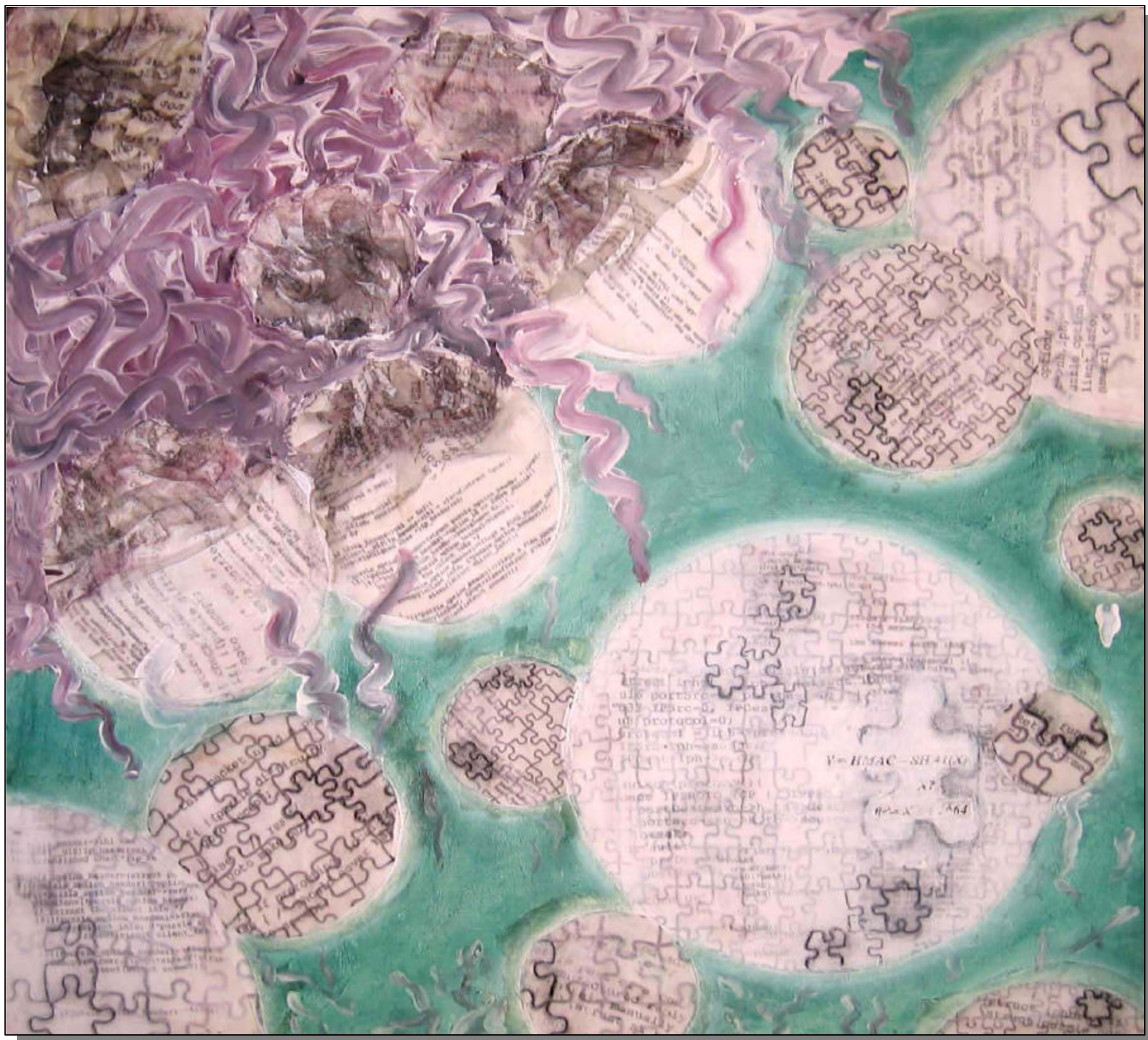


# Reducing Malicious Traffic With IP Puzzles

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



## Motivation

Arrgh! 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

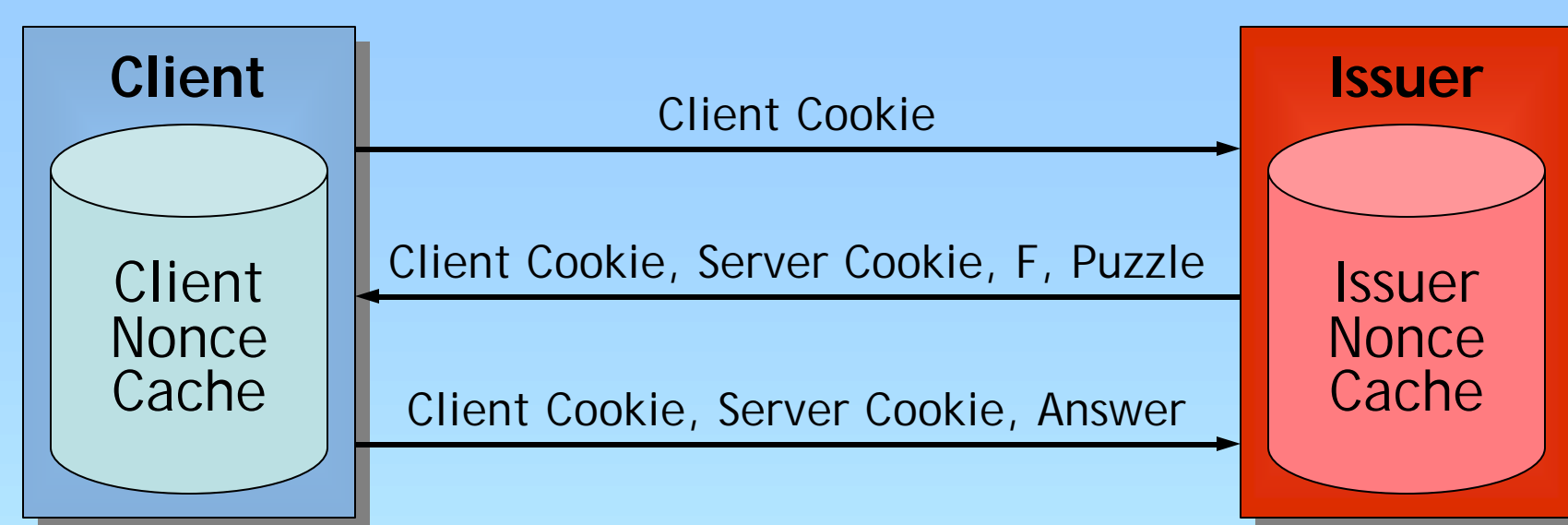
### Tamper Resistance

- Replay attacks
- Spoofing attacks
- Work ahead attacks

### Support for Real Time Apps

- Online games
- Streaming media

## Puzzle Protocol



Protocol Field	Description
Client Cookie	$TS_c, N_c$
Server Cookie	$TS_s, TS_m, TS_o, h(F, TS_c, N_c, TS_s, N_s, TS_m, TS_o)$
Puzzle	Difficulty, Puzzle Parameters
Answer	Puzzle Answer
$TS_c$	Client Logical Timestamp
$N_c$	Client Nonce
$TS_s$	Issuer Logical Timestamp
$N_s$	Issuer Nonce
$F$	Flow Identifier
$TS_m$	Puzzle Maturity Time
$TS_o$	Puzzle Expiry Time
$h()$	Hash Message Authentication Code (HMAC)

## Puzzle Algorithm

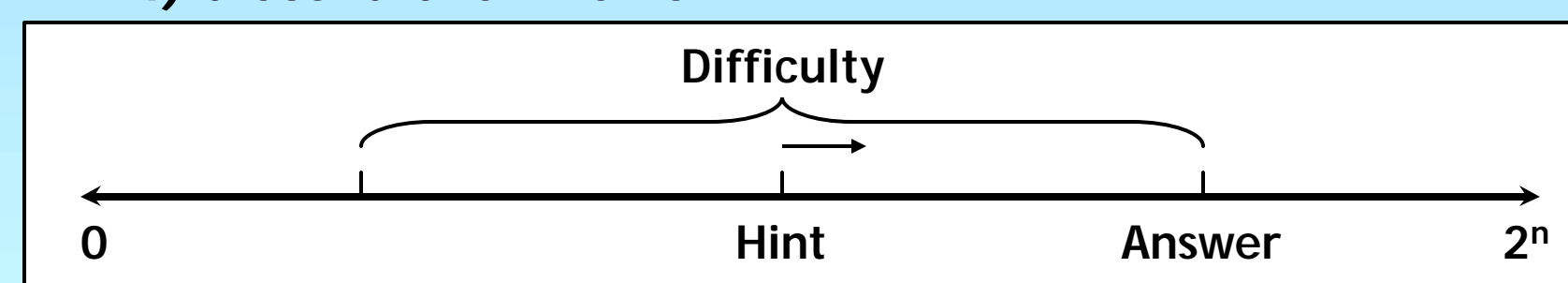
### Hint-Based Hash-Reversal

Requires:

- Keyed HMAC;  $h()$
- high entropy random number generator;  $rand()$

Creating the Puzzle:

- 1) Answer  $\leftarrow rand()$
- 2) Hint  $\leftarrow Answer - (rand() \bmod Difficulty)$
- 3) Puzzle Hash  $\leftarrow h(Answer)$
- 4) discard the Answer



Solving the Puzzle:

- 1) Search Value  $\leftarrow Hint$
- 2) if  $h(Search Value) = Puzzle Hash$   
Answer  $\leftarrow Search Value$
- 3) Search Value  $\leftarrow Search Value + 1$
- 4) go to step 2

## Protocol Extensions

IP Options

Cookie:

Type = 25	Length	Control
Client Timestamp		Client Nonce

ICMP

Puzzle:

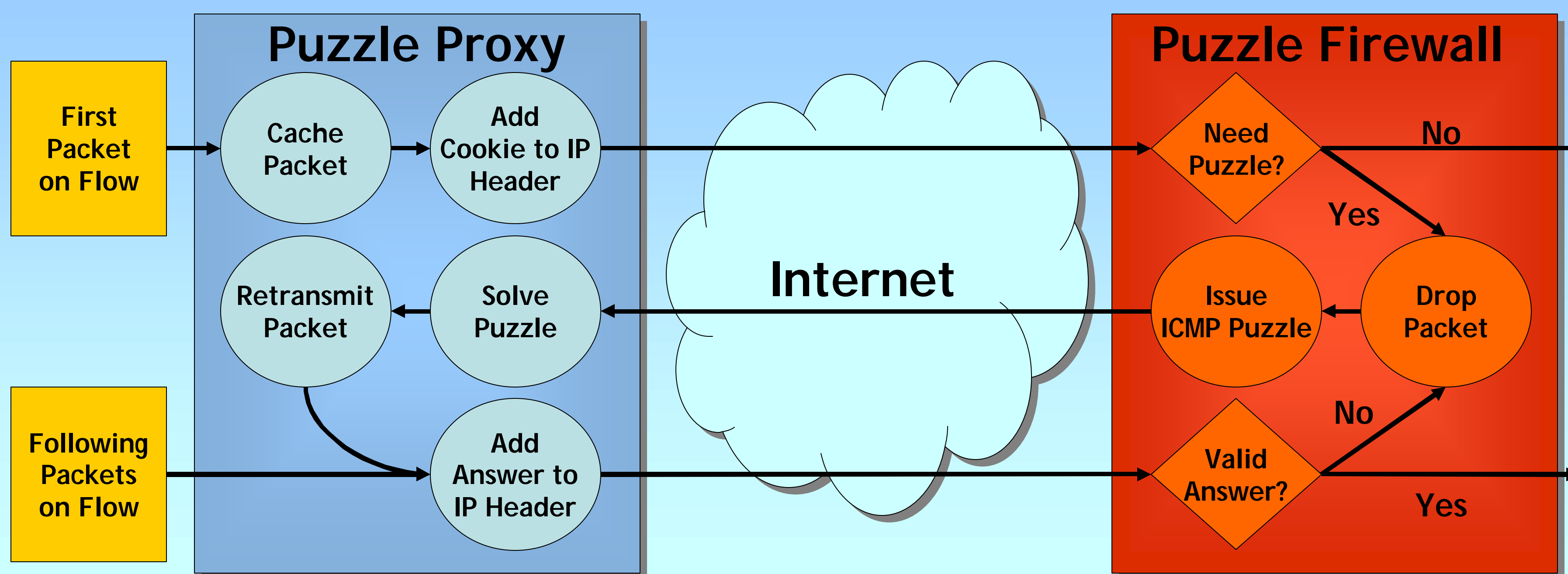
Type = 38	Code	Checksum
PuzzleType	Length	Control
Client Timestamp		Client Nonce
Issuer Timestamp		Maturity Time
Expiry Time		Protocol
Client IP		
Server IP		
Client Port		Server Port
Hash of Parameters and Secrets		
Puzzle Difficulty		
Puzzle Parameters (variable length)		

IP Options

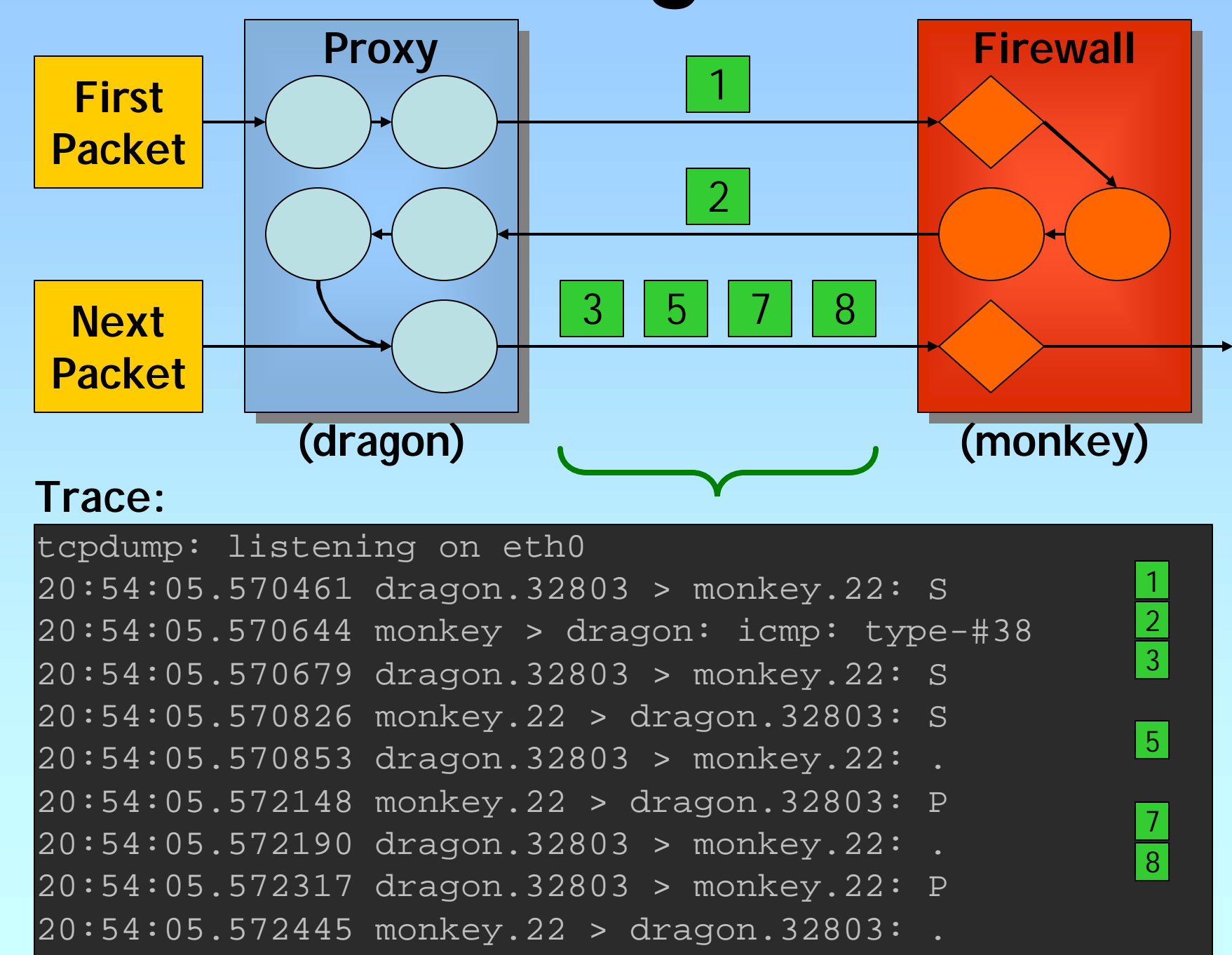
Answer:

Type = 26	Length	Control
Client Timestamp		Client Nonce
Issuer Timestamp		Maturity Time
Expiry Time		
Hash of Parameters and Secrets		
Puzzle Answer (variable length)		

## iptables Implementation



## Tracing ssh



## 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

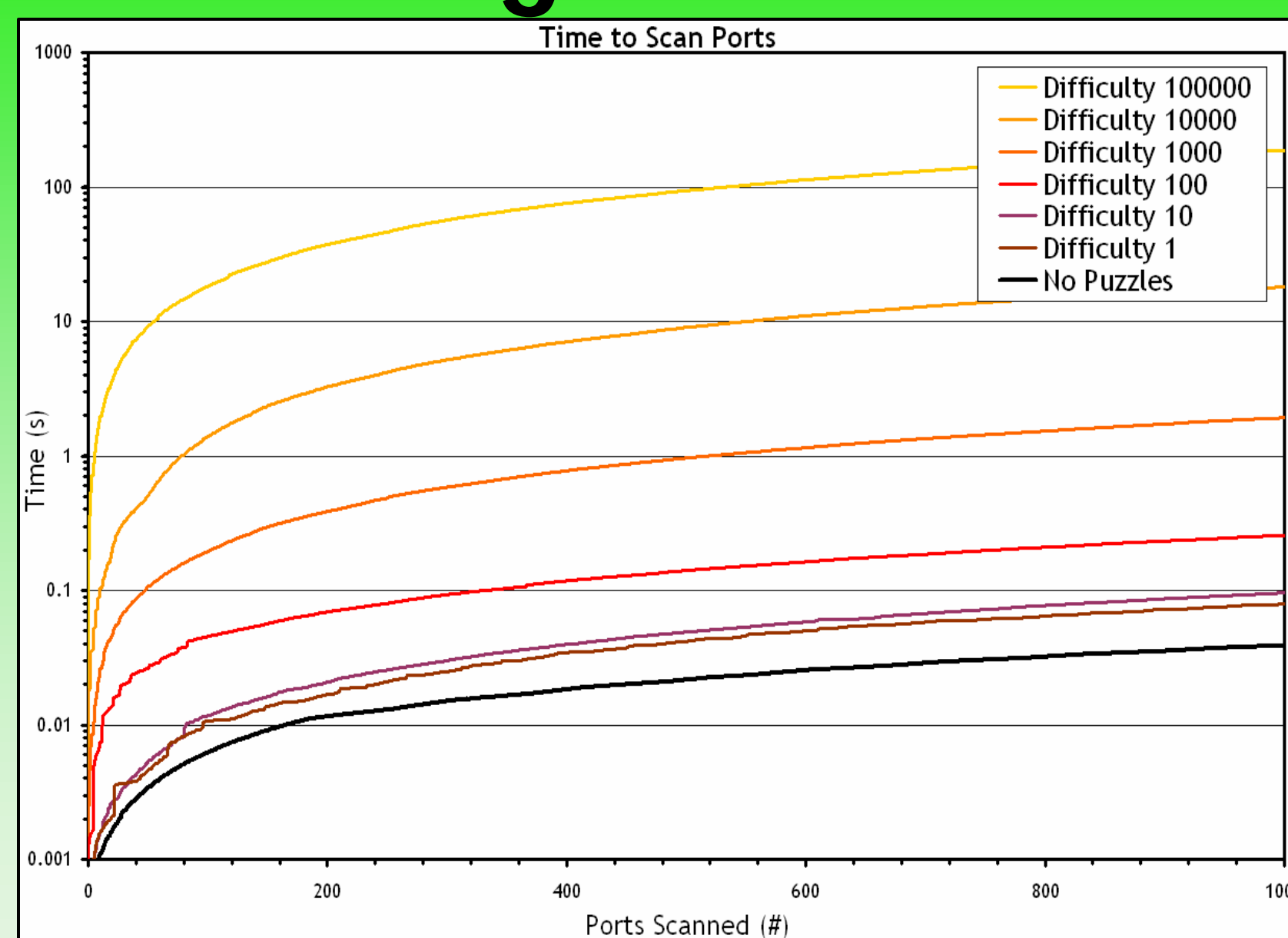
- can linearly increment puzzle difficulty

Experimental Throughput

- 1.8GHz Intel Xeon machines on Gigabit switch

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

## Slowing Port Scans



Adjusting the difficulty of IP Puzzles can force port scans to take a selectively long time to complete.

## 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/sys1/>  
Funded by: