Amplification Attacks

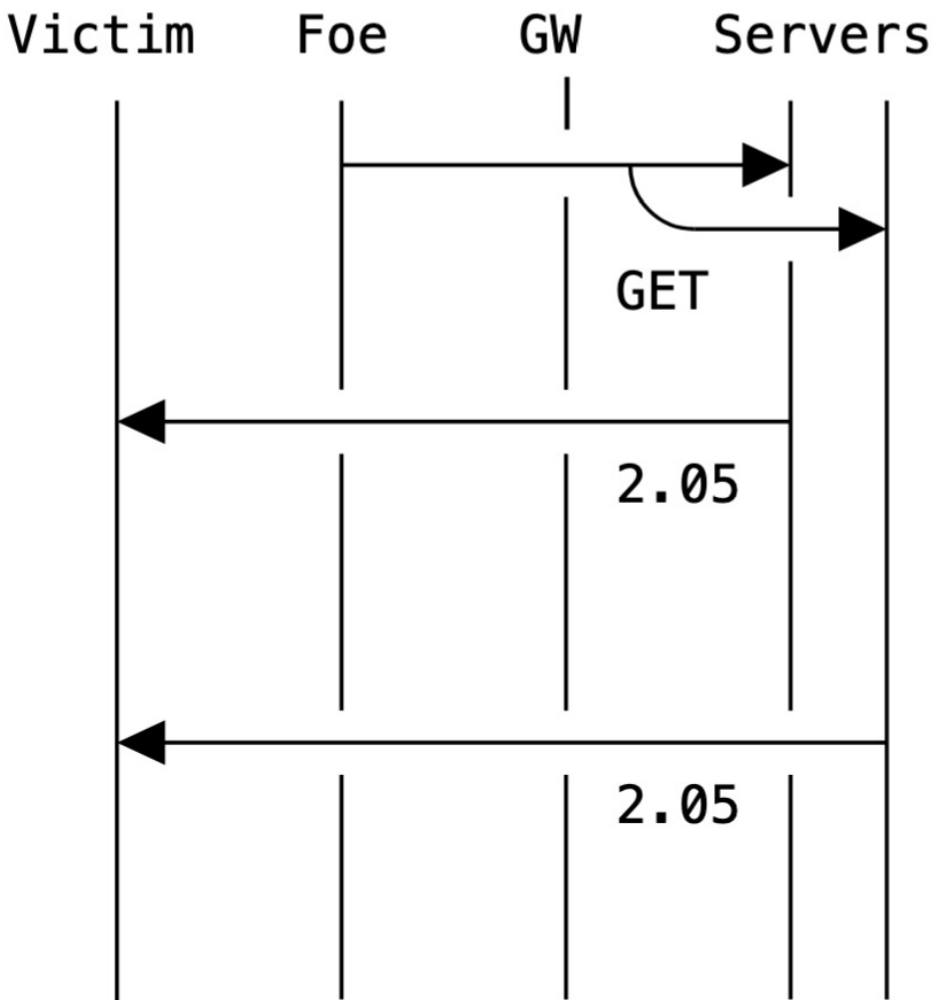
draft-irtf-t2trg-amplification-attacks

Changes in since draft-mattsson-02

Most changes based on comments from Achim Kraus and discussions with Sultan Alshehri

- Added a gateway in the multicast figures. Gateways are commonly discussed for CoAP group communication.
- Made a separate observe figure (not just observe and multicast combined).
- Added that the intent is not to suggest that CoAP is more vulnerable to amplification attacks than other protocols.
- Added that POST/PUT is only possible if supported. Server likely limits size.
- Added that conditional attributes are only possible if supported.
- Removed section on actual amplification attacks.
- Changed “client” to “victim” and “server” to “servers” in figures
- Added SVG figures with aasvg.
- Editorial changes

Changes in since mattsson-02




```
     Code: 0.01 (GET)
    Token: 0x44
Uri-Path: temperature

     Code: 2.05 (Content)
    Token: 0x44
  Observe: 217
  Payload: "301.2 K"

     Code: 2.05 (Content)
    Token: 0x44
  Observe: 363
  Payload: "293.4 K"
```

What is left to do

- Address two remaining comments from Achim Kraus regarding MITM attacks.
- 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?~~
- Proposed way forward is to add suggested mitigations for the currently described attacks and then publish. Currently described attacks:
  - Simple Amplification Attacks
  - Amplification Attacks using Observe
  - Amplification Attacks using Group Requests
  - MITM Amplification Attacks
- Any other views?

Mitigations

- **General**
  - Use a security protocol and/or use the ECHO option. Harden devices to prevent hacking.
- **Simple Amplification Attacks**
  - Limit the amplification factor. Rate limit.
- **Amplification Attacks using Observe**
  - Confirm the the subscriber is still interested
  - Limit the number of observations per client. Be careful with pmax attribute
- **Amplification Attacks using Group Requests**
  - Let gateway authenticate client. Let gateway limit bandwidth. Limit the number of servers that send requests.
- **MITM Amplification Attacks**