

Community Based Blacklists

Open Community Camp 2012



Rick van der Zwet <info@rickvanderzwet.nl>

Made Using/At/With



wifisoft
.org

Today's 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

```
POSSIBLE BREAK-IN ATTEMPT!  
Jul 24 15:31:39 riff sshd[85403]: Invalid user woojin from 59.175.218.166  
Jul 24 15:31:44 riff sshd[85405]: reverse mapping checking getaddrinfo for 166.218.175.59.broad.wh.hb.dynamic.163data.com.cn [59.175.218.166] failed  
POSSIBLE BREAK-IN ATTEMPT!  
Jul 24 15:31:44 riff sshd[85405]: Invalid user fernando from 59.175.218.166  
Jul 24 15:31:50 riff sshd[85408]: reverse mapping checking getaddrinfo for 166.218.175.59.broad.wh.hb.dynamic.163data.com.cn [59.175.218.166] failed  
POSSIBLE BREAK-IN ATTEMPT!  
Jul 24 15:31:50 riff sshd[85408]: Invalid user thomas from 59.175.218.166  
Jul 24 15:31:56 riff sshd[85410]: reverse mapping checking getaddrinfo for 166.218.175.59.broad.wh.hb.dynamic.163data.com.cn [59.175.218.166] failed  
POSSIBLE BREAK-IN ATTEMPT!  
Jul 24 15:31:56 riff sshd[85410]: Invalid user ferdinando from 59.175.218.166  
Jul 24 15:32:01 riff sshd[85412]: reverse mapping checking getaddrinfo for 166.218.175.59.broad.wh.hb.dynamic.163data.com.cn [59.175.218.166] failed  
POSSIBLE BREAK-IN ATTEMPT!  
Jul 24 15:32:01 riff sshd[85412]: Invalid user pedro from 59.175.218.166  
Jul 24 17:07:00 riff sshd[85697]: Accepted publickey for tunnel from 77.166.174.177 port 14878 ssh2  
Jul 24 18:03:07 riff sshd[85877]: Accepted publickey for rvdzwet from 2001:7b8:2ff:8446:d69a:20ff:fe5a:3fcf port 34859 ssh2  
riff%
```

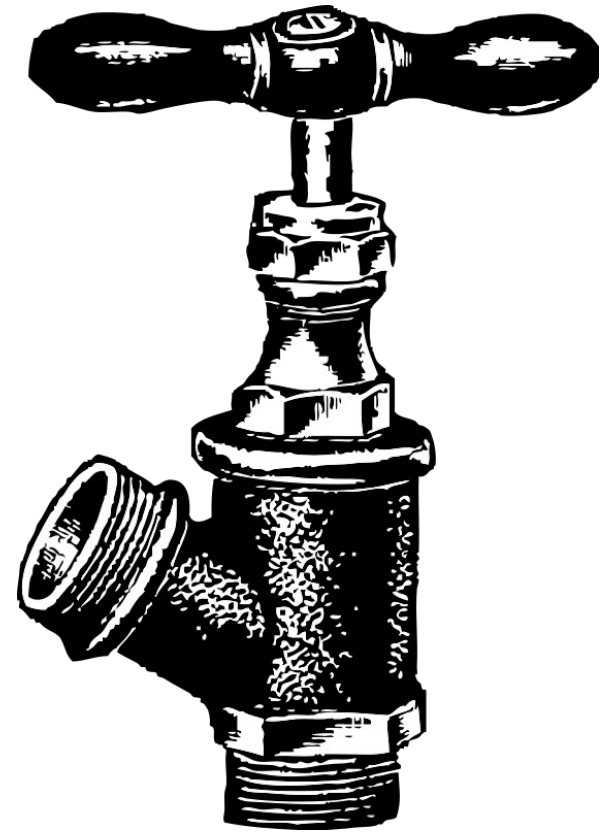
The Problem: Trust Models

- The Internet is open and blocking parts of it could be considered harmful (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 being and relation set.
- Automatic Autonomous 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.

