CSci 8271
Security and Privacy in Computing
Day 5: "Great Firewall" DNS poisoning

Stephen McCamant
University of Minnesota

China's nation-level Internet blocking

- China provides the largest example of nation-state level network blocking
  - "Great Firewall of China" is a western coinage
- A combination of techniques are used
  - Packet filtering
  - Application-level keyword filtering
  - Pressure and incentives for companies
  - DNS poisoning

GFWatch design

- Start with a large and varied corpus of interesting domain names
- Check for injections between two controlled hosts
- First checks are inbound (US to Chinese server)
- Results confirmed with outbound checks
- UDP only for low overhead, multiple checks per day

Findings about blocked domains

- Wildcard rules multiply the number of blocked domains
  - Significant amount of collateral damage, e.g. `ventilatorproject.org`
- Only 1.3% of the 138.7K blocked domains are popular
- Wide variety of content categories blocked

Findings about forged IPs

- Forged IPv4 results are mostly chosen dynamically from modest pool
  - 600 IPs cover 99% of responses
  - Mainly routable with unrelated owners (e.g., Facebook)
- A smaller set of domains have static fake results
- Forged results pollute public DNS services

Circumvention and suggestions

- (DNSSEC, DNS over HTTPS/TLS)
- Wait and filter multiple DNS responses
- Use set of forged IP addresses to detect poisoning
- Can GFW operators reduce collateral damage at no cost to them?