Reducing Malicious Traffic With IP Puzzles

Ed Kaiser, Wu-chang Feng, Wu-chi Feng, Antoine Luu

Motivation

Argh! There is so much bad traffic on the internet!
- DoS attacks
- Port scans
- Spam e-mail
- Worms
- Hacking
- Game cheaters

Question: What can be done?
Answer: Make clients accountable for their behavior by using a mechanism for punishing them if they behave badly.

Client puzzles offer an ideal punishment mechanism:
- Easy to assign punishment
- Can make punishment arbitrarily difficult
- False positives degrade but do not deny service

Other work secures individual protocol vulnerabilities, however the most effective solution should protect all network traffic; thus it must be placed in the IP layer.

Our approach:
IP layer client puzzles

Challenges

Flexible Deployment
- Puzzle issuers at arbitrary network locations

Minimal Overhead
- Puzzles can be generated at line speed
- Constant state at the puzzle issuer
- Minimal packet expansion

Tamper Resistance
- Replay attacks
- Spoofing attacks
- Work ahead attacks

Support for Real Time Apps
- Online games
- Streaming media

OGI SCHOOL OF SCIENCE & ENGINEERING
OREGON HEALTH & SCIENCE UNIVERSITY

Performance

Constant State at Issuer

Fast Issuer
- creation: 2 random numbers and 2 hashes
- verification: 1 hash

Minimal Overhead
- puzzle is 51 bytes; answer is 26 bytes

Fine Grain Difficulty Control
- can linearly increment puzzle difficulty

Experimental Throughput
- 1.8GHz Intel Xeon machines on Gigabit switch

Issues: validate and create puzzles at 182k packets/s
Client: solve min-difficulty puzzles at 130k packets/s

Slowing Port Scans

Performance

Constant State at Issuer

Fast Issuer
- creation: 2 random numbers and 2 hashes
- verification: 1 hash

Minimal Overhead
- puzzle is 51 bytes; answer is 26 bytes

Fine Grain Difficulty Control
- can linearly increment puzzle difficulty

Experimental Throughput
- 1.8GHz Intel Xeon machines on Gigabit switch

Issues: validate and create puzzles at 182k packets/s
Client: solve min-difficulty puzzles at 130k packets/s

Future Work

Reputation-Based Networking
- Keep interaction history about clients
- Determine their reputability
- Use IP Puzzles to punish clients who are bad
- Share knowledge with other IP Puzzle firewalls

Publicly Auditable Puzzles
- Puzzle answers can be independently verified by intermediate IP Puzzle routers
- Answers can indicate amount of work done

Puzzles With Useful Answers
- Puzzle algorithms where the answers provide useful computation for the puzzle issuer
- Puzzle answer must be easily verifiable

IXP Implementation

OGI SCHOOL OF SCIENCE & ENGINEERING
OREGON HEALTH & SCIENCE UNIVERSITY

http://www.cse.ogi.edu/sysl/
Funded by: intel