CoAP Attacks

draft-mattsson-core-coap-attacks

IETF 111, CORE, John Preuß Mattsson

draft-mattsson-core-coap-attacks

- In his IESG review of draft-ietf-core-echo-request-tag, Security AD Benjamin Kaduk suggested that it would be good to publish also draft-mattsson-core-coap-actuators.

- Based on this suggestion we have resubmitted draft-mattsson-core-coap-actuators as draft-mattsson-core-coap-attacks. The draft has been rebranded and expanded with a new section on amplification attacks.

- The draft gives background on the attacks motivating draft-ietf-core-echo-request-tag
  - Updated client Token processing requirements
  - Request-Tag option to match block-wise message fragments
  - Echo option to verify the freshness of a request
  - Echo option to to demonstrate reachability at its claimed network address

- **We aim to publish draft-mattsson-core-coap-attacks as an informational RFC.**

- **We think CORE need to discuss and take more concrete action against amplification attacks.**

CoAP amplification attacks gets media attention

- https://www.netscout.com/blog/asert/coap-attacks-wild
- https://www.shadowserver.org/news/accessible-coap-report-scanning-for-exposed-constrained-application-protocol-services/
- https://www.zdnet.com/article/the-coap-protocol-is-the-next-big-thing-for-ddos-attacks/
- https://www.zdnet.com/article/fbi-warns-of-new-ddos-attack-vectors-coap-ws-dd-arms-and-jenkins/
- https://www.helpnetsecurity.com/2019/03/08/iot-coap-ddos-weapon/
- https://blog.mazebolt.com/understanding-the-coap-ddos-attack-vector
- https://www.securityweek.com/attackers-use-coap-ddos-amplification
- https://medium.com/nsc42/what-is-coap-and-is-it-the-next-ddos-for-iot-de8ee97e57e6
- https://www.globaldots.com/resources/blog/iot-devices-using-coap-increasingly-used-in ddos-attacks/

Amplification attacks with IP address spoofing

- In an amplification attack, the amplification factor is the ratio between the size of the request and the total size of the response(s) to that request.
- Amplification attacks are often combined with the attacker spoofing the source IP address of the targeted victim to create a distributed denial-of-service attack on the target.
- When transported over UDP, the CoAP NoSec mode is susceptible to source IP address spoofing.
- [CoAP-Report] and [CoAP-Wild] report average amplification factor of 27 and 34 respectively from a single response to a GET request for /.well-known/core to the default UDP port 5693.
- The open CoAP servers are mostly concentrated to a few countries and a few implementations, which do not follow the recommendations in Section 11.3 of [RFC7252] (but the requirements are a bit soft).

TOTAL RESULTS

546,795

TOP COUNTRIES

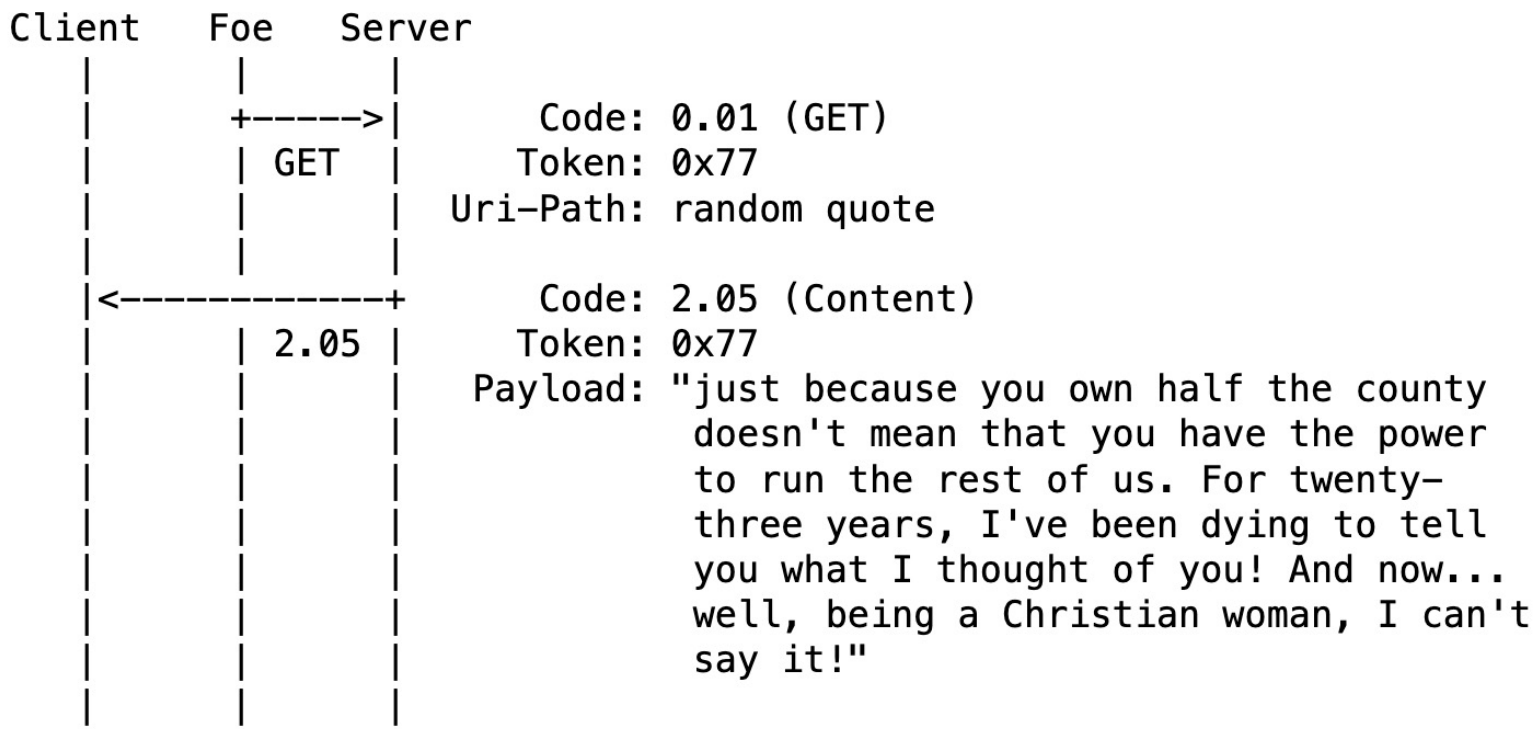
Philippines	214,187
China	111,700
Russian Federation	109,638
Malaysia	81,530
Thailand	11,278

More...

Amplification attack using a single response

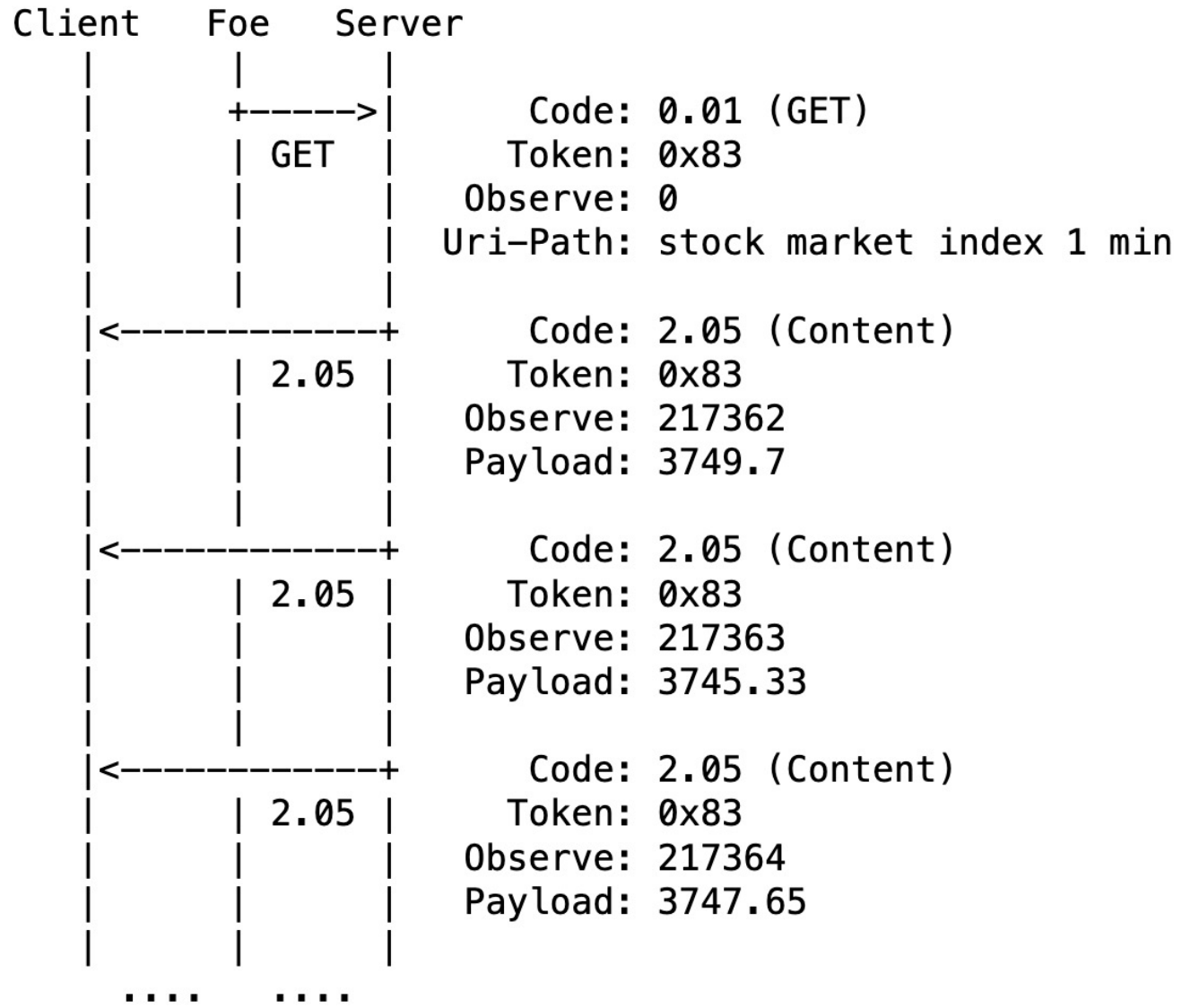
— If the response is a times larger than the request, the **amplification factor is a.**

— Amplification factors can be significantly worse when combined with observe [RFC7641] and multicast [I-D.ietf-core-groupcomm-bis].



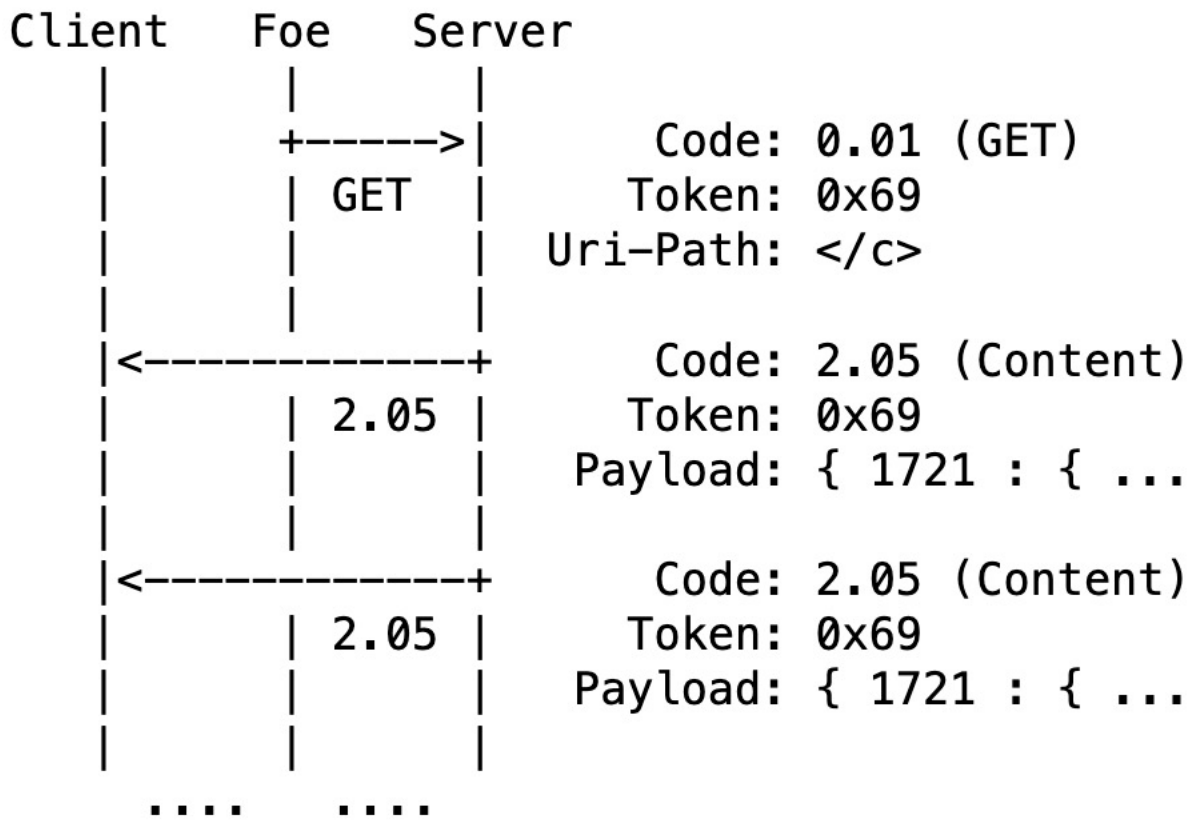
Amplification attack using observe

— If each response have an amplification factor of a, and the server sends n responses, the total **amplification factor is an.**



Amplification attack using multicast

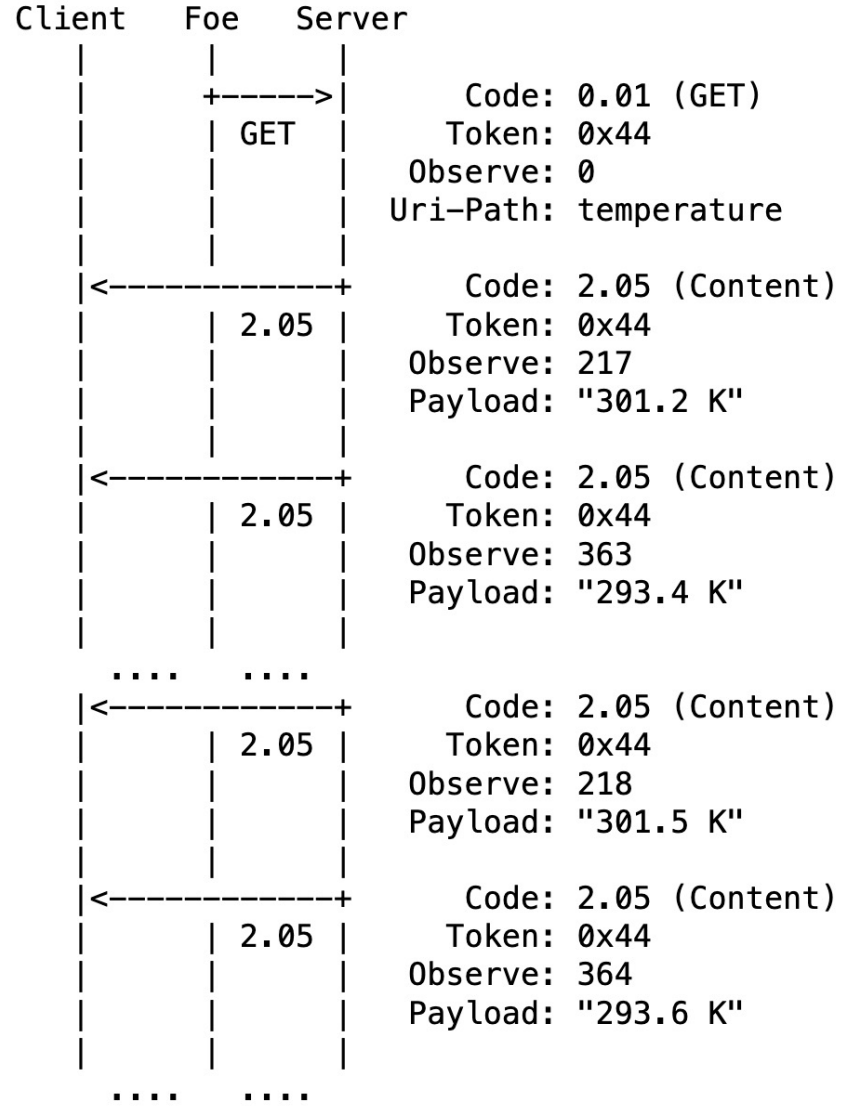
- If each response have an amplification factor of a, and there there are m servers, the total **amplification factor is am.**
- Note that the servers usually do not know the variable m.



Amplification attack using multicast and observe

- If each response have an amplification factor of a, and there there are m servers, and each server sends n responses, the total **amplification factor is amn.**

- Note that the servers usually do not know the variable m.



There is a need for harder requirements

- CORE has considered amplification attacks since the start, but the current recommendations are a bit soft:
  - RFC 7252: *"**large** amplification factors **SHOULD NOT** be provided in the response if the request is not authenticated"*
  - RFC 7252: *"**SHOULD NOT** accept multicast requests that can not be authenticated in some way"*
  - RFC 7252: *"**If possible**, a CoAP server **SHOULD** limit the support for multicast requests"*
  - RFC 7641: *"**MUST** strictly limit the number of notifications that it sends between receiving acknowledgements that confirm the actual interest of the client in the data; i.e., any notifications sent in non-confirmable messages **MUST** be interspersed with confirmable messages. **Note that an attacker may still spoof the acknowledgements**"*
  - draft-ietf-core-groupcomm-bis-04: *"it is **generally NOT RECOMMENDED** to use CoAP group communication in NoSec mode"*

- QUIC [RFC9000] mandates "an endpoint **MUST limit the amount of data it sends to the unvalidated address to three times the amount of data received from that address**" without exceptions. This approach should be seen as current best practice.

- DDoS is a major problem. Networks and services are targeted by CoAP Amplification attacks. This tarnishes CoAP's reputation. Even if we can not fix existing deployments, CORE should make sure to not make it worse.

- **RFC 7252, RFC 7641, and draft-ietf-core-groupcomm-bis needs to be augmented with strict normative requirements (MUST) on implementations similar to QUIC with a specified anti-amplification limit.**
  It should be clear that devices used in DDoS attacks are violating IETF requirements.
  - **How?, Where?, When?**