This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688421.

PLUS Red Team Analysis

mami

measurement and architecture for a middleboxed internet

Situation

- PLUS development stuck in IETF
- It’s effectively dead
- Killed by concerns that having an official channel for exfiltration of metadata would be a disaster for privacy
- Idea: Why don’t we subject PLUS to an adversarial analysis where we look at the implications for privacy
- Hence the PLUS Red Team Analysis
- Lead by me (Stephan), contributions by (in alphabetical order) Brian, Gorry, Mirja, Roman, Stephan, and Thomas.

Document

- MAMI gitlab(!) in Deliverables/D3.3/PLUS-red-team.md
- 36k of text (hard to say how many lines with .md)
- Focus explicitly *not* on PLUS, but on *any* kind of middlebox cooperation protocol (MCP), or on any kind of MCP mechanism, even if it’s not embodied in a separate protocol
  - (e.g., some mechanisms invented for QUIC, like connection identifiers)
- Looked at *header fields*, *scratch space*, and *integrity protection*
- In the context of attacks that are *detectable* (or not) and *change protocol behaviour* (or not)

Some Specific Attacks Considered

- Brian’s investigation of using RTT for geolocation
  - TL;DR: doesn’t work. No, it *really* doesn’t work
- Coercion of scratch space (“put scratch space in your packets or we won’t route them”)
  - Very detectable, so undesirable for a mostly passive adversary
  - With active adversary, already possible
- Connection identifiers for linkability
  - Is indeed a problem, but privacy-preserving designs exist, e.g., draft-mavrogiannopoulos-tls-cid
- Compared to e.g. TCP hypercookies, no attack adds appreciably to what is possible today

Way Forward

- Option 1: Keep as MAMI-internal whitepaper
  - No further action needed, finalise document, then stop activity
- Option 2: Try to publish as a standalone paper
- Question: Which venue?
  - Usenix Security: Deadline 5 February, unlikely to be accepted, but possible
  - NDSS: `<cynical>`(Used to be) sponsored by NSA, they might like this`</cynical>` (but they can't influence the TPC)
    - NDSS 2018 deadline: 22 January, so would have to go for 2019
  - CCS/S&P: academic conferences, so unlikely to be accepted
    - CCS 2018 deadline: 19 May
    - S&P 2019(!) deadline: rolling

Way Forward (contd.)

- CCR
  - Technical paper acceptance rate *very* low (< 15%)
  - Editorial Note possible, but *not* peer-reviewed
  - Deadline: rolling
- MAMI blog post
  - Acceptance rate 100% :-)
  - No peer review, doesn’t reflect the work that went into the document

- Problem with publication is that it is a negative result, which will get rejections purely because of that (“we looked at this, and you know what, it’s not actually a problem!”)