent of protocol

Fallback and connection racing mechanisms

API Specifications: MAMI Documents

Inputs: *Post Sockets (see D3.2; Other IETF Participants: EU NEAT Project; Apple; TU Berlin)*

API/transport state-of-the-art

IETF Transport Services *(published as RFC 8095)*

draft-ietf-taps-transports-usage-udp *(published as RFC 8304)*

API/transport evolution contributions

draft-kuehlewind-taps-crypto-sep *(contribution to WG)*

draft-trammell-taps-post-sockets *(contribution to WG)*

API/transport evolution work items

draft-ietf-taps-arch *(expected to be published 2019)*

draft-ietf-taps-impl *(expected to be published 2019)*

draft-ietf-taps-interface *(expected to be published 2019)*

A Flexible Transport Layer (FTL)

Transport / Network Signaling Mechanisms

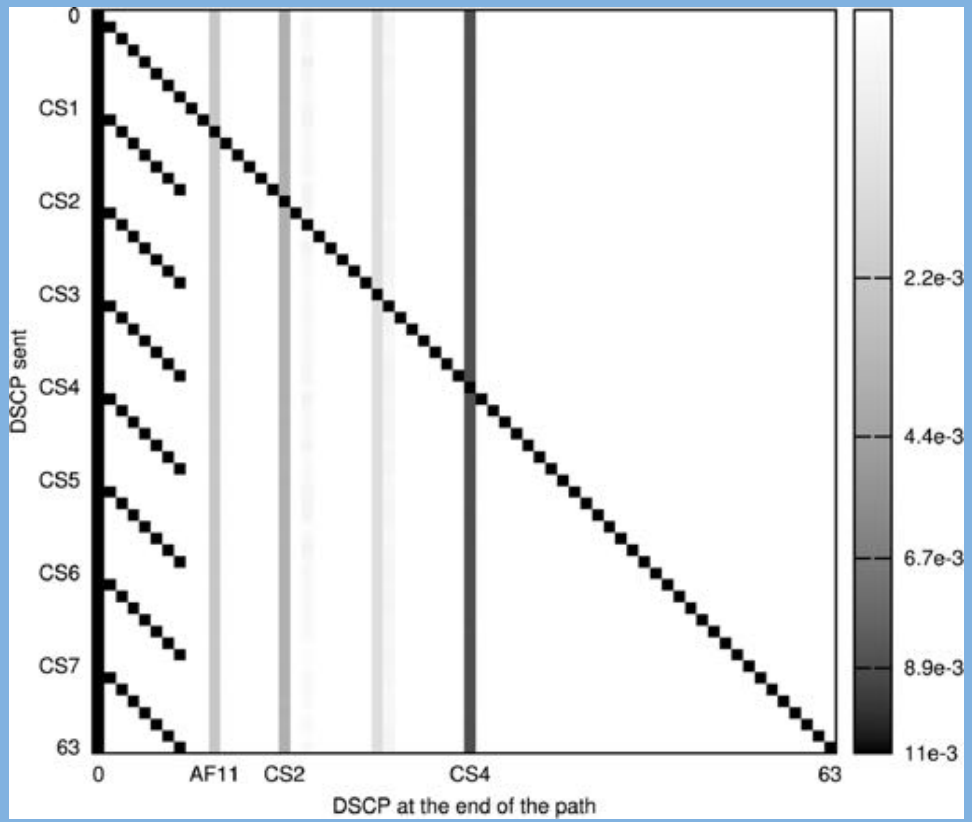
- Explicit Sender-to-Path Signaling
- Explicit Path-to-Sender Signaling

Transport / Network Signaling Mechanisms: Explicit Sender-to-Path Signaling

- Differentiated Services Code Point (DSCP)
- ACME STAR
- The LoLa Signaling Mechanism
- Explicit Support for Passive Latency Measurement in QUIC

Explicit Sender-to-Path Signaling: Differentiated Services Code Point (DSCP)

Problem; contribution; inputs



Explicit Sender-to-Path Signaling: ACME STAR

Small words only?

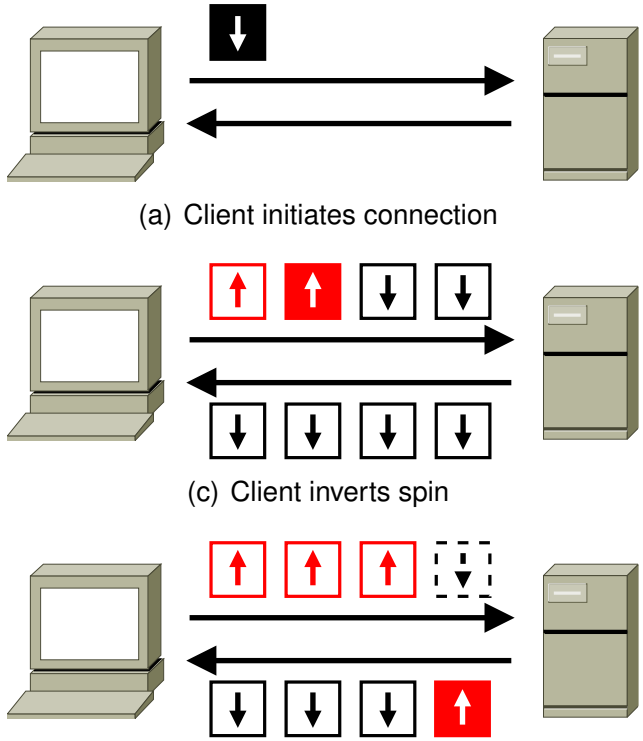
draft-mavrogiannopoulos-tls-cid

draft-ietf-acme-star *(adopted)*

Explicit Sender-to-Path Signaling: The LoLa Signaling Mechanism

- Low Latency Low Loss Tradeoff
- draft-you-tsvwg-latency-loss-tradeoff (expired)
-

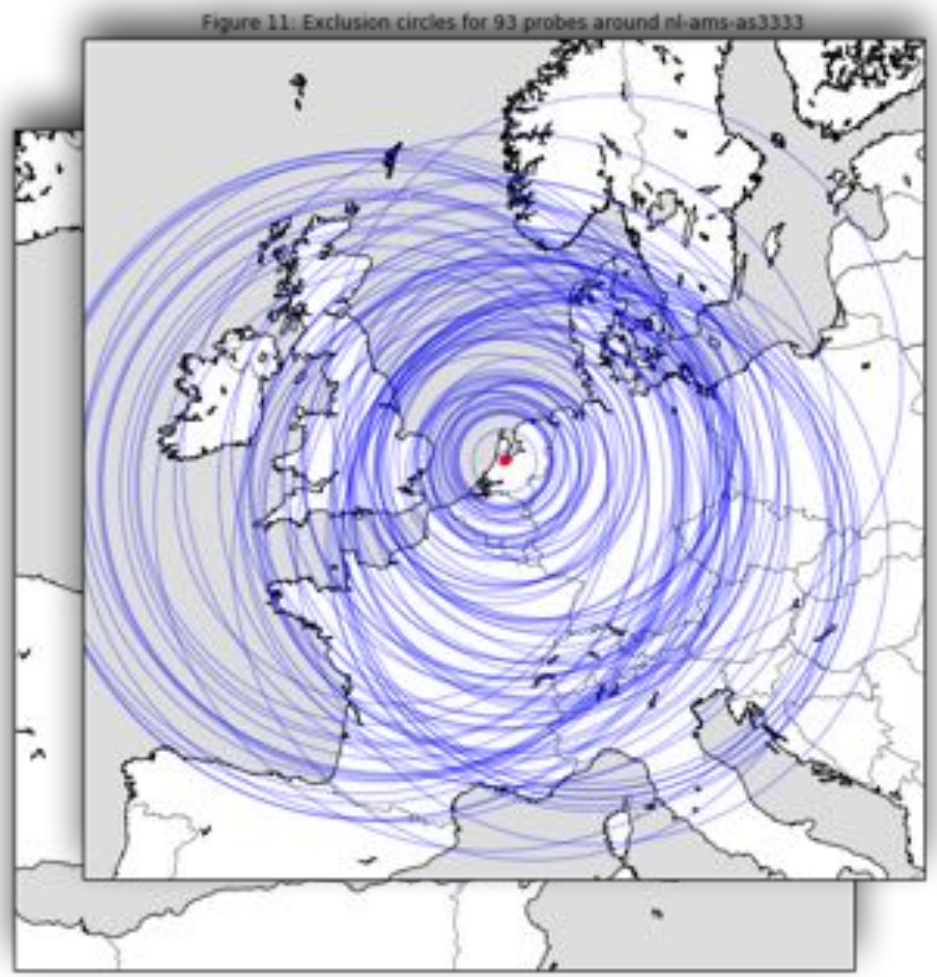
Explicit Sender-to-Path Signaling: Passive Latency Measurement in QUIC



- Extensions to QUIC wire image to support measurability
- In-network support for supporting network operations
- In-network support for managing low latency

Is RTT exposure to the path a threat to geoprivacy?

No.



- min(rtt) from Atlas anchoring measurements, fiber lightspeed assumption

SPIN in QUIC

IETF Contributions

- draft-trammell-privsec-defeating-tcpip-meta *(expired)*
- RTT exposure privacy analysis to QUIC RTT design team: github.com/britram/trilateration
- draft-trammell-quic-spin-03 (see below)
- draft-trammell-ippm-spin *(active)*

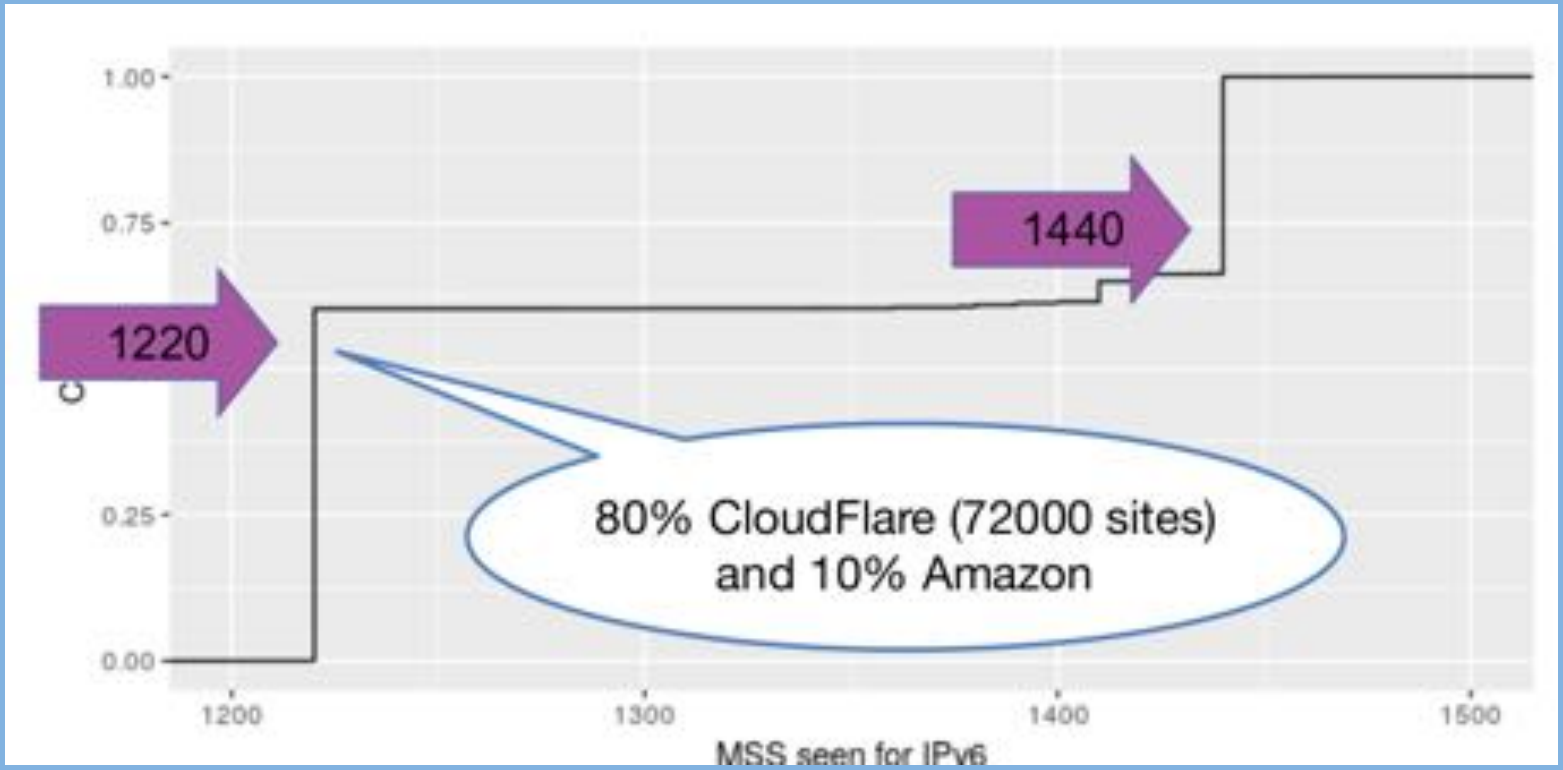
Simple extension to QUIC adopted for QUIC v 1

Transport / Network Signaling Mechanisms: Explicit Path-to-Sender Signaling

- The TCP MTU
- The Datagram PLPMTUD Mechanism
- Explicit Congestion Signaling
- Explicit Capacity Signals

Explicit Path-to-Sender Signaling: The TCP MTU

- Problem
-



Explicit Path-to-Sender Signaling: Datagram PLPMTUD

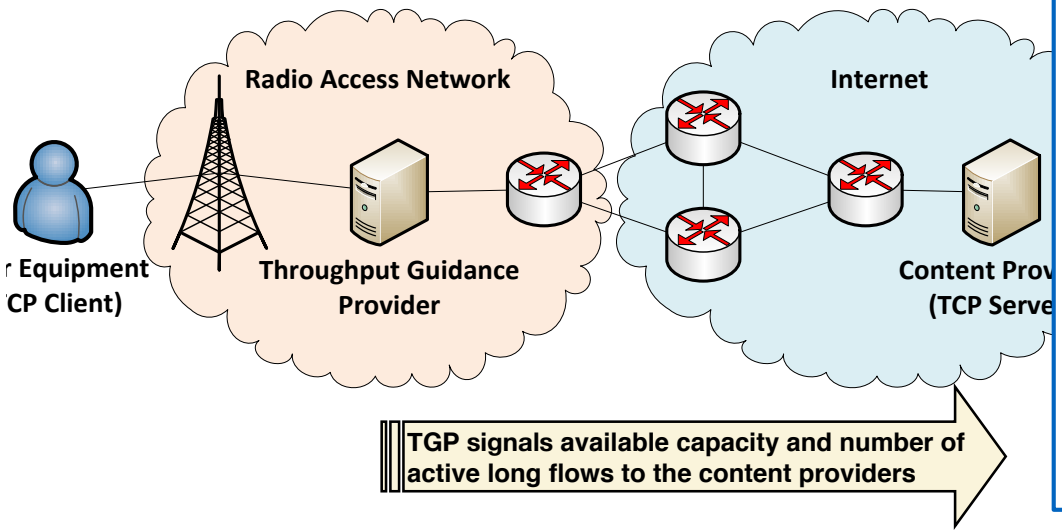
- draft-ietf-tsvwg-datagram-plpmtud (expected to be standardised in 2019)
-

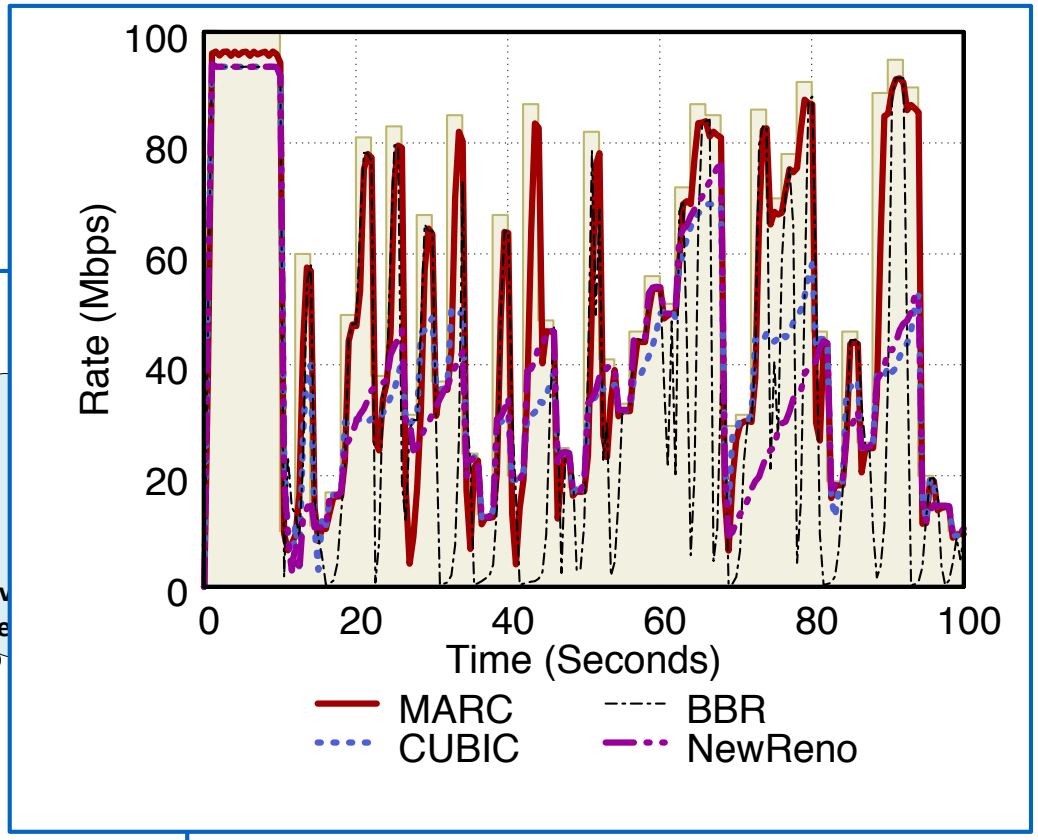
Explicit Path-to-Sender Signaling: Explicit Congestion Signaling

Contribution to QUIC RTT design team

Explicit Path-to-Sender Signaling: Explicit Capacity Signals (MARC)

- Signal from mobile to endpoint





Threat and Trust Analysis & Manageability

Security and Privacy Analysis for MCP (in D3.2)

Workshops and dissemination

MAMI Management and Measurement Summit (M3S)

Invitation-only Industry workshop

Concrete examples of what is done today

Friday, March 16, 2018 in London

(https://mami-project.eu/index.php/events/mami-management-and-measurement-summit-m3s/)

MAMI Outputs

- 3 White papers (public access):
  - Challenges in Network Management with Encrypted Traffic Transport Encryption) (based on M3S)
  - Analysis and Consideration on Management of Encrypted Traffic
  - Security and Privacy Implications of Middlebox Cooperation Protocols

- IETF Informational Document
  - The Impact of Transport Header Confidentiality on Network Operation and Evolution of the Internet (draft-ietf-tsvwg-transport-expected to be published 2019)
  -

Summary of WP3 Achievements

- Dissemination to Industry and Academe

- WP3 has directly impacted standardization organizations
  - XX Contributions
  - Efforts to continue beyond end of project

-

- Brief Summary counts for Standards

Related WP3 scientific publications during the reporting period

- B. Trammell. On the suitability of rtt measurements for geolocation, Aug. 2017. https://github. com/britram/trilateration/blob/master/paper.ipynb.
- B.Trammell,E.Boschi,G.Procissi,C.Callegari,P.Dorfinger,andD.Schatzmann.Identifyingskype traffic in a large-scale flow data repository. In Proceedings of the Third International Conference on Traffic Monitoring and Analysis, TMA'11, pages 72–85, Berlin, Heidelberg, 2011. Springer-Verlag.
- B. Trammell, D. Gugelmann, and N. Brownlee. Inline Data Integrity Signals for Passive Measure- ment. In Proc. Sixth Int. Wksp. on Traffic Measurement and Analysis, London, England, April 2014.
- B. Trammell, C. Perkins, and M. Ku¨hlewind. Post sockets: Toward an evolvable network transport interface. In Proceedings of Networking 2017 Workshop on Future Internet Transport, Stockholm, Sweden, June 2017.
- B. Trammell, C. Perkins, and M. Ku¨hlewind. Post sockets: Toward an evolvable network transport interface. In Proceedings of Networking 2017 Workshop on Future Internet Transport, Stockholm, Sweden, June 2017.
- . A. Aranda, D. Lpez, and T. Fossati. Analysis and consideration on management of encrypted traffic. cs.NI arxiv:1812.04834, 2018.
- A. Custura, G. Fairhurst, and I. Learmonth. Exploring usable path mtu in the internet. In Network Traffic Measurement and Analysis Conference (TMA 2018), 2018.
- A. Custura, R. Secchi, and G. Fairhurst. Exploring dscp modification pathologies in the internet. Computer Communications, 127:86–94, 9 2018.
- G. Fairhurst, T. Jones, and R. Zullo. A Tale of Two Checksums, Nov. 2018. Presentation
- G. Fauirhurst, M. Khlewind, and D. R. Lopez. Measurement-based protocol design. In European Conference on Networks and Communications (EuCNC'2017), 2017.
- T. Fossati. Content classification. Technical Report Document No IG.01, rev 1.0, GSM Association (GSMA), 2018.
- T. Fossati, R. Muentener, S. Neuhaus, and B. Trammell. Security and privacy implications of mid- dlebox cooperation protocols. cs.NI arXiv:1812.05437, 2018. ETH TIK Technical Report 370.
- M. Kuehlwind, B. Trammell, G. Fairhurst, T. Jones, S. Neuhaus, R. Muentener, and T. Fossati. Middlebox cooperation protocol specification and analysis. Deliverable 3.2, Measurement and Ar- chitecture for a Middleboxed Internet (MAMI), March 2018.
- M. Ku¨hlewind, T. Bu¨hler, B. Trammell, R. Mu¨ntener, S. Neuhaus, and G. Fairhurst. A Path Layer for the Internet: Enabling Network Operations on Encrypted Protocols. In Proceedings of the International Conference on Network and Service Management (CNSM). IEEE, 201
- R. Secchi, A. Venne, and A. Custura. Measurements concerning the DSCP for a LE PHB , Aug. 2017. IETF 99.
- P. D. Vaere, T. Bhler, M. Khlewind, and B. Trammell. Three bits suffice: Explicit support for passive measurement of internet latency in quic and tcp. In Internet Measurement Conference (IMC) 2018, 2018.

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

Q&A

mami

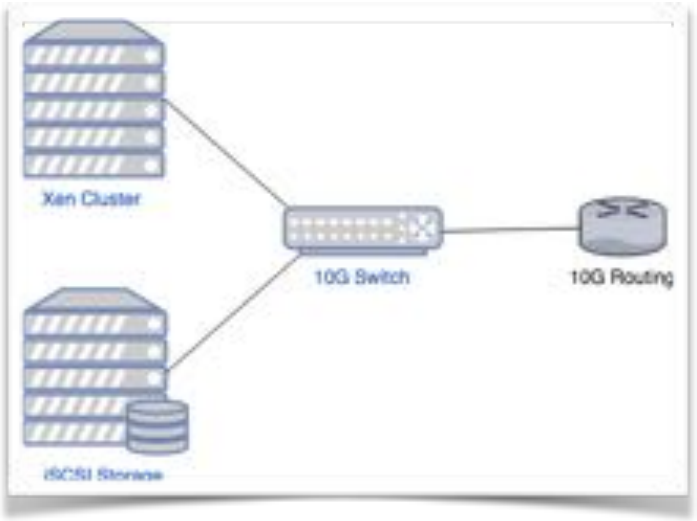
measurement and architecture for a middleboxed internet

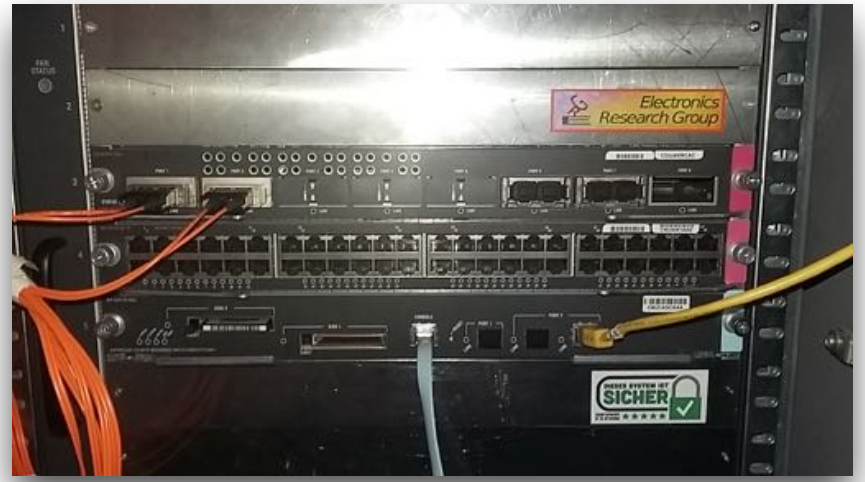
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688421.

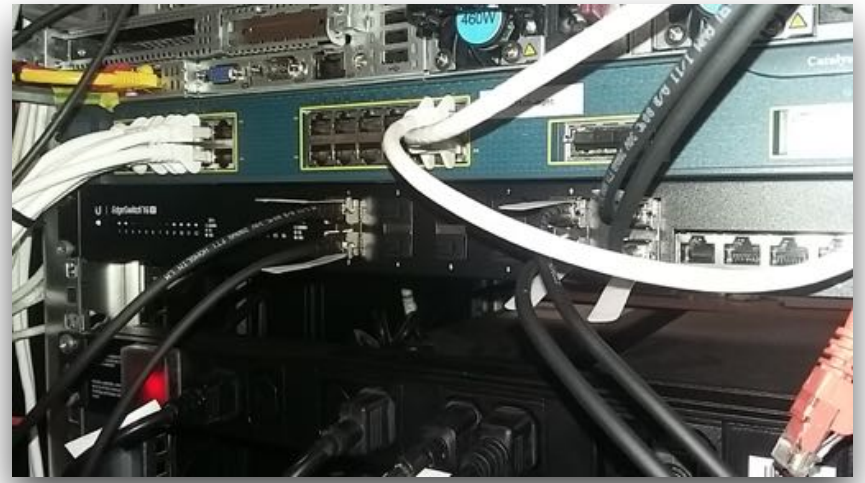
Spare Slides

May be used in this or other talks

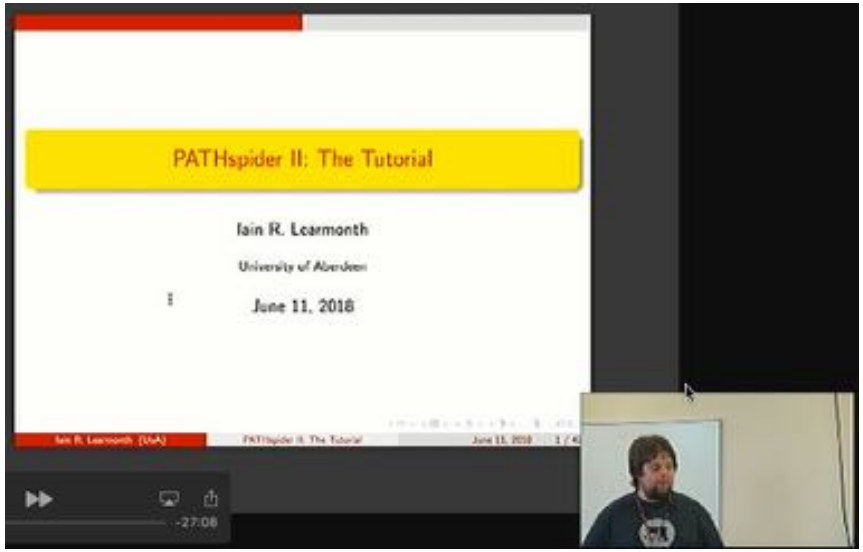
UoA MAMI Testbed Hardware

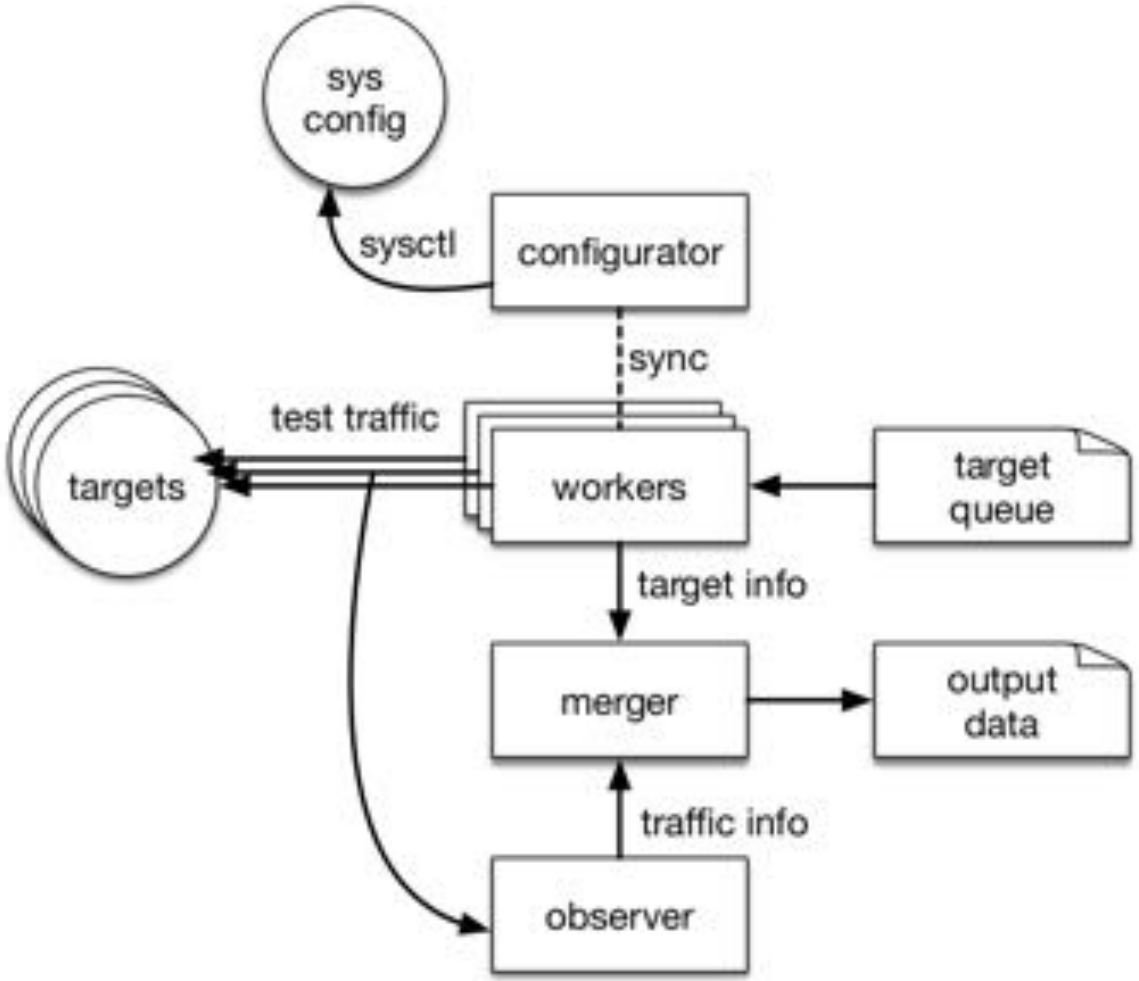






MAMI Summer SChool




sys
config
sysctl
configurator
sync
test traffic
targets
workers
target
queue
target info
merger
output
data
traffic info
observer