

Publicly Auditable Puzzles

Ed Kaiser

Advisor: Wu-chang Feng

Portland State University

edkaiser@cs.pdx.edu

Distributed Denial-of-Service (DDoS) attacks against a network protocol arise from the imbalance of resources (computation and memory) committed by a client and server. A client may simply transmit a request to initiate a protocol, however, the server must retrieve data from memory and possibly perform a non-trivial computation. A group of clients can launch an effective DDoS attack by sending requests faster than the server can satisfy them.

Cryptographic puzzles are a mechanism added to various protocols in order to reverse the imbalance of resources committed by the client and server. At the start of the protocol, the server assigns a puzzle to the client and will not commit any resources until the client produces the puzzle's answer. The puzzle is designed such that solving it requires the client to commit enough resources to shift the imbalance in favor of the server. A parameter set by the server controls the resources required by a client to solve the puzzle. The server can scale this parameter to match the aggregate request rate.

It has been argued that unless cryptographic puzzles are placed in the lowest common layer of the network stack (i.e., the network layer), puzzles can be easily sidestepped by attacking the protocol of a lower layer [1]. For example, application layer puzzles are thwarted by attacks depleting the connection buffer of TCP. Network layer puzzles are a service-independent form of mandatory congestion control and as such, the puzzle issuer does not need to be the same machine as the server.

As a form of congestion control, puzzles are analogous to postage stamps but are paid for in computation rather than money. In both the network and postal systems, resources are expended to deliver communication. It is best to verify postage close to the entry point in order to limit the resources wasted on delivering communication with insufficient postage. Thus, network layer puzzle issuers should be located throughout the Internet so that they are much closer to the network entry points.

This material is supported in part by the National Science Foundation under Grant ANI-0230960 and the generous donations of Intel Corporation. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation or Intel.

There are significant challenges in implementing network layer puzzles:

- *Limited space*: There is a limited space in the packet header to accommodate puzzle answers. With puzzle issuers located throughout the network, there may be several issuers along the path from a client to a server; it is possible that there may be more puzzles issued than there is room for answers.
- *Parsing complexity*: Even given an unrestricted amount of room in the packet header, the complexity of parsing through a variable number of answers and verifying the correct one with what an issuer expects may not be possible in the fast path of Internet routers.
- *Communication overhead grows*: The cost of communicating new puzzles and answers grows quickly for each additional issuer along the path.

My proposed solution is a class of puzzles with answers that are *publicly auditable*. The answer to a publicly auditable puzzle can be validated by any machine that handles it. This means that each puzzle issuer does not require a separate answer: only a single answer is ever necessary.

There are three required properties for an answer to be publicly auditable:

- *Public verification*: Any machine can check if an answer is correct and can reject incorrect answers.
- *Public work estimation*: Any machine can estimate how much work was required to produce the answer. This allows issuers who are under more load than other issuers along a path to fight congestion based on their needs.
- *Public expiration*: Any machine can determine if an answer has been used before. This prevents malicious clients from avoiding work by replaying answers.

Research into constructing puzzles that are publicly auditable has been promising. More information can be found at: <http://syn.cs.pdx.edu/projects/puzzlenet>.

REFERENCES

- [1] W. Feng, E. Kaiser, W. Feng, and A. Luu, "The Design and Implementation of Network Puzzles," in *IEEE INFOCOM*, March 2005.