Amplification Attacks

draft-mattsson-t2trg-amplification-attacks

Changes in -02

— Updated references. Several references have been published as RFCs.

— Included some updated text from the T2TRG presentation.

— Changes definition of amplification factor to align with what is used in the examples (“received from attacker” instead of “sent from attacker”). In the case of intermediaries, this might differ on lower layers.

— Discussion of that amplification factor and bandwidth depend on the protocol layer that is used for the calculation (whole IP packets, UPD payloads, or CoAP payloads). [Based on comment from Achim]

Sultan Alshehri has expressed interest in simulating the amplification attacks.
https://github.com/EricssonResearch/coap-actuators/issues/17

Many New Comments Since -02

— Implementation for amplification attacks targeting CoAP
https://github.com/EricssonResearch/coap-actuators/issues/17

— Example for "amplification attack alone"?
https://github.com/EricssonResearch/coap-actuators/issues/19

— Creating resources
https://github.com/EricssonResearch/coap-actuators/issues/20

— Amplification Attacks using Observe
https://github.com/EricssonResearch/coap-actuators/issues/21

— MITM Amplification Attacks
https://github.com/EricssonResearch/coap-actuators/issues/22

— Adding proposals for mitigation?
https://github.com/EricssonResearch/coap-actuators/issues/23

Future of the Document

- Decide on the goal and scope of the document:
  - Raise awareness of IoT Amplification Attacks?
  - Suggest mitigations?
  - Non-amplification DDoS attacks?
  - Concrete information about actual attacks?
- Request for "newer or more concrete information about actual attacks" but the available information is not very concrete, and there is little new information. Maybe instead remove the section on actual attacks?
- Maybe make the document high-level less CoAP-focused. Maybe remove CoAP from title but keep CoAP in examples. The goal is not to make CoAP look bad.
- Research Group adoption?