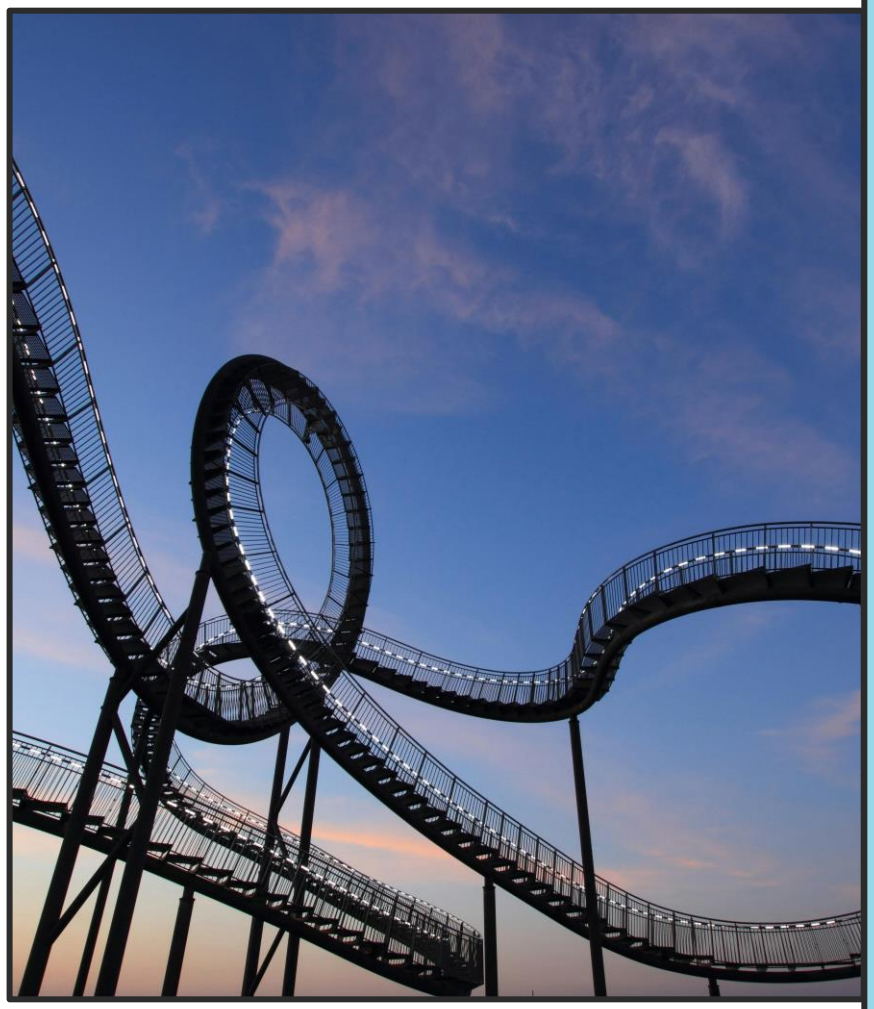
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Loopy Hell(ow): Infinite Traffic Loops at the Application Layer

Yepeng Pan, Anna Ascheman, Christian Rossow

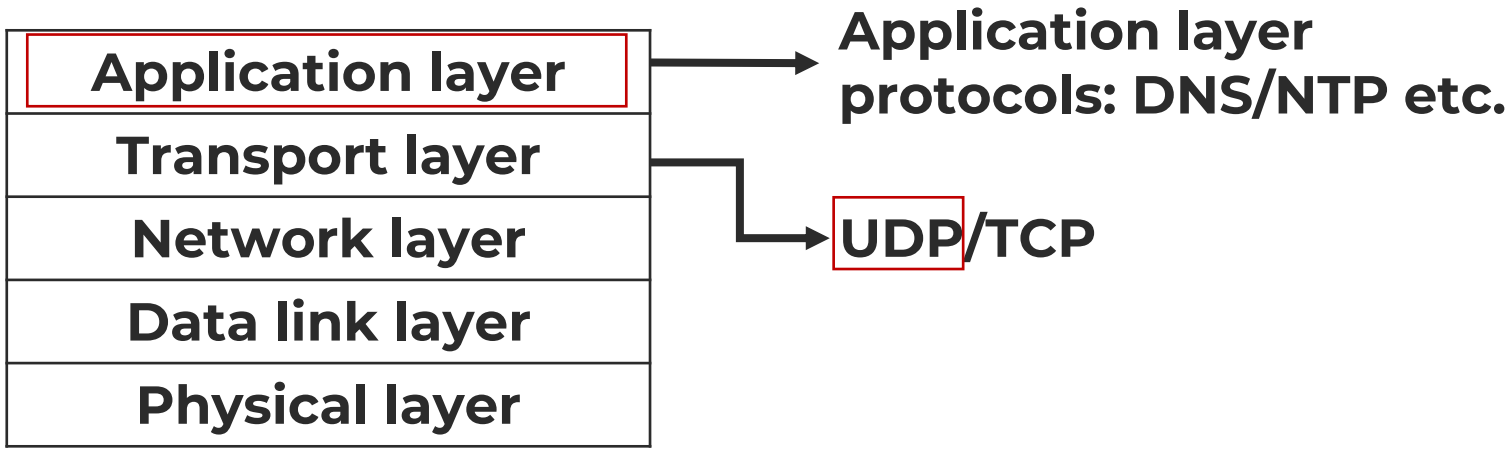
CISPA Helmholtz Center for Information Security



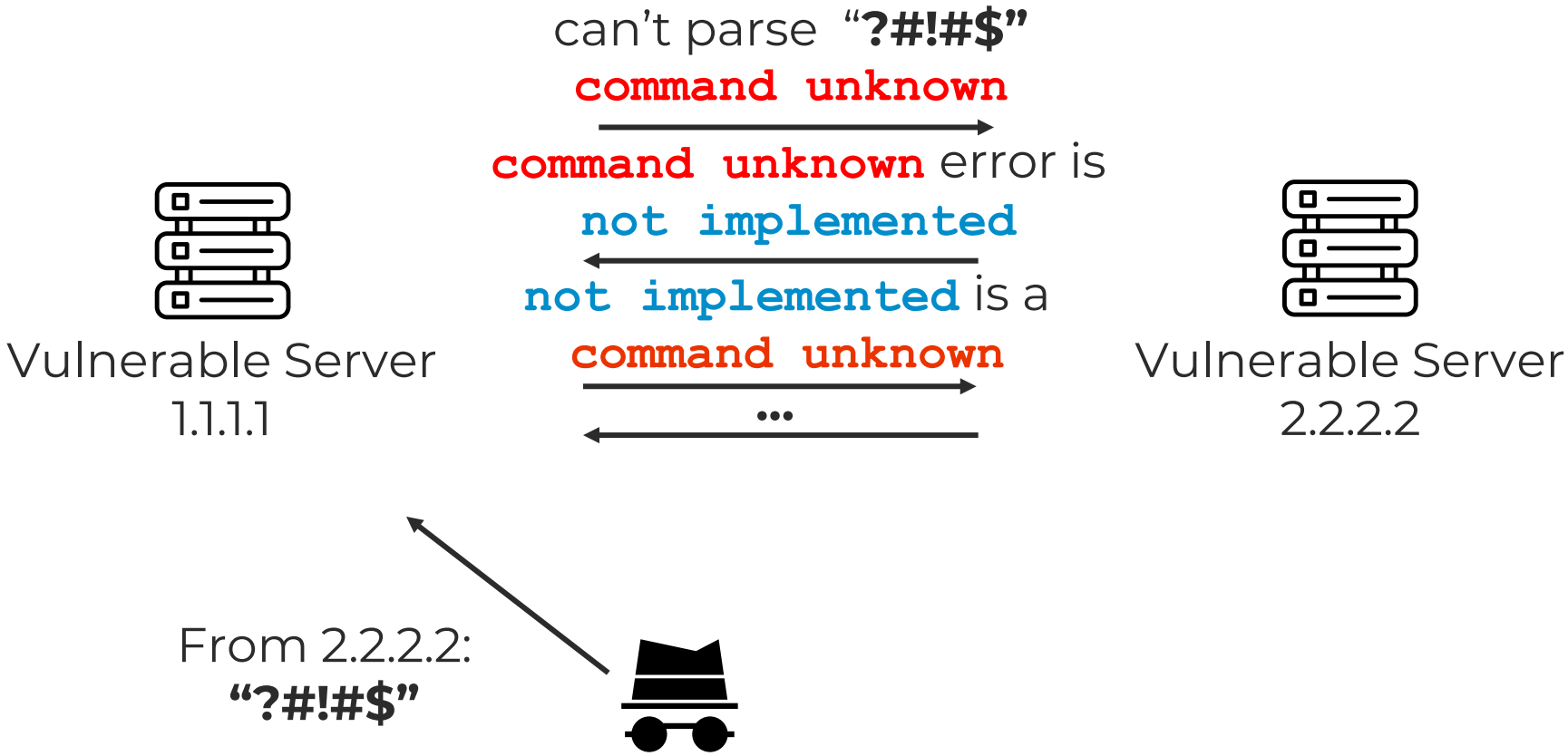
Background

An introduction to application layer traffic loops.

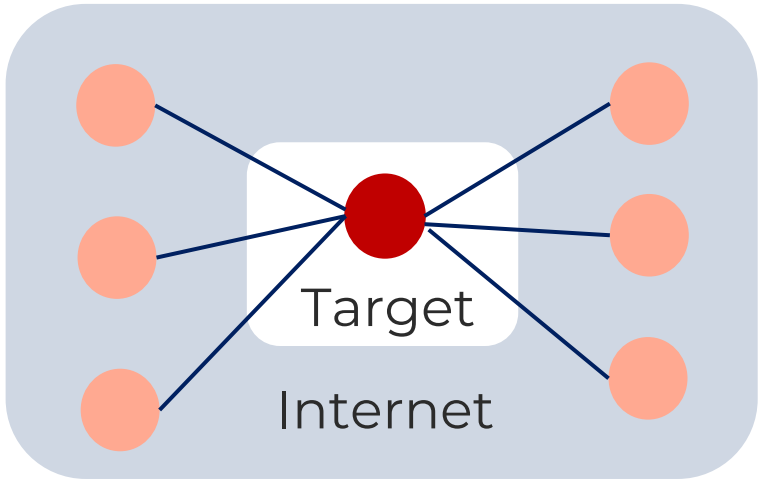
An Example Application Layer Traffic Loop



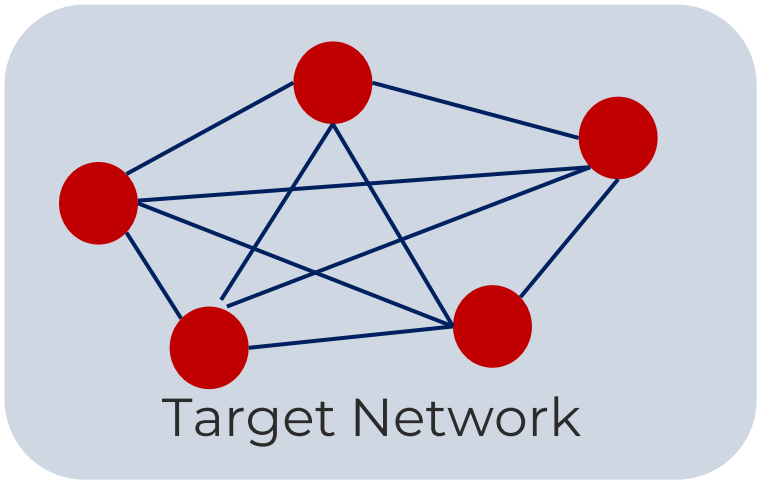
An Example Application Layer Traffic Loop



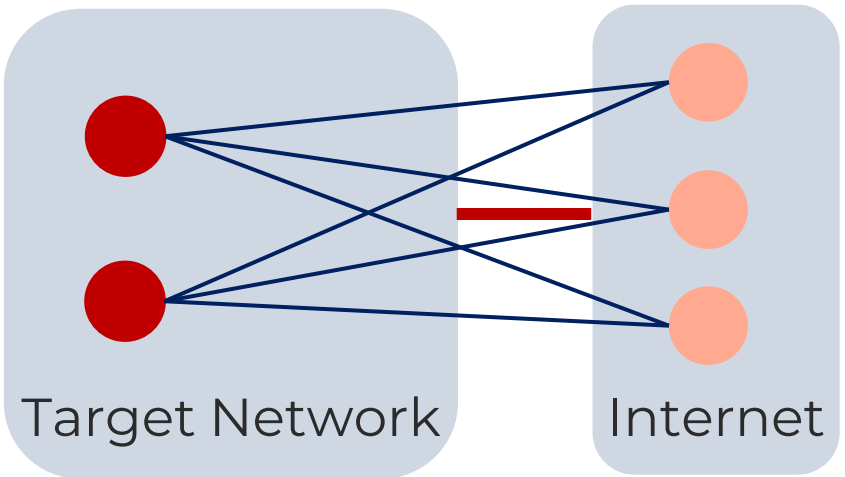
Attack Scenarios



(1) Overload a target host



(2) Overload backbone of the target network

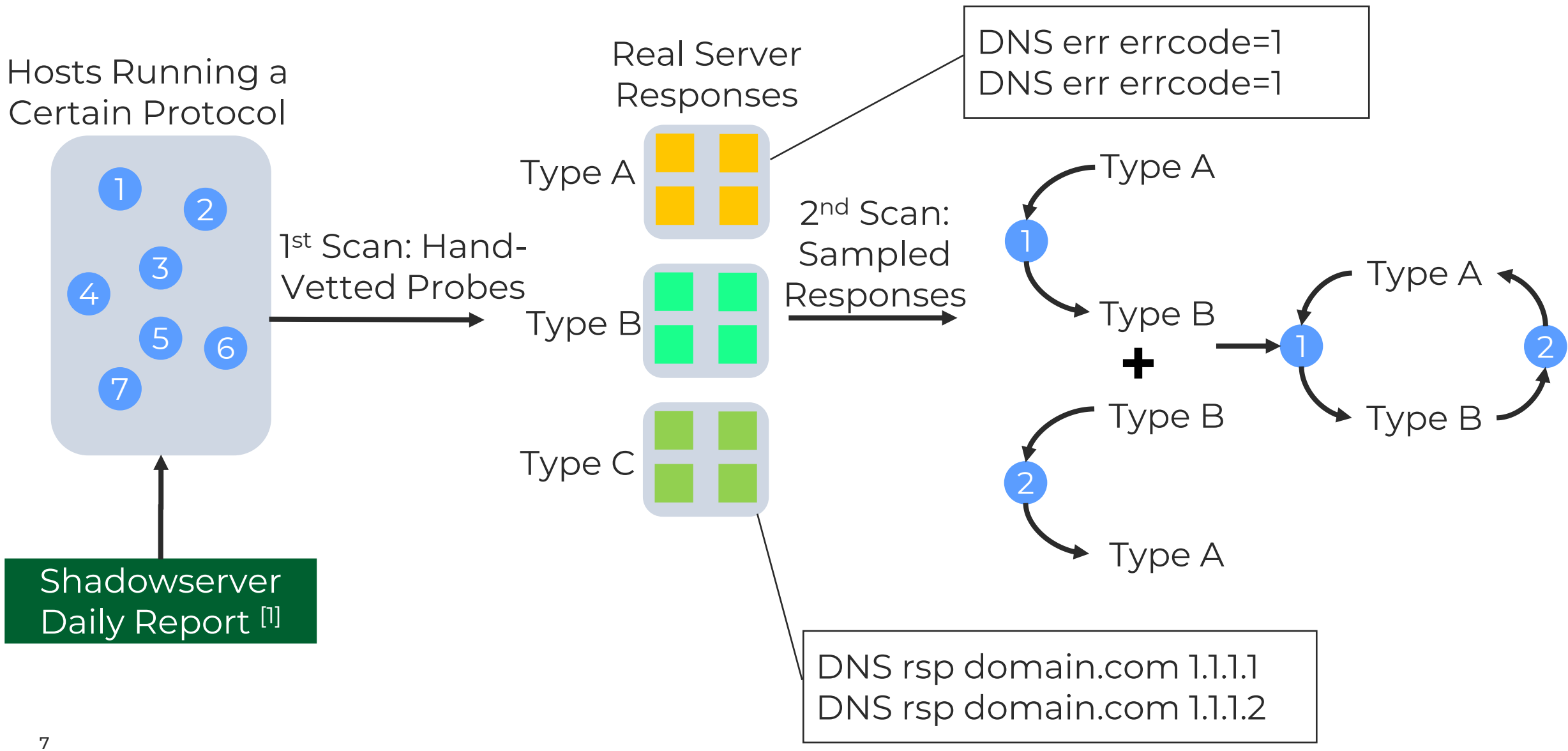


(3) Overload a link of the target network

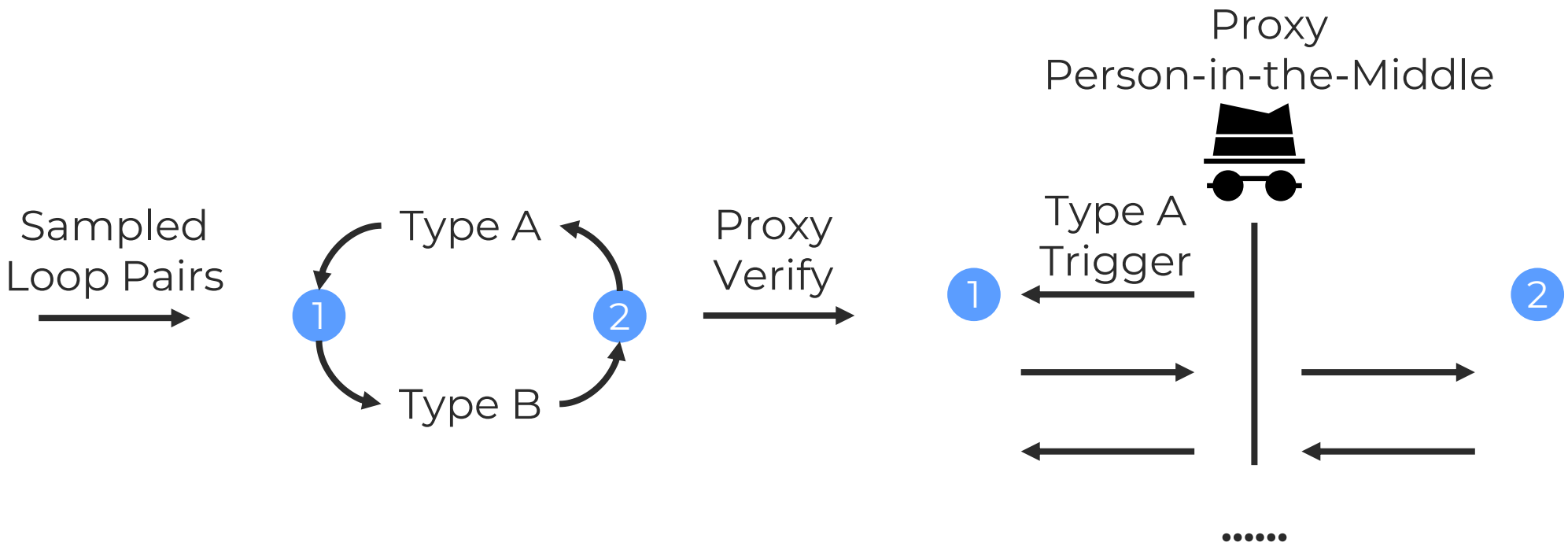
Methodology

Methodology to identify and verify traffic loops.

Methodology: Loop Hosts Identification



Methodology: Loop Verification



Results

Examined protocols and affected hosts

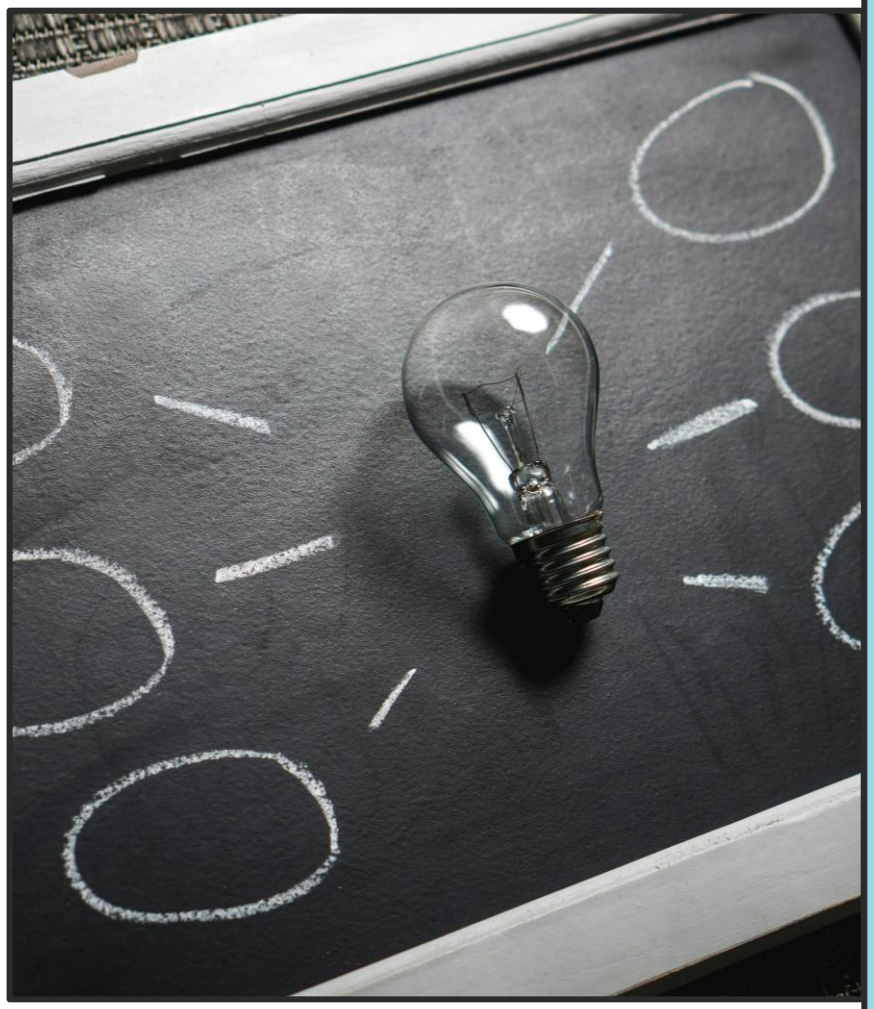
Results

- Non-Legacy Protocols:
  - TFTP ~19k
  - DNS ~111k
  - NTP ~82k
  - QUIC ~833k
- Legacy Protocols:
  - Echo ~56k
  - Chargen ~22k
  - QOTD ~21k
  - Daytime ~14k
  - Time ~13k
  - Active users ~3k

Number of loop pairs per protocol
~= (number of loop hosts)^2 / 2

Cross-Protocol Loop

- Cross-protocol loops between non-legacy protocols are possible, e.g., DNS + TFTP.
- DNS servers copy the Identification field in a request, but other protocols (e.g., TFTP) interpret the same bytes range as flags.
- DNS responses may pass semantic checks of other protocols.



Mitigations

Mitigations

- Quality of service, e.g., deprioritize legacy protocols
- Source port validation

} For administrators

- Suppress error messages
- Rate limiting

} For developers

Summary

1. We provide a methodology to identify and verify application layer traffic loops in real networks.
2. We examined several non-legacy protocols and legacy protocols and identified hunders of thousands of affected hosts.

We thank all the community contributions for helping us identify vulnerable devices and for providing constructive feedbacks to our **advisory**. [4]

Reference

[1] Shadowserver. Shadowserver Report.

[2] Paul Mockapetris. RFC 1035, Domain names – implementation and specification.

[3] Karen R. Sollins. RFC 1350, The TFTP Protocol (Revision 2).

[4] Christian Rossow. Application-Layer Loop DoS Advisor.