Community Based Blacklists

Open Community Camp 2012

Rick van der Zwet <info@rickvanderzwet.nl>

Made Using/At/With

Todays' Program

- The Cause: Type of Attacks
- The Problem: Trust Models
- The Current: Known Implementations
- The Future

The Cause: Type of Attacks

- SSH BruteForce logins
- SPAM
- DDOS Controlled Attacks
- Phishing Websites

The Problem: Trust Models

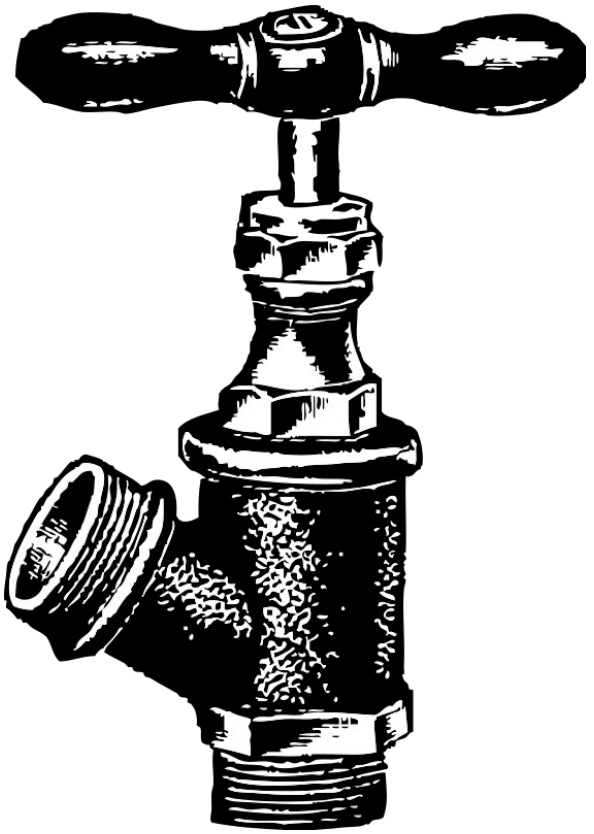
- The Internet is open and blocking parts of it could be considered harmfull

  (False Positives).
- Who do you trust to tell the truth

  (in a secure way)
- Who maintains the infrastructure

The Current: Known Implementations

- DNS-based Blackhole List (DNSBL)
- Real-time Blackhole List (RBL)
- Abuse Triggered Blocking (SSHGuard)
- Statistics Based Blocking (Subnet blocking)



The Future – Requirements

- We need a decentralized trust model
- Charging needs to be done at sender

  (like in the real world)
- Trust can only be set by human beeing and relation set.
- Automatic Autonomious Detection at

  hosts around the net to gather robust(er) information.

The Future – Framework Idea

- P2P based distribution system.
- Charging by sender (BitCoins?) or using space requirements (mail2000 anyone?).
- Grid of systems detecting attacks and sharing this information in realtime into the p2p grid.
- Based on the trust model and the rule set of the site-owner he could build the groundworks for defence.

Thanks & Homework

- Bring your design to the table.
- Alter your setup to trust others.
- Bring your problems on the table.