

# Conception of Anti-Spam Solutions

Lento Yip  
Vice Chairman  
HKISPA  
[lento@hkispa.org.hk](mailto:lento@hkispa.org.hk)



Hong Kong  
Internet Service  
Providers Association

# Agenda

- **The broad categories of solutions – Blacklists, Cooperative, E-mail body, database, administrative.**
- **What can you do ?**
- **Q & A**



Hong Kong  
Internet Service  
Providers Association

# Blacklists

- **DNS based, IP based**
- **Free or subscription**
- **Pros : Easy deployment**
- **Cons : Kill the wrong mails**
- **Spam sources – Complaints, Honey Pots**



Hong Kong  
Internet Service  
Providers Association

# Cooperative Approach

- **Signature based, content based**
- **Synergy effect**
- **Has a network of central servers sharing information**
- **Can be utilized by both servers and end-users**
- **Computationally more costly**
- **More accurate**

# Cooperative Approach

- **Spamnet – Spam or not**
- **Pyzor – Spam or not**
- **DCC – Count All**
- **Not always free**
- **Spam Sources – Signatures from mail clients and servers, honey pots.**



Hong Kong  
Internet Service  
Providers Association

# E-mail Body Analysis

- **Header Forgery – Received, Scanned, false message ids, etc.**
- **Unusual Format**
- **Header IPs**
- **Language etc**



Hong Kong  
Internet Service  
Providers Association

# Database Methods

- **Content based**
- **Break content into tokens in a logical way**
- **Verify the tokens with the database to decide spam probability**
- **Identified spam/ham is again used to train the database**
- **Spam sources – honey pots, complaints**

# Administrative Measures

- Rate limiting of e-mail servers, both in and out
- Connection control – e.g. each IP can only make two connections to your server
- SMTP Authentication – Not always practical
- Greylisting – Do not accept for the first time
- Confirmation for initial e-mail delivery – Not really practical, for e.g. mailing lists

# What can you do ?

- **Evaluate your situation and use some or combinations of the solutions**
- **Reference Figures – If all of the methods employed, spam filtering rate can reach 97% with zero false positives**



Hong Kong  
Internet Service  
Providers Association