D3.2

Mirja Kühlewind

Jan 30, 2018

5. MAMI Plenary Meeting, Cambridge, UK

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.

Deliverable 3.2

- Title:
  ~~Middlebox Cooperation Protocol (MPC) Specification~~
  Middlebox Cooperation Protocol Specification and Analysis
- Editor: ~~UoA~~ ETH
- Contributors: ETH (Mirja, Brian), UoA (Gorry), ZHAW (Stephan, Roman), Nokia (Thomas)
- Due date: M26 (Wed, Feb 28)

- https://gitlab.mami-project.eu/deliverables/D3.2

D3.2 Content

1. PLUS spec incl. abstract mech & statefulness (paper & drafts)
2. Applying middlebox cooperation mechanism to new and existing protocols (new text needed) !
   - QUIC RTT (spin bit, PN echo), DTLS conn ID, confirmation signal, Congestion Exposure (and ECN), LoLa DSCP, …
3. Security Analysis of Middlebox Cooperation protocols (red team analysis) ?
4. Post Sockets: A protocol-independent API for flexible deployment of new protocols such as PLUS ???

D3.2 ToC

1. Motivation
    - 1.1. Design Goals *(see paper but also need to be derived from requirements in D3.1)*
    - 1.2. ~~Statefulness~~ ***(here or 3.?)***
    - 1.3. Abstract Mechanisms *(from draft)*
    - 1.4. Use Case: Network Performance Measurement *(from paper)*
    - 1.5. ~~Related Work~~
2. Path Layer UDP Subtrate (PLUS) Specification *(from paper as more up-to-date than draft)*
    - 2.1. Basi~~c~~e Header
    - 2.2. ~~State Establishment and Maintenance~~ **(depends on statefullness~~)~~**
    - 2.3. Extended Header
    - 2.4. Extended Header Types
    - 2.5. Encrypted Feedback
    - 2.6. Transport layer API
3. ~~Insights from Implementation~~ **(move to conclusion and D3.3)**
4. ~~Deploying PLUS~~ **(move to conclusion and D3.3)**
3. Applying middlebox cooperation mechanism to new and existing protocols **(new! see next slide)**
4. Security Analysis of Middlebox Cooperation protocol **(red team analysis! see next slides)**
5. Post Sockets: A protocol-independent API for flexible deployment of new protocols **(optional? see next slides)**
6. Summary, Conclusion, and Outlook **(incl. deployment and implementation considerations?)**

D3.2 Chapter 3

3. Applying middlebox cooperation mechanism to new and existing protocols
   - 3.1. Protocol-independent State Management using Confirmation Signaling
     - Statefullness and PLUS state establishment *(from paper and evtl. draft)*
   - 3.2. Packet Group Binding using Connection ID
     - QUIC Managability and DTLS connID ***(Mirja and Thomas)***
   - 3.3. Latency Measurements
     - PN echo and Spin bit ***(Brian)***
   - 3.4. Congestion Measurements
     - ConEx and QUIC ***(Mirja)***
   - 3.5. Low Latency Support
     - LoLa DSCP ***(Thomas and Mirja)***
   - **3.6.** PMTU Discovery
     - Datagram PLPMTUD using UDP options ***(Tom)***
   - **3.7. Others?**

D3.2 Chapter 4

4. Security Analysis of Middlebox Cooperation protocols
   - 4.1. Attacker Model
   - 4.2. Data Exfiltration
   - 4.3. Data Manipulation
   - 4.4. Coercion
   - 4.5. Application Fingerprinting (Thomas)
   - 4.6. Localization
   - 4.7. Analysis and Comparison

➡ Approach: For each attack explain the general approach and discuss examples based on information in the PLUS header? *(Stephan?)*

D3.2 Chapter 5

5. Post Sockets: A protocol-independent API for flexible deployment of new protocols
    5.1. Overview and Concepts *(from FIT paper)*
        5.1.1. (Message) Carrier
        5.1.2. Message
        5.1.3. Transient
        5.1.4. Association
        5.1.5. Path
        5.1.6. Protocol Stack Instance (PSI)
    5.2. Using PLUS with Post Sockets ***(next text needed!)***
    - Use QUIC with fallback to TCP as example (~~maybe even with crypto-sep using ALNP and TLS over TCP to redirect to 0-RTT QUIC~~) ***(Brian?)***

➡Maybe discuss mechanism for racing and rendezvous (from FIT paper) in D3.3?

D3.2 ToDos

- Copy and paste paper and drafts (Mirja)
  - ➡ Deadline: Fri, Feb 9
- New intro and conclusion? (Mirja)
- New text for section 3: Brian, Thomas, others?
- Rewrite section 4: Stephan?
- Section 5.2: Brian?
  - ➡ Deadline: Wed, Feb 21
- Reviewer: Diego, maybe Gorry
  - ➡ Deadline: Mon, Feb 26

Outlook D3.3 and D2.2 Implementation reports

- D3.3: ~~MCP and Flexible Stack Implementation Report~~
  Middlebox Cooperation and Flexible Stack Implementation Report
- D3.2: Final Middlebox Model, Experimentation and Evaluation Report
- Proposal: D3.3 endpoint-focused & D2.2 in-network/middlebox-focused

Content D3.3 (ZHAW)

- PLUS implementation (Roman)
- Post Sockets/taps?
- QUIC (Piet/ETH)
- STAR/ACME
- AccECN?
- Multi-context encryption
- More…?

Content D2.2 (UoA)

- Middlebox simulator
- VPP Monitoring (Tobias)
- LoLa (use case 1 in D3.1)
- Throughput Guidance (use case 2)
- ~~Web Identity Translation (WIT) (use case 3)~~
- Multipath Bonding (use case 3)?
- Others…