# Overview:
# The MAMI project

Mirja Kühlewind

Oct 21, 2016

Technical Review Meeting - Brussels

mami

measurement and architecture for a middleboxed internet

measurement | architecture | experimentation

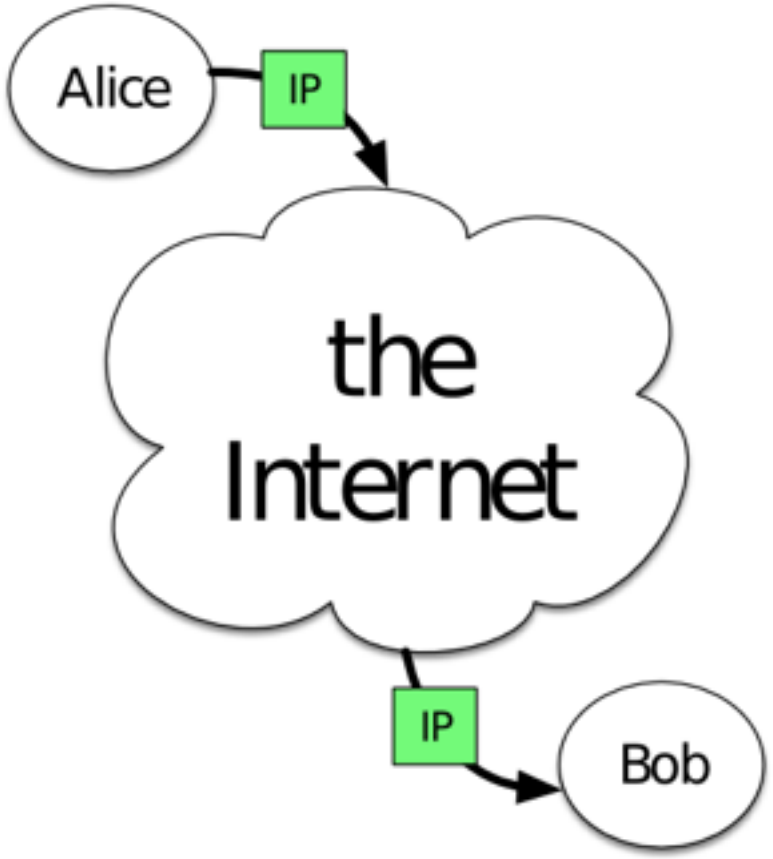
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688421.The opinions expressed and arguments employed reflect only the authors' view. The European Commission is not responsible for any use that may be made of that information.

Supported by the Swiss State Secretariat for Education, Research and Innovation under contract number 15.0268. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government.

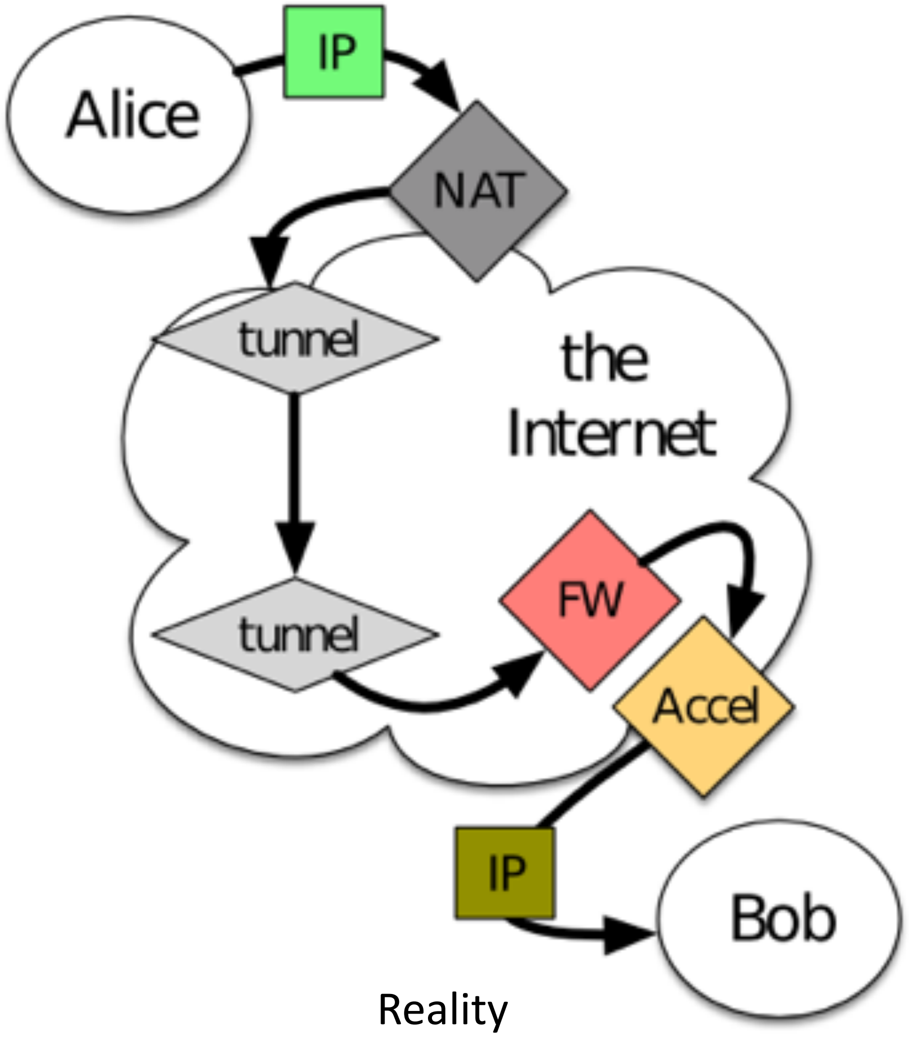
# Packet Mangling in the Internet

Middleboxes make restrictive, implicit assumptions about traffic passing through them

➡ Deployment of "new" protocols/extension limited



End-to-end view



Reality

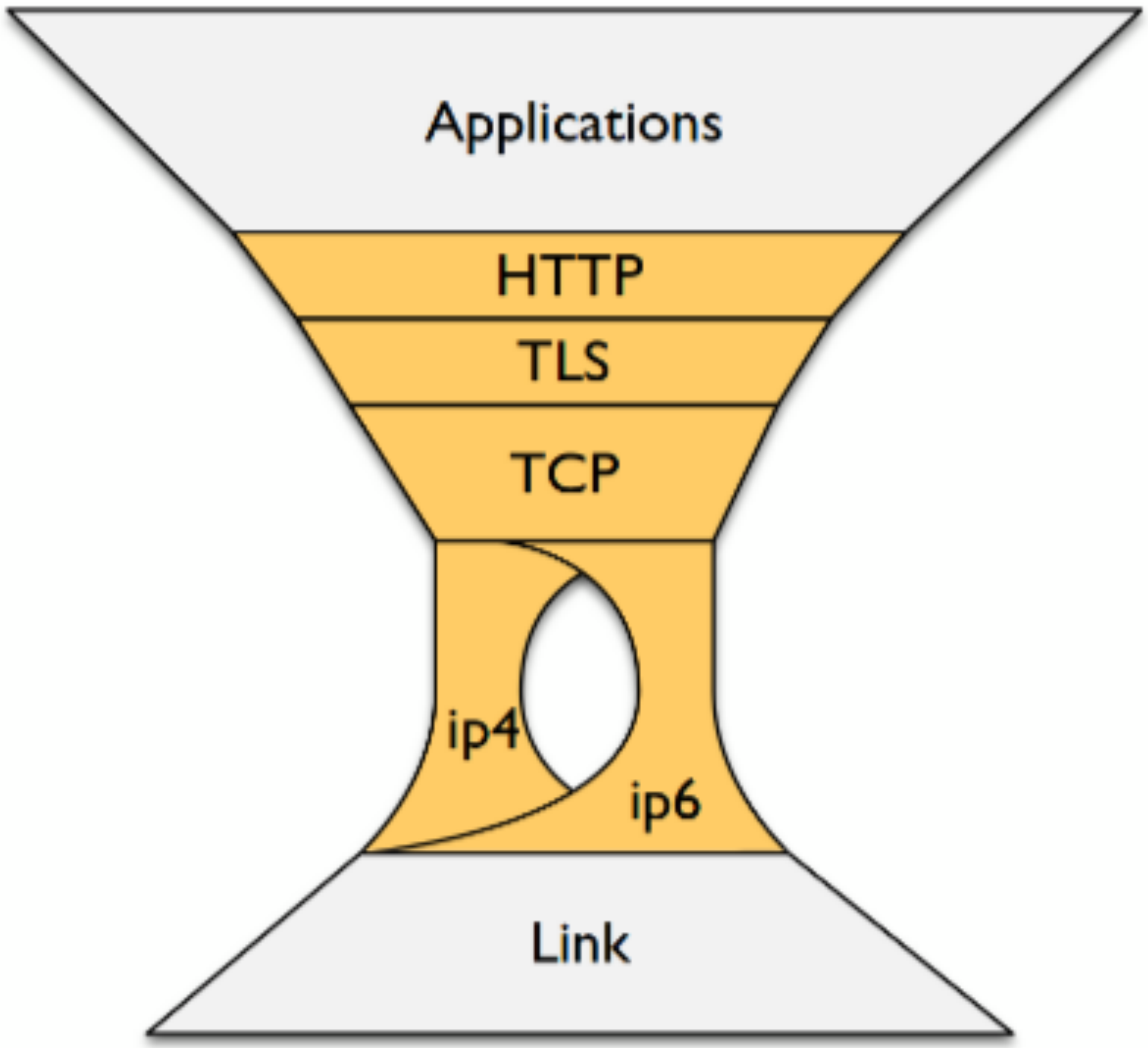
**Goal**: Reduce the *accidental manipulation* to zero, while minimizing the *essential manipulation*!

# Ossification and Encryption

- Are all applications forced to use the same protocol(s)?
  - HTTP (on TLS) on TCP

**OR**

- Large-scale encryption to restore of the e2e principle?
  - But some in-network function are needed to make the Internet manageable and viable



# MAMI Goal and Approach

**Goal**

Enable **innovation in network protocols** and the provision of **in-network functionality in a cooperative way** while preserving privacy by ***encryption***!

**Needed**

1. More data about the nature and distribution of middlebox impairments

   ➡ ***Common data model*** for storage and analysis of middlebox impairment

2. Explicit Middlebox cooperation to declare assumptions and intentions independent of the used transport or higher-layer protocol

   ➡ New (UDP-based) ***transport encapsulation*** + in-band signaling

# MAMI Objectives

**measurement**
of deployed middleboxes

**architecture**
for middlebox cooperation

**experimentation**
of use case applicability and deployability

- Strong interaction with relevant standards organizations for impact on deployment
- FIRE testbed (MONROE) support for measurement as well as experimentation, especially on mobile broadband access networks

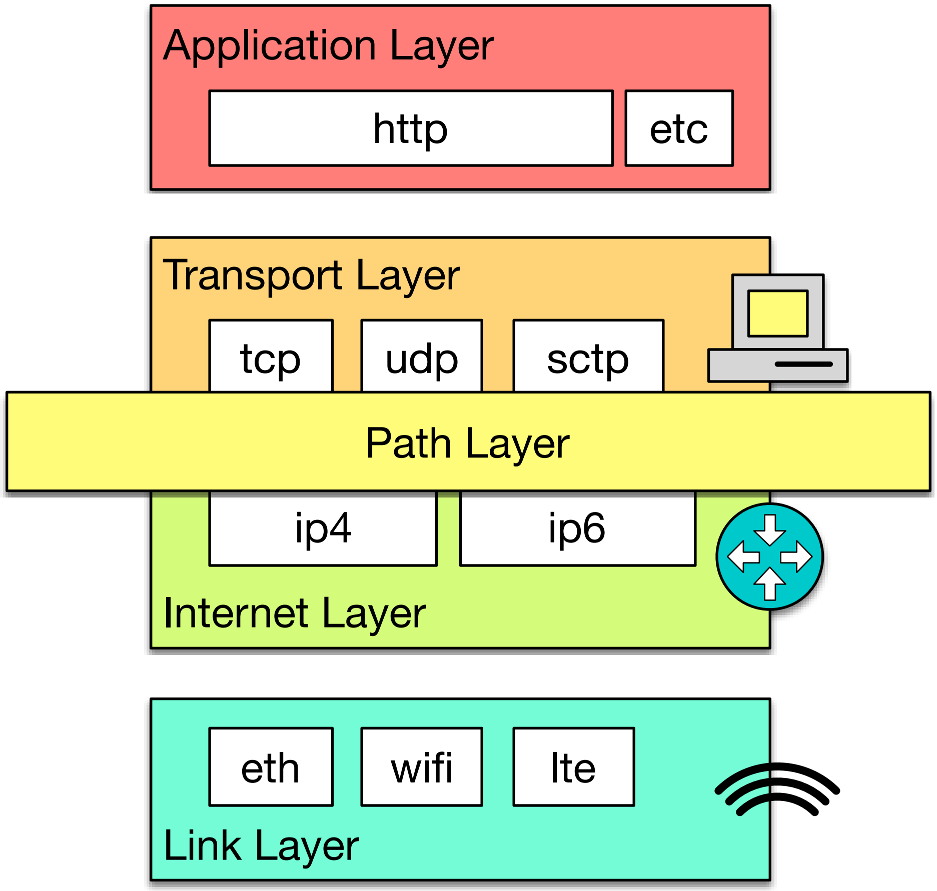
# Internet Path Transparency and Middlebox Impairments

- **Path transparency:** the likelihood a packet that arrives unmodified at the end of the path
- **Impairment:** something that keeps a path from being transparent for a certain kind of traffic, dependent on that traffic's characteristics, e.g.
  - Blocking: 100% packet loss
  - Differential treatment: Increased drop rate or latency
  - Bleaching/modification: removal or rewrite of header bits
  - Proxying: replacing one e2e path with two

# Mapping Manipulation in the Internet

1. **Large-scale measurements of path impairments**
   - using FIRE MONROE as well as RIPE Atlas, CAIDA Ark…
   - UDP/TCP/SCTP connectivity, TCP options (e.g. TFO, MPTCP), and other protocol (ICMP, DNS, …)
2. **Development of new measurements tools:** https://github.com/mami-project/
   - Tracebox: tracing + impairment analysis
   - PathSpider: A/B testing (currently on ECN support)
3. **Path Transparency Observatory**
   - Active measurements by the project + external measurements
   - Query interface to access observations on path impairments:
     - *What is the likelihood that a certain path impairment impacts my traffic* (modifications/stripping/dropping/blocking)?

# Why a new shim?



- Transport layer: end-to-end sockets
  - flow information
  - stateful and s g at the
- handling
  - rmation
  - ss and simple processing in the middle

Missing:
Per-flow information for stateful in-network functions

➡ **Path layer** for explicit cooperation with middleboxes instead of implicit assumptions

# Middlebox Cooperation

1. **Shim for Middlebox Cooperation Protocol (MCP)**
   - Transport and applications can selectively expose semantic information to middlebox
   - Higher layers can fully be encrypted
2. **Flexible Transport Layer (FTL)**
   - Maintain connectivity (even if the MCP is not supported) e.g. fallback or happy-eyeball mechanisms
   - Provision of encryption context for different layers/ protocols

# Middlebox Modeling and Testing

1. **Middelbox classification and modeling**
    - Understanding the key characteristics of middleboxes to develop a middlebox taxonomy based on measurements
    - Model-based approach for NFV-based testing
2. **Incremental deployability and testbed experimentation**
    - Handling uncooperative middleboxes
    - Evaluation of operational challenges in mobile networks (based on MONROE testbed)
3. **Applicability and evaluation of selected use cases**
    - Incentives for adaptation of the developed protocols and extensions

# Summary and Conclusion

**Problem**

Ossification of the Internet Protocol Stack

**Needed**

1. Measurement to identify path impairments
    - Large-scale using all available testbeds (incl. MONROE)
    - New measurements tools (Tracebox, PathSpider)
    - Path Transparency Observatory
2. Path layer for explicit middlebox cooperation
    - Middlebox Cooperation Protocol (MCP): trust by verify
    - Encrypted everything else!

3.Experimentation and Testing (in mobile networks)