Objective

- Increase long-term cost and decrease throughput of web spam
- Minimize impact on legitimate users

Approach

- Force an arbitrary sequence of computation before servicing requests
- Adapt computation based the request

Challenges

- Discerning legitimate from adversarial requests
- Resistance to attack via metamorphism

Reputation service

Augment local metrics with global metrics to determine puzzle difficulty

IP blacklists (DShield, Spamhaus, Project Honeypot)
URL blacklists (SURBL, URIBL)
Content analysis (SpamAssasin, Akismet)
Geographic location (GeoIP)

Architecture
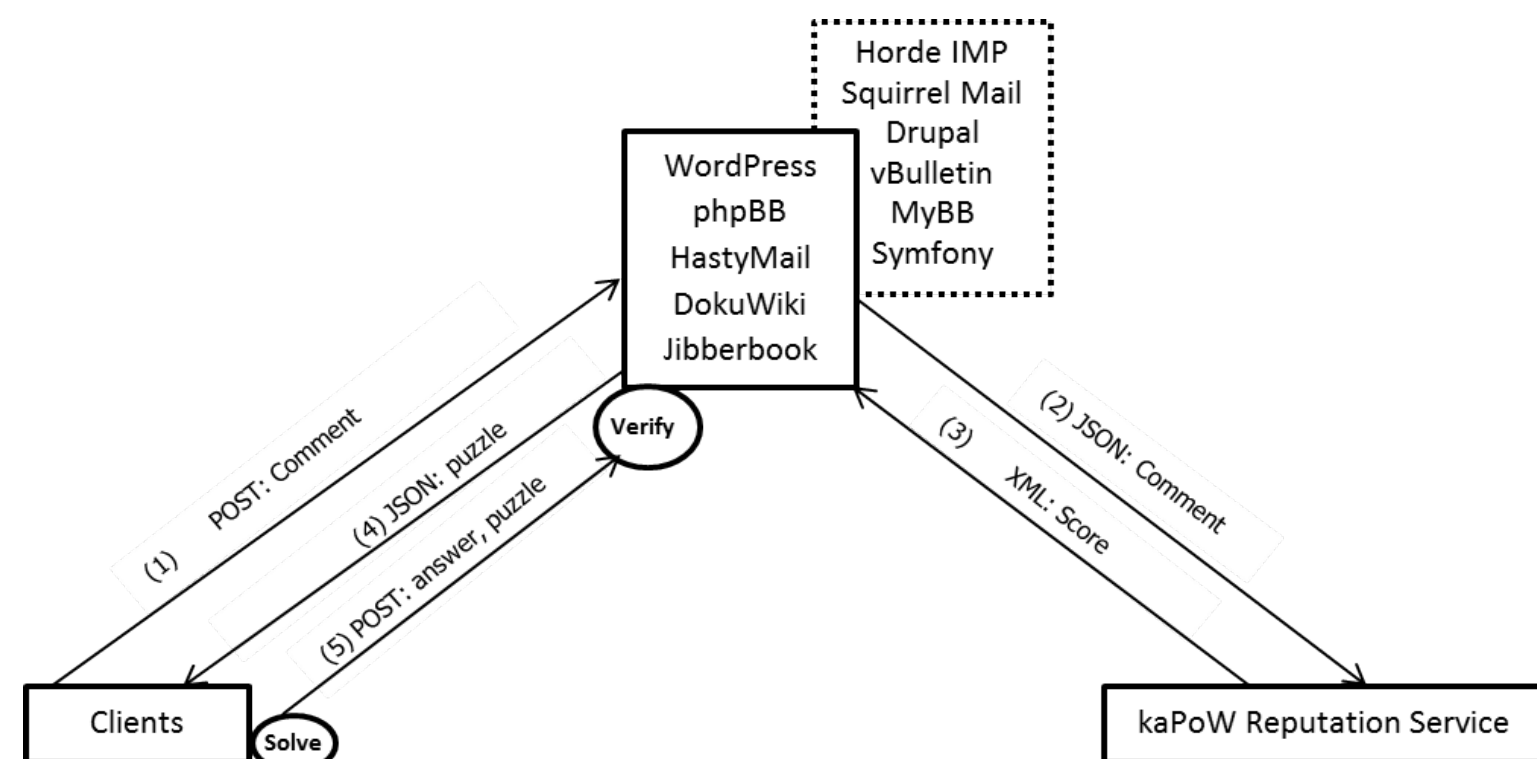
Demo

Metamorphic sub-puzzles

Selected from a dynamic puzzle library

Modified Time-lock

- <u>non-parallelizable deterministic solution</u>

  Server issues parameters:
  $n \leftarrow p \times q$ (two large random primes)
  $D_C \leftarrow$ client-specific difficulty
  $N_C \leftarrow SHA1_K(URL, IP_C, D_C)$

  Client solves $A' = (N_C^2)^{D_C} \bmod n$
  Server verifies A':
  $r \leftarrow 2^{D_C} \bmod \Phi(n)$
  $A' = N_C^r \bmod n$?

Targeted Hash-Reversal

  Server issues parameters:
  $D_C, N \leftarrow$ client-specific difficulty, nonce

  Client solves for A such that
  $SHA1_K(N, URL, A) = 0 \bmod D_C$

Hint-based Hash-Reversal

  Server issues parameters:
  $A \leftarrow Random()$
  $Hint \leftarrow A - Uniform(0, D_C)$
  $P \leftarrow SHA1_K(A)$

  Client searches from Hint to find A such that
  $SHA1_K(A) = P$

Targeted Large Prime Generation

  Server issues parameter A
  Client finds smallest prime number > A

Halting Problem

  Server traps client into unending sequence of puzzles

Software

Project webpage
   http://kapow.cs.pdx.edu

phpBB plugin
   https://www.phpbb.com/customise/db/mod/kapow

WordPress plugin
   https://wordpress.org/extend/plugins/headwinds

Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

National Science Foundation
WHERE DISCOVERIES BEGIN

Portland State UNIVERSITY

intel