MAMI Trust/Attacker Model

Thomas Fossati, Nokia

Stephan Neuhaus, ZHAW

Matteo Varvello, Telefonica

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.

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
    - Should noe contain PII in any case
  - Middlebox authentication
    - Probably implies PKI or something similar
    - Allows selective exposure, but bad MBs can still collude

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