CoAP Attacks

draft-mattsson-core-coap-attacks-02

John Preuß Mattsson

draft-mattsson-core-coap-attacks-02

- "CoAP Attacks" is an informational companion document to "CoAP: Echo, Request-Tag, and Token Processing"
  - Discusses security properties needed to secure CoAP
    - Data-to-data binding
    - Data-to-space binding
    - Data-to-time binding
  - Describes some attacks on CoAP
    - The Block Attack
    - The Request Delay Attack
    - The Response Delay and Mismatch Attack
    - The Request Fragment Rearrangement Attack
    - The Relay Attack
  - Describes some attacks using CoAP
    - Denial-of-Service Attacks / Amplification Attacks

- "CoAP: Echo, Request-Tag, and Token Processing" provides solutions to several of the attacks
  - Echo can be used against delay and denial-of-service attacks.
  - Request-Tag can be used against request fragment rearrangement attacks
  - Updated Token processing mitigates the response delay and mismatch attack

draft-mattsson-core-coap-attacks-02

- 02 addresses almost all received comments on -00 and -01.
  - A paragraph explaining freshness, replay protection, and sequence numbers has been added.
  - More references to the soon to be published RFC 9175 (Echo, Request-Tag, and Token Processing)
  - All RFC2119 terminology has been removed based on a comment from Carsten.
  - Added more details on which protocols are affected by the attacks and some practical difficulties based on comments from Achim.
  - Corrected text on OSCORE over TCP. It is TLS-like replay protection that mitigates the attack, not TCP.
  - Added a sentence on why misbinding attacks do not work on HTTPS.
  - Changed homeless/hitman/killed to something nicer based on Carsten' comment.
  - Smaller editorial changes (several based on comments from Carsten)

Current status and next steps

- "CoAP: Echo, Request-Tag, and Token Processing" is is AUTH48.
  - Issue #77 is being addressed in AUTH48, pending approval of the AD

- Conclusion at IETF 111 that denial-of-service and amplification attack requirements are best handled by writing a BCP. T2TRG has also started to discussed DoS and amplification attacks.

- We should publish CoAP Attacks as an informational document describing attacks as suggested by Security AD Benjamin Kaduk. First step would be WG adoption. I think the document is more then ready. It has been worked on since 2015.

(It is the only IETF document that talks about spacetime, wormholes, and gravitational time dilation :)