Milestone 8

Brian Trammell (ETH)

MAMI Plenary Oslo, 4-5 July 2017

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.

What’s the question?

- MS8 in M20 (end August 2017):
  “Red team analysis of MCP and flexible transport layer; internal white paper release by ZHAW.”

- Intention: partially-independent security analysis of PLUS.

- Can this be made more useful?

Classes of threat against a middlebox cooperation protocol

- Overexposure: giving unintentional access to information in the header to devices on path.
- Traceability: allowing analysis of exposed information to aid in the identification of a flow's source device.
- Incorrectness: good old fashioned bugs in the implementation.
- The first two of these are attacks against a *vocabulary and data model,* and the latter actually isn't very interesting for a pilot implementation

Let’s talk about QUIC

- QUIC’s CID shares some applicability and semantics with the PLUS CAT; linkability is a concern here.
- QUIC probably won’t end up with a PSN/PSE mechanism, but other ways to expose latency are on the table.
- Thinking about ways to attack these mechanisms in general might be useful in both contexts.