Design of a DDoS Attack-Resistant Distributed Spam Blocklist

Jem E. Berkes
Dept. Electrical and Computer Engineering
University of Manitoba
Winnipeg, Canada

Introduction

- Anti-spam blocklists are vital for the Internet
- Blocklists are targets of DDoS attacks
  - Making operation impractical, costly

- How to make blocklists resistant to attacks?

Presentation outline

- Background
  - Spam blocklists
  - DNSBL technology
  - DDoS attacks
  - Design motivation
- Proposed solution
  - Structure
  - Security
  - Implementation
- Conclusion
- Questions

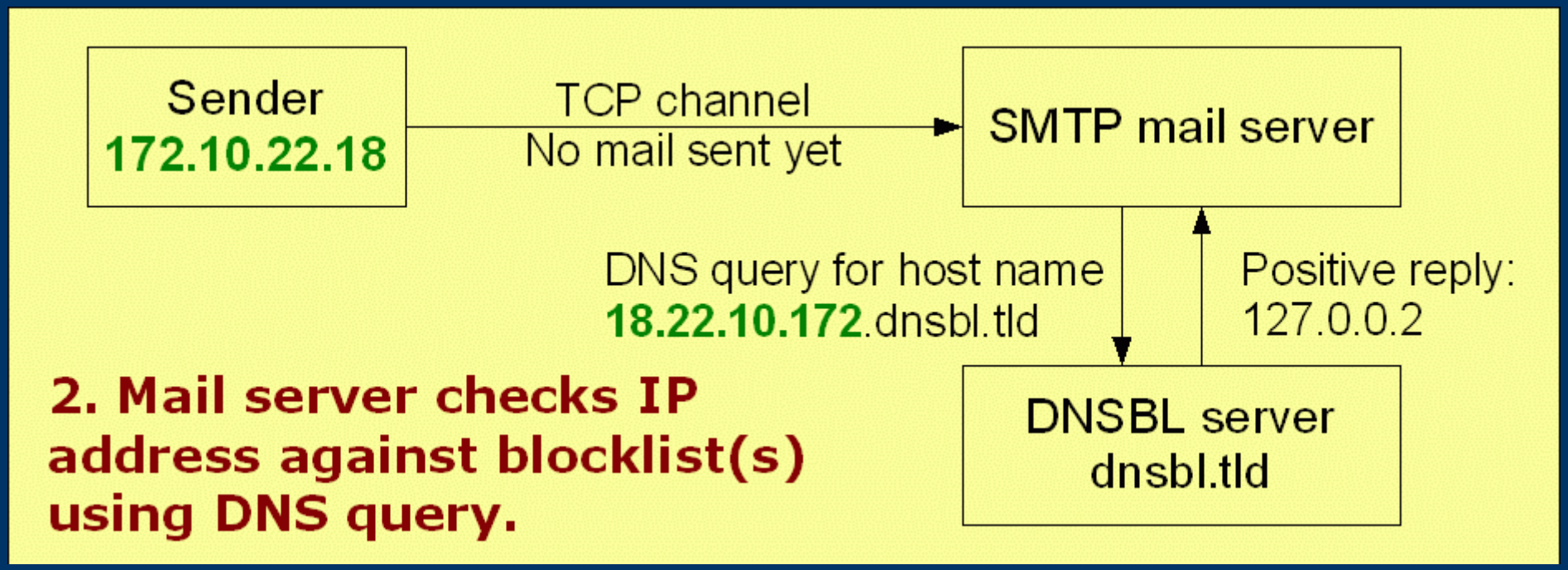
Background: Spam blocklists

- Primary anti-spam measure for ISPs
- Simple, efficient, effective
- Third party database
- IPs or domain names meeting criteria, e.g.
  - Insecure hosts/open relays/open proxies
  - Hosts that sent spam
  - Hosts belonging to networks that send spam
- Many databases available, nearly all are free and maintained by volunteer organizations

Background: DNSBL technology

- DNSBL: DNS Blocklist (“RBL”, “blacklist”)
- First used for Paul Vixie's MAPS/RBL, 1997

Background: DNSBL technology



Background: DNSBL technology

- DNSBLs save bandwidth!
- Front line of spam defence
- Vital for ISPs

Background: DDoS attacks

- DDoS: Distributed Denial of Service
  - Continuous TCP/ICMP traffic from many hosts
- Blocklists are popular attack targets

- Permanently shut down due to DDoS attacks:
  - Osirusoft, Monkeys
- Current targets of ongoing attacks:
  - SPEWS, Spamhaus, SpamCop
- Withstanding attacks is costly

Background: Design motivation

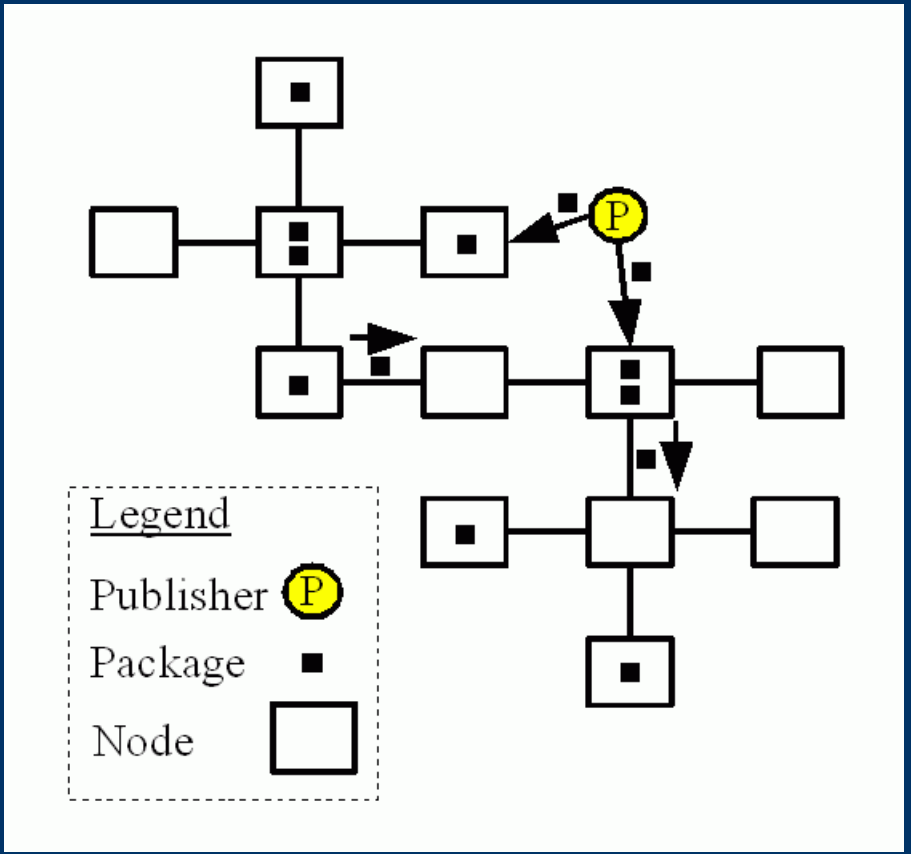
- DNSBLs are easy to attack
- Central servers
  - Can add more servers, but there is high cost
  - Almost all blocklists run by volunteers

- Can blocklists be made resistant to attacks,
  - **while maintaining data integrity**
  - **without requiring costly resources?**

Proposed solution: Structure

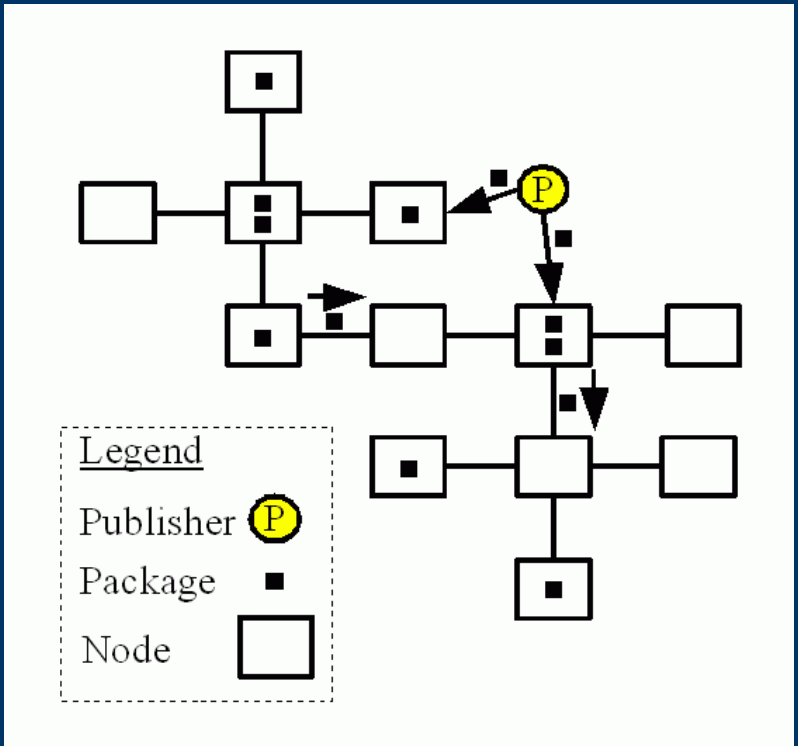
- **Distributed blocklist**
- Peer-to-Peer system
- Pooling resources
- No central server

- Publisher in control



Proposed solution: Structure

- Who are the Nodes?
  - Small, medium, large ISPs
  - Anyone with resources
- Who is Publisher?
  - Authority on blocklist data
  - Likely, anonymous



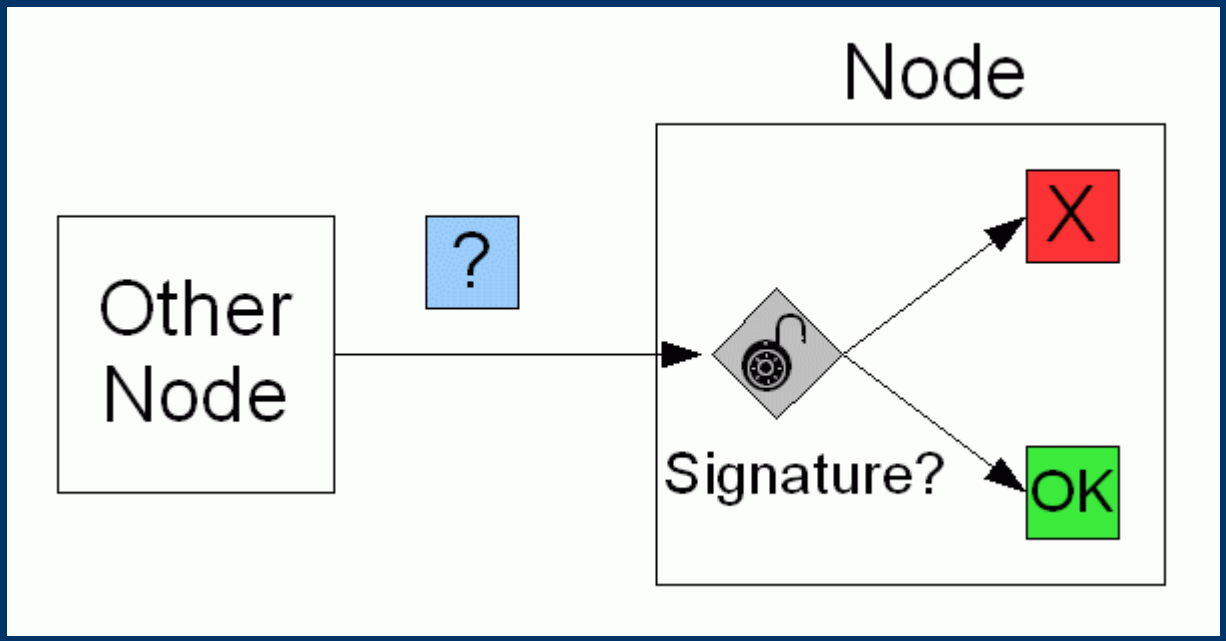
- The point: there is no vital entity to attack

Proposed solution: Security

- All Nodes serve blocklist data
- No central server
- How can we trust blocklist contents?
  - What enforces Publisher's control?

- Digital signatures (PGP/OpenPGP)

Proposed solution: Security



- Nodes (and users) can verify data integrity
- All Packages must be signed by Publisher
- Guarantees propagation of authentic data

Proposed solution: Implementation

- Required protocols already exist
  - OpenPGP data signatures
  - HTTP data transfers, or
  - Gnutella for P2P structure
- Users could run local DNSBL
  - i.e. No changes required to mail server software

Conclusion

- Current spam blocklists are threatened
- A distributed (Peer-to-Peer) system
  - Eliminates central servers
  - Allows pooling of resources
- Enforcing digital signatures
  - Maintains data integrity and reliability
  - Gives a Publisher sole control of data
- Distributed spam blocklist can be built using existing protocols

Questions

Any questions?