WP 3: Architecture: Middlebox Cooperation

Gorry Fairhurst

Brussels, October 21st 2016

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.

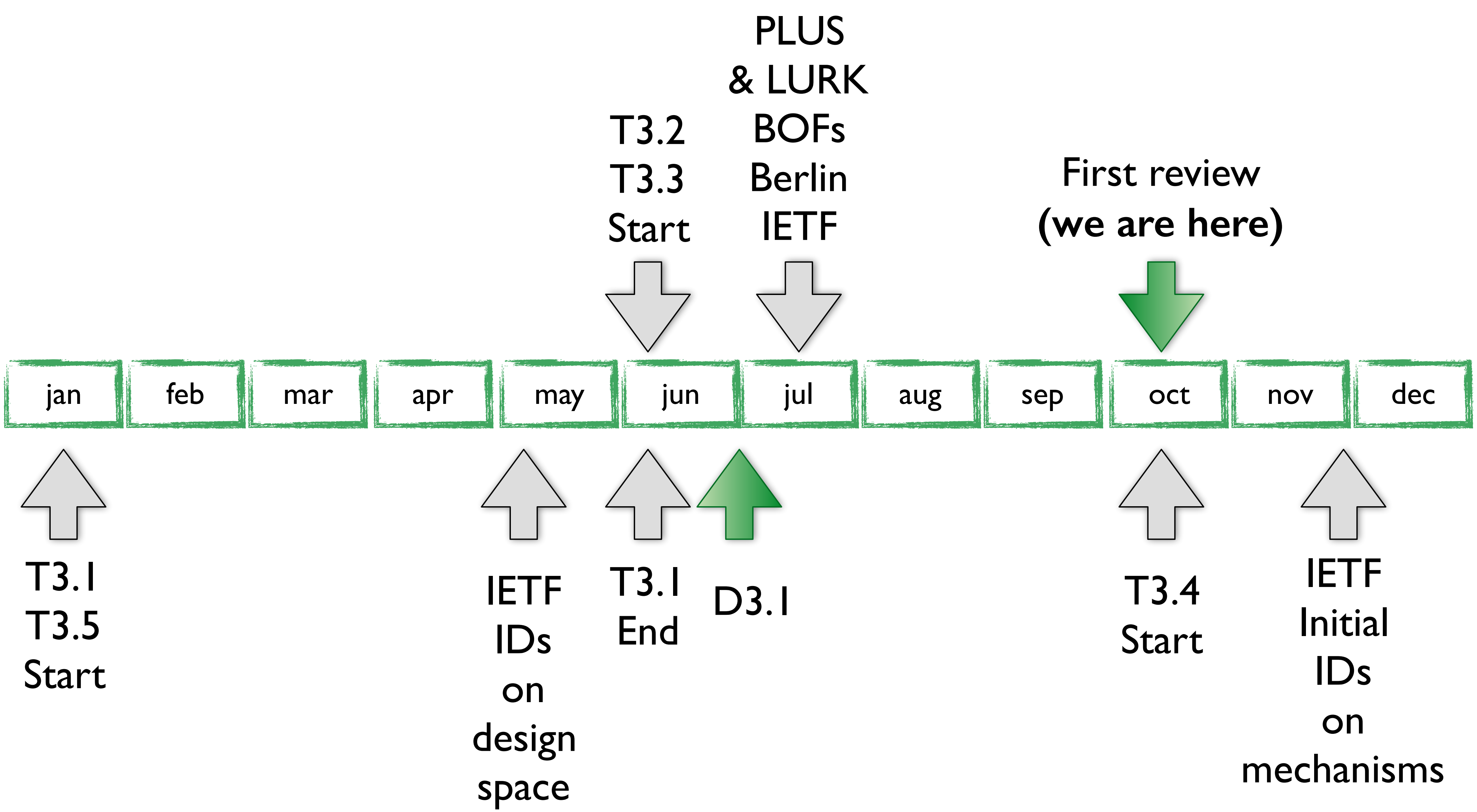
Agenda

- Overview
- Use Cases and Requirements
- Architecture & Implementations
- Security Analysis
- Next Steps for WP3
- Publications

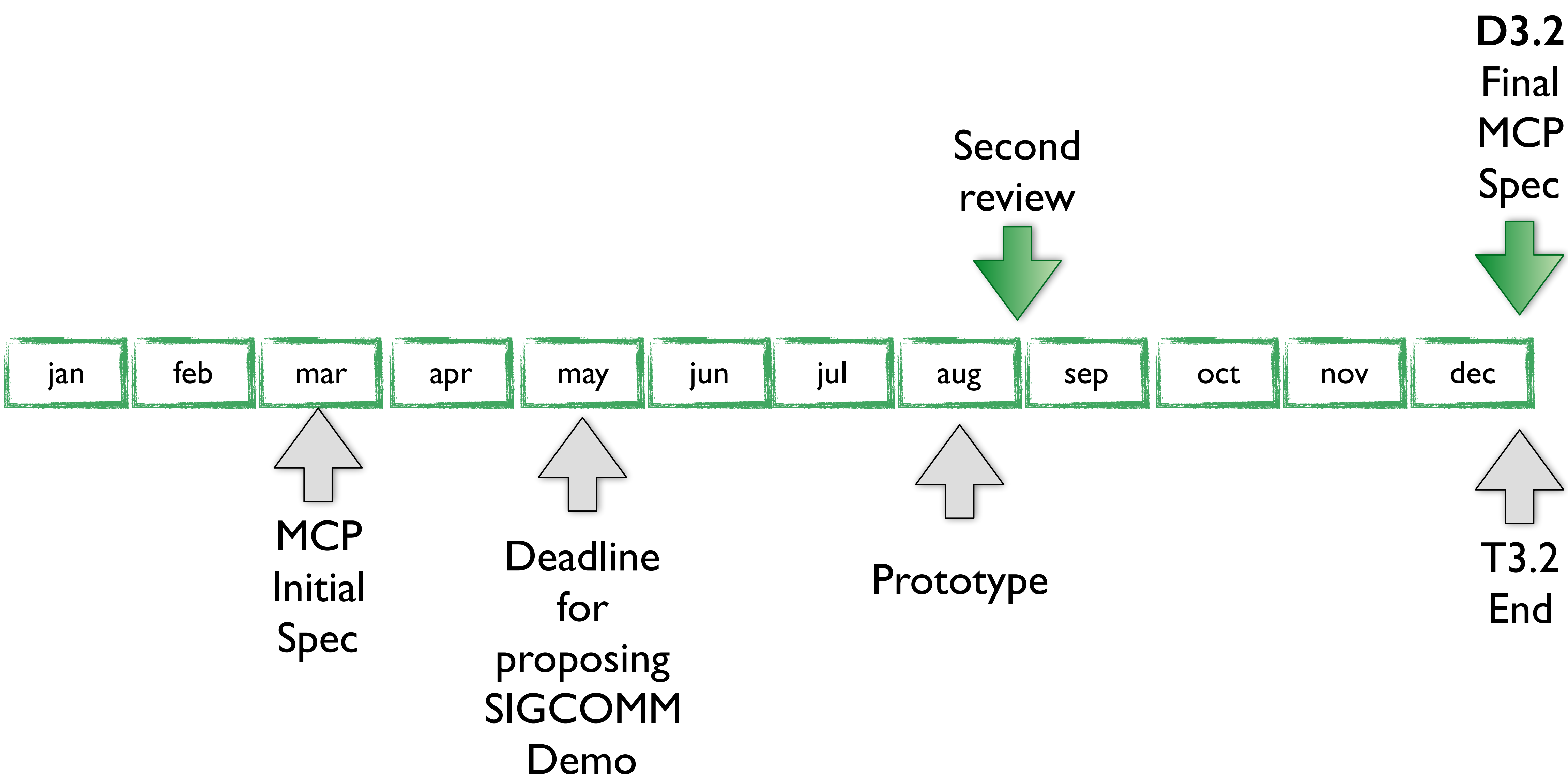
Overview for WP3

- Define ***use cases*** and requirements for architecture
    - Analysis of deployment restrictions
    - Incentives for middlebox cooperation
- Design, implement, and initial test of ***MCP***
- Design a ***flexible transport stack*** to complement MCP
- ***Threat and trust analysis*** of developed protocols

Overview - Timeline 2016 (Y1)



Overview - Timeline 2017 (Y2)



Overview: Who does what

		Done	On going			Ongoing
Partner	**MM**	**Task 3.1 Use Case and Requirements**	**Task 3.2 Design of MCP**	**Task 3.3 Flexible transport**	**Task 3.4 Implementation and Testing**	**Task 3.5 Threat and Trust Analysis**
1. ETH	18	✓	✓	✓	✓	
2. TID	10	✓	✓	✓		
4. UoA	12	-	✓	✓	✓	
5. ZHAW	18	✓		✓	✓	✓
7. ALU	10	✓	-	✓	✓	✓

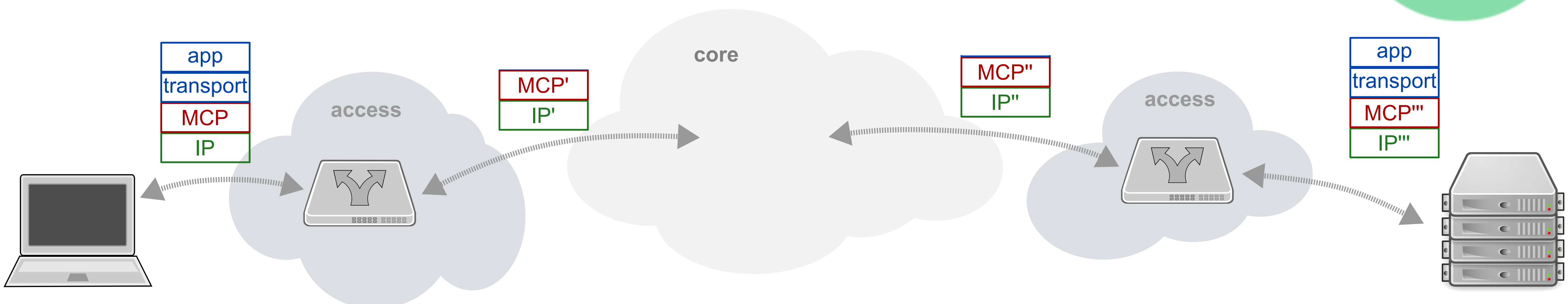
- Overview
- Use Cases and Requirements
- Architecture & Implementations
- Security Analysis
- Next Steps for WP3
- Publications

Task 3.1
Use Case Analysis and Requirement Definition

- Derives requirement for the protocol design of MCP
  - Derives protocol extensions to support deployment
  - Identify and coordinate with relating standards activities
- Analysis of the 4 use cases for MCP

- D3.1 is the final outcome of Task 3.1

MCP Design Requirements



- ***Endpoint control*** over cooperation with a clear ***boundary*** between what the path can see and what it cannot, enforced by encryption
- A design that ***deploys*** on the endpoints from day zero
- ***No required trust relationship*** needed between endpoints and middleboxes

Use cases developed in D3.1

1. Low Latency Support in Mobile Access Networks
2. Throughput Guidance for Congestion Management in Mobile Networks
3. Web Identity Translation (WIT) as a Network Service
4. Multipath Bonding of Mobile and Fixed Network Capacity

1. Low Latency Support in Mobile Access Networks

- **Varying traffic characteristics**: voice, web, messaging, streaming,
  e.g. WebRTC: streams with different characteristics and requirements
- 3GPP networks classify traffic to select appropriate ***bearer for each flow***
  Assumption: 5-tuple represents a single flow with QoS attributes
- ***Opportunistic encryption*** does not provide a proper bearer identification
  Lack of information to perform classification translates into a degradation of mobile network stability and a poorer service to users

Information Exposed

- Declarative signaling of trade-off bt. latency-sensitivity vs. loss-sensitivity
- Indication of maximum acceptable single-hop queueing delay per tube

2. Throughput Guidance for Congestion Management in Mobile Networks

- ***Application-limited, adaptive traffic*** (e.g. streaming video) vs. bandwidth probing
- ***Mobile network knows RAN bandwidth available*** and hence can predict capacity available to any user's mobile device

Information Exposed

- Maximum capacity available to a tube, e.g. similar to QuickStart
- Explicit per-tube indication of the maximum intended data rate

3. Web Identity Translation (WIT) as a Network Service

- Ad agencies' trackers enable a ***free-to-use*** model of web
- Web Identity Translation (WIT) service proxy between users and web-sites, intercepts tracking cookie (in encrypted traffic):

  When a particular user's browsing habits start making her uniquely identifiable, WIT intervenes via private-to-public cookie mappings to restore anonymity in Online Behavioral Advertising (OBA) ecosystem.

Information Exposed

- Visited domains: this data allows building user history vectors
- Cookies: WIT requires cookie access to strip them off during quarantine and manipulate them to allow intervention

4. Multipath Bonding of Mobile and Fixed Network Capacity

- ***Aggregate fixed and mobile capacity***, especially in areas with marginal fixed connectivity, e.g. using MPTCP proxies
- Layer 3 Multipath bonding can handle all traffic (not only TCP) but needs to ***re-order at proxy egress***
- Likely that new protocols will be be (more) robust to re-ordering

Information Exposed

- Reordering sensitivity as a per-tube signal
- Policy indications to the scheduler about which channel is preferred for which tube or packet

Requirements Derived from the Use Cases and Principles

- **1 Grouping of Packets and Bidirectionally**
- **2 Signaling Per-Tube Properties**
  - 3 Path to Receiver Signaling under Sender Control
  - 4 Receiver to Sender Feedback
  - 5 Path to Sender Signaling
  - 6 Tube Start and End Signaling
- **7 Additional Per-Packet Signaling & Declarative signaling**
- **8,9 Extensibility and Common Vocabulary**
- **10,11,12 Privacy, Authentication & Integrity**
- **13 Encrypted Feedback**

- Overview
- Use Cases and Requirements
- **Architecture & Implementations**
- Security Analysis
- Next Steps for WP3
- Publications

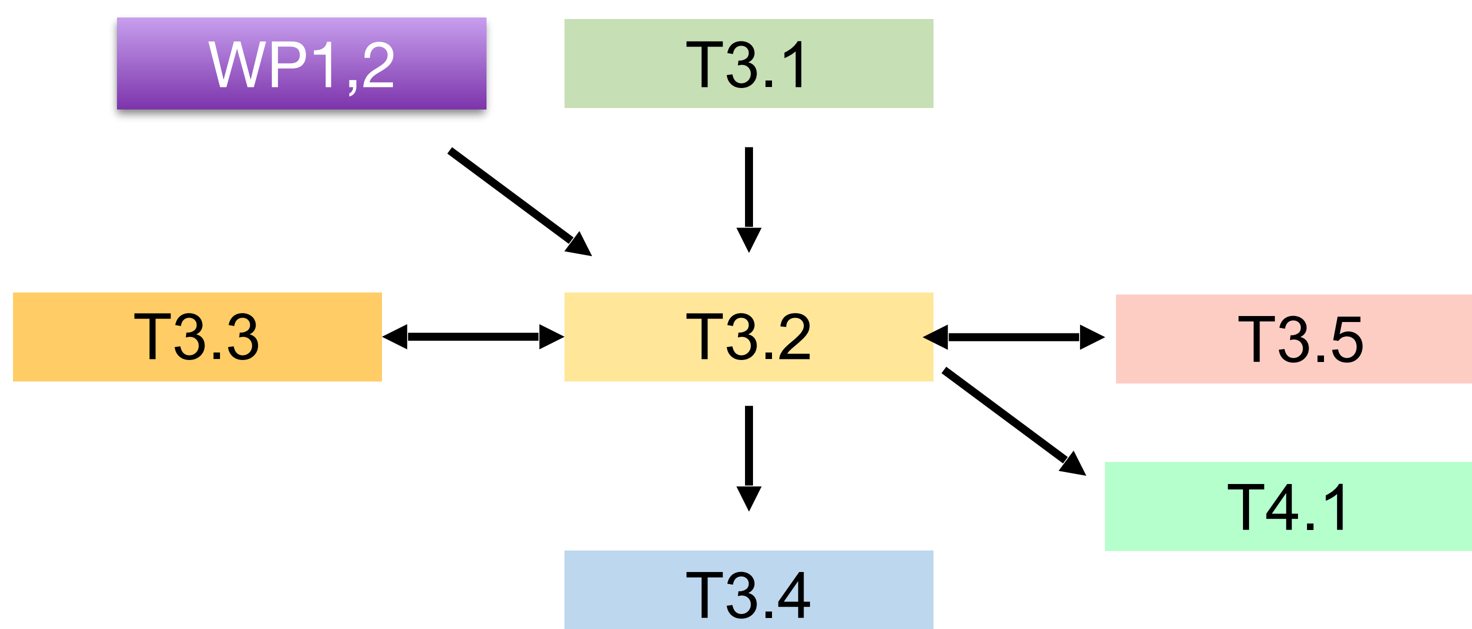
Requirements Related by Use Case

Principle	1	2	3	4	5	6	7	8	9	10	11	12	13
1. Low Latency Support	X	X					X	X					
2. Throughput Guidance	X	X	X	X	X			X				X	X
3. Web Identity Translation	X	X				X		X		X	X		
4. Multipath Bonding	X	X					X	X					

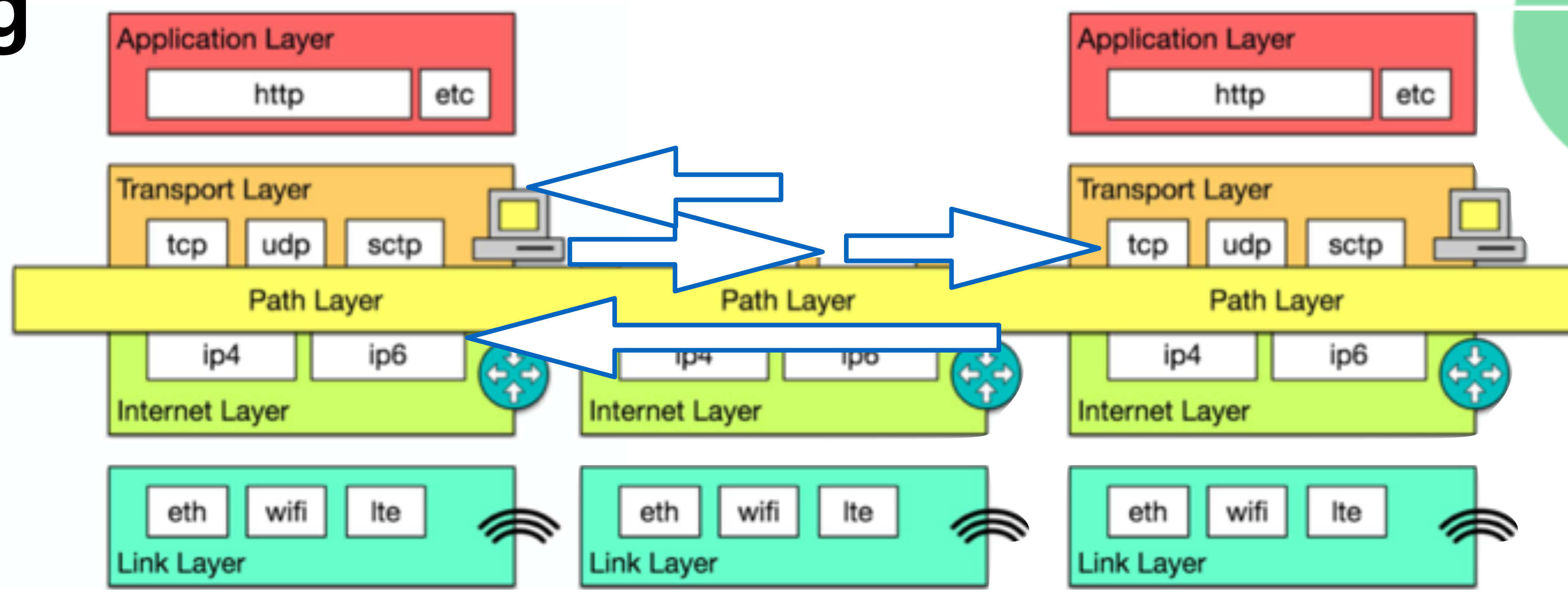
1= Tube; 2= Sig prop; 3= Path to recv; 4= Recv to send; 5= Path to sender; 6= Tube start; 7= Per packet sig; 8= Declarative signalling; 9= Extensibility; 10= Privacy; 11= Authentication; 12= Integrity; 13= Encrypted feedback

T3.2: Design of the MCP *- Started m7*

- Input from T3.1, WP1,2 (and coexists with T3.3 and T3.5)
- Design a protocol for applications and on-path devices to selectively expose information about traffic and the environment without requiring access to the payload
- Feeds T3.4 to implement, and T4.1 to standardise



Signaling



- **Sender – Path Signaling**
  - Enable ubiquitous deployment of ***encrypted higher layer protocols*** by exposure of basic TCP-like semantics to devices.
  - Applications and transport can ***explicitly provide limited information to devices on path***
- **Path – Receiver Signaling & Path – Sender Signaling**
  - ***Information about the path*** to receiving endpoints

draft-trammell-plus-abstract-mechanisms

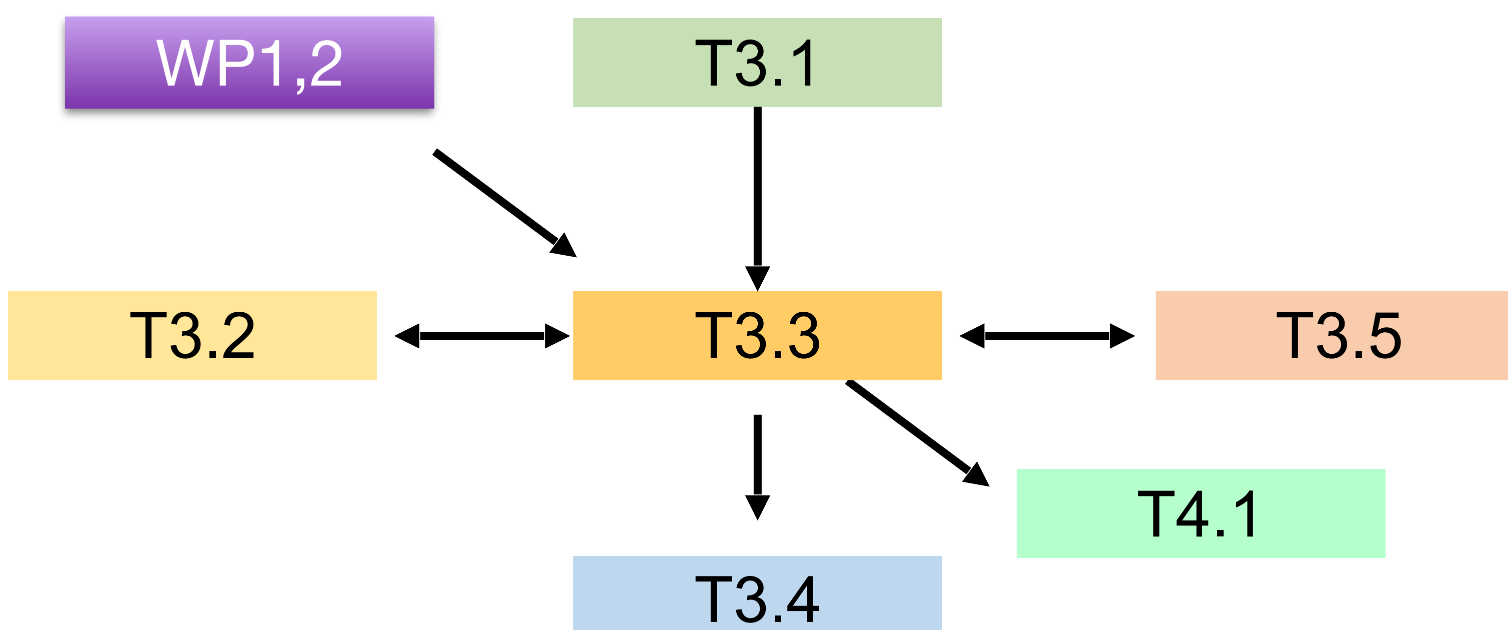
Path Layer UDP Substrate BOF at IETF-96, Berlin, July 22nd 2016

- 238 Attendees at meeting for 2.5 hours
- Presentation of concept of MCP
- In-depth discussion of security-related topics
- Input to IETF decision on how to standardise

draft-trammell-spud-req
draft-kuehlewind-spud-use-cases

T3.3: Design of a Flexible Transport Layer (FTL) *- Started m7*

- Input from T3.1 and WP1,2 (and coexist with T3.2, T3.5)
- Research candidate transport mechanisms
- Propose mechanisms to complement the core MCP
- Feeds T3.4 to implement, and T4.1 to standardise

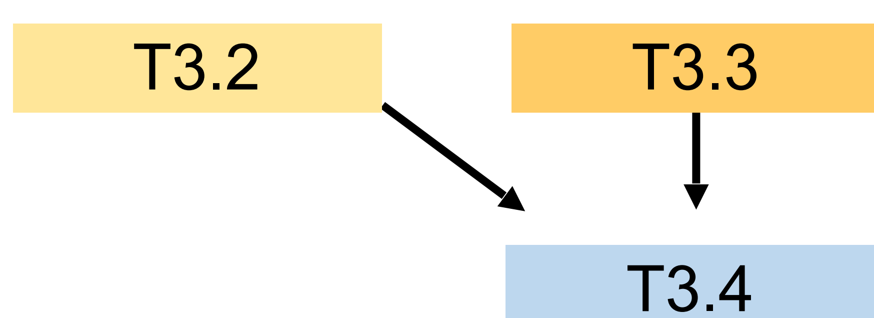


A flexible cooperative transport layer

- How quickly can MCP discover cooperating middleboxes along the path?
- What to do when middleboxes do not cooperate?
- How does the endpoint react when middleboxes mangle headers despite an expressed wish that they shouldn’t?

T3.4: Implementation and Testing
- (just) started m9

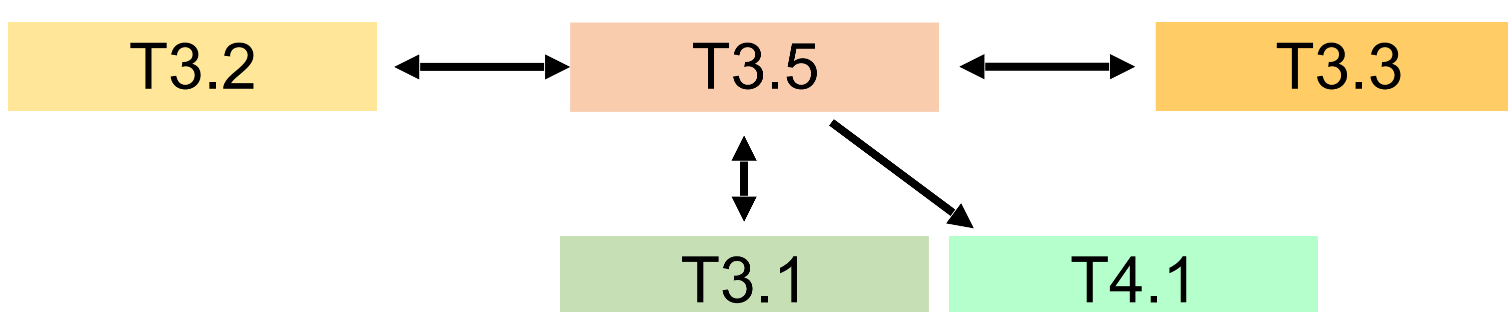
- Based on design in T3.2 and T3.3
- Cooperation with WP1 and WP2 based on measurements
- Endpoint and middlebox MCP implementation of protocols and protocol extensions
- Middlebox reference implementation for an NFV development platform.



- Overview
- Use Cases and Requirements
- Architecture & Implementations
- **Security Analysis**
- Next Steps for WP3
- Publications

Task 3.5 Threat and Trust Analysis for Middlebox Cooperation - Started

- Coexists with T3.2, T3.3
- Developing a threat model to investigate confidentiality, integrity, authentication and trust issues
- Exploring security mechanisms and their applicability
- Providing input to T3.1, and T4.1



Attacker Model

- Can sniff any packet from any source
- Can combine different flows from different sources
- Can arbitrarily inject traffic
- Can not subvert authentication schemes
- Collusion is a problem
  - Exposing different metadata to different MBs is nice…
  - …in theory; but in practice, it matters little
  - “I did not expose data to Middlebox *x*” means little if *x* can learn the data from someone else

Trust Model

- Trust implies authentication
- The more trust relationships exist, the harder the system is to run securely, so fewer trust relationships are better
  - **No trust**
    - Data is advisory only, can be manipulated by anyone
  - **Middlebox authentication**
    - Probably implies PKI or something similar
    - Allows selective exposure, but bad MBs can still collude

- Overview
- Use Cases and Requirements
- Architecture & Implementations
- Security Analysis
- **Next Steps for WP3**
- Publications

Next steps for WP3

- Initial design
  - Define abstract mechanisms
    - draft-trammell-plus-abstract-mechanisms
  - Define transport independent state machine for middleboxes
    - draft-trammell-plus-statefulness
- Framing format (target Mar 2017)
- Experience from WP1 and WP2 (usability of UDP, July 2017)
- Experimentation with prototype (target Aug 2017)
- Red team analysis of (MS8) for Aug 2017

- D3.2 “Middlebox Cooperation Protocol Specification” for Dec 2017

- Overview
- Use Cases and Requirements
- Architecture & Implementations
- Security Analysis
- Next Steps for WP3
- **Publications**

Dissemination

- **Publications (preparation by MAMI team)**
  - *EFGH,* ACM Hot Middlebox, London, Aug 2015.
  - *Multi-Context TLS (mcTLS),* ACM Sigcomm, London, Aug 2015.
  - B Trammell M Kuehlewind and E Gubser and J Hildebrand, *A New Transport Encapsulation for Middlebox Cooperation* IEEE Conf on Standards for Communications and Networking, Tokyo, Japan, Oct 2015.
- **Publications (relating to WP3 during MAMI project)**
  - M Kühlewin, B Trammell, *Middlebox Measurement and Cooperation,* CleanSky Conference, Heidelberg, Germany, Feb 2016.
  - M Kühlewind, B Trammell, J Hildebrand, *A Vision for Explicit Path-Cooperative Transport,* Conference on Innovations in Clouds, Internet and Networks (ICIN), Paris, France, Mar 2016.
  - M Bednarek, G Kobas, M Kühlewind, B Trammell, *Multipath bonding at Layer 3,* Applied Network Research Workshop (ANRW), ACM, Jul 2016.
  - S Liénardy, B Donnet, *Towards a Multipath TCP Aware Load Balancer,* Applied Network Research Workshop (ANRW), ACM, Jul 2016.

Standards activities (at current time)

- **Internet Drafts**
  - draft-trammell-stackevo-explicit-coop
  - draft-trammell-spud-req
  - draft-kuehlewind-spud-use-cases
  - draft-trammell-plus-statefulness
  - draft-trammell-plus-abstract-mechanisms
  - draft-nglt-lurk-tls-use-cases
  - draft-ietf-taps-transports-usage

- **Other relevant meetings**
  - ACCORD BOF, IETF BA, https://www.ietf.org/proceedings/95/accord.html
  - PLUS BOF, IETF Berlin, https://datatracker.ietf.org/meeting/96/agenda/plus/
  - LURK BOF, IETF Berlin, https://datatracker.ietf.org/meeting/96/agenda/lurk/

Main MAMI Achievements

1. Middlebox Measurements
   - Measurement tools available: Tracebox, PATHspider, copycat, Revelio
   - Published measurement results on ECN, TFO, DSCP, UDP, NAT, …
   - Path Transparency Observatory and public Web UI alive
   - **Next**: Large-scale measurement (on MONROE) and full integration of all measurement data in the PTO
2. Middlebox Modeling and Testing
   - Basic classification and initial modeling
   - **Next**: Longitudinal analysis of middleboxes behavior and model-based testing
3. Middlebox Cooperation Architecture
   - Use cases, requirements and initial security analysis completed
   - Abstract mechanisms and modeling of middlebox states
   - **Next**: Framing format and prototype implementation