1. Problem: Attacks on the Web

- Distributed Denial-of-Service
- Click fraud
- Comment spam
- Ticket purchasing robots

2. CAPTCHA to the rescue?

- Problem #1: Inaccessible
- Problem #2: Economics broken
  - Fixed human workload
  - Outsourced for under $0.01 per CAPTCHA
- Problem #3: Hackers are solving the hard AI problem
  - Yahoo! CAPTCHA broken 1/16/2008

3. What about Proof-of-Work (PoW)?

- Addresses Problem #1: No user-interface issues
- Addresses Problem #2: Variable workload
- Addresses Problem #3: Hard cryptographic problem

Q: Why is the landscape littered with unused PoW protocols?
- Hashcash, TLS puzzles, TCP puzzles, IP puzzles, Public work
- PoW requires protocol changes and universal deployment
- CAPTCHAs do not!

5. Example

6. Implementation

- JavaScript solver (kaPoW.js)
  - `onLoad` event handler to solve PoW challenges for embedded images
  - `onClick` event handler to solve challenges for embedded links
  - Solve routine finds a value A, such that
    \[ \text{SHA1}(N, 1 || \text{URL} || A) \equiv 0 \mod D_c \]
    
  - Client-specific server-assigned difficulty
  - Client-specific server-generated nonce

- mod_kaPoW Apache module

7. Thwarting DoS

8. Future work

- Policy module for setting per-client D_c
  - Client history
  - Client reputation
  - Client location
  - Request type
  - Resource requested

- Adding to applications
  - Forums (phpBB)
  - Wikis (MediaWiki)
  - Blogs (WordPress, Slashcode)
  - Web 2.0 / AJAX

- Economic analysis
  - What is the cost of idle CPU cycles?
  - Markets based on CPU cycles

9. Availability

- Demo site
- http://kapow.cs.pdx.edu
- Non-commercial source release
  - In progress

10. Publications

- "New weapon against today's web attacks"
- "Deployable alternative to CAPTCHAs"
- "New approach for transparent proof-of-work"