Fachhochschule Gelsenkirchen

IP Reputation Exchange
→ e-mail security research …

Prof. Dr. Norbert Pohlmann

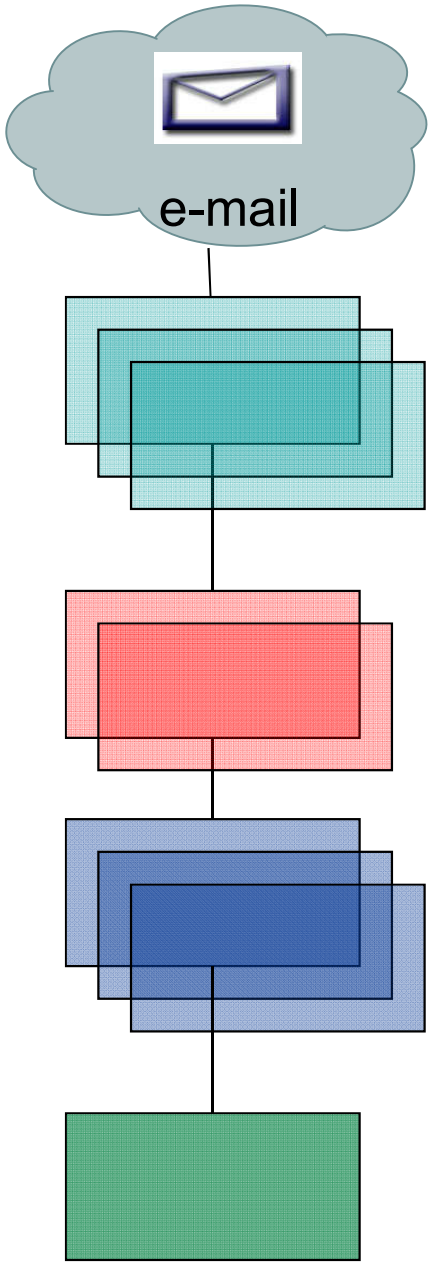
Institute for Internet Security – if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Content

- IP Reputation (general Idea)
- Current best practice
- IP Reputation Exchange (Idea, Approach, Results)
- Summary

Anti Spam Technology
→ Model of different levels



e-mail gateway / e-mail proxy

- Network level (IP-Address)
  - Black lists
  - Reverse MX
  - Frequency analysis
- SMTP level
  - Check HELO
  - Check sender e-mail address (black-/white-/grey list)
  - Check recipient e-mail address (DB, LDAP)

1

Spam filter

- Check of header and content level
  - Heuristically e-mail header and content analysis
  - Statistical methods
  - Checksum comparison

2

Virus scan

- Check e-mail for virus

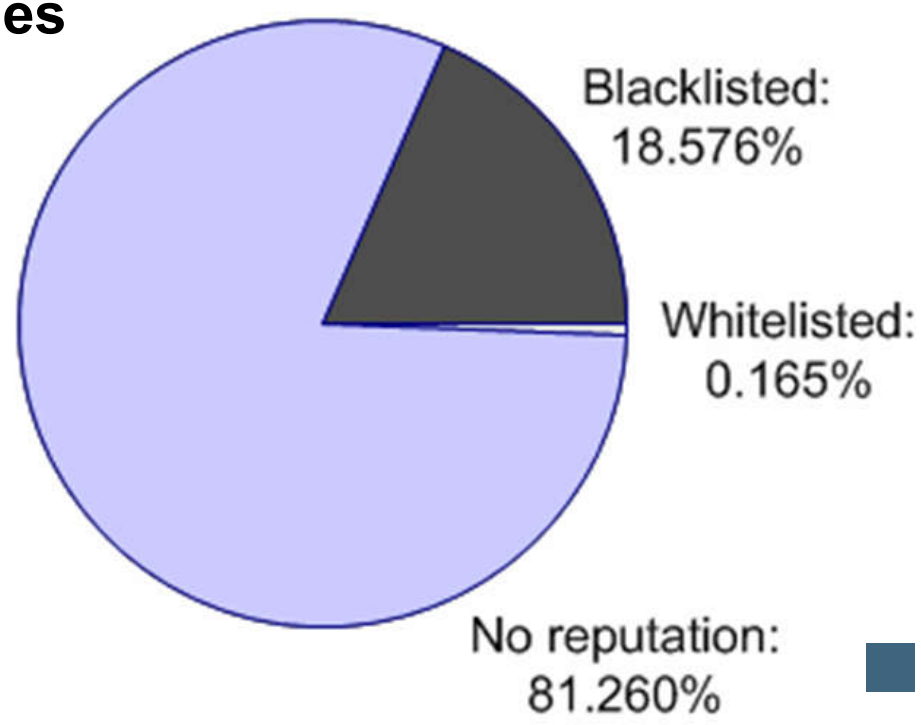
3

use of resources

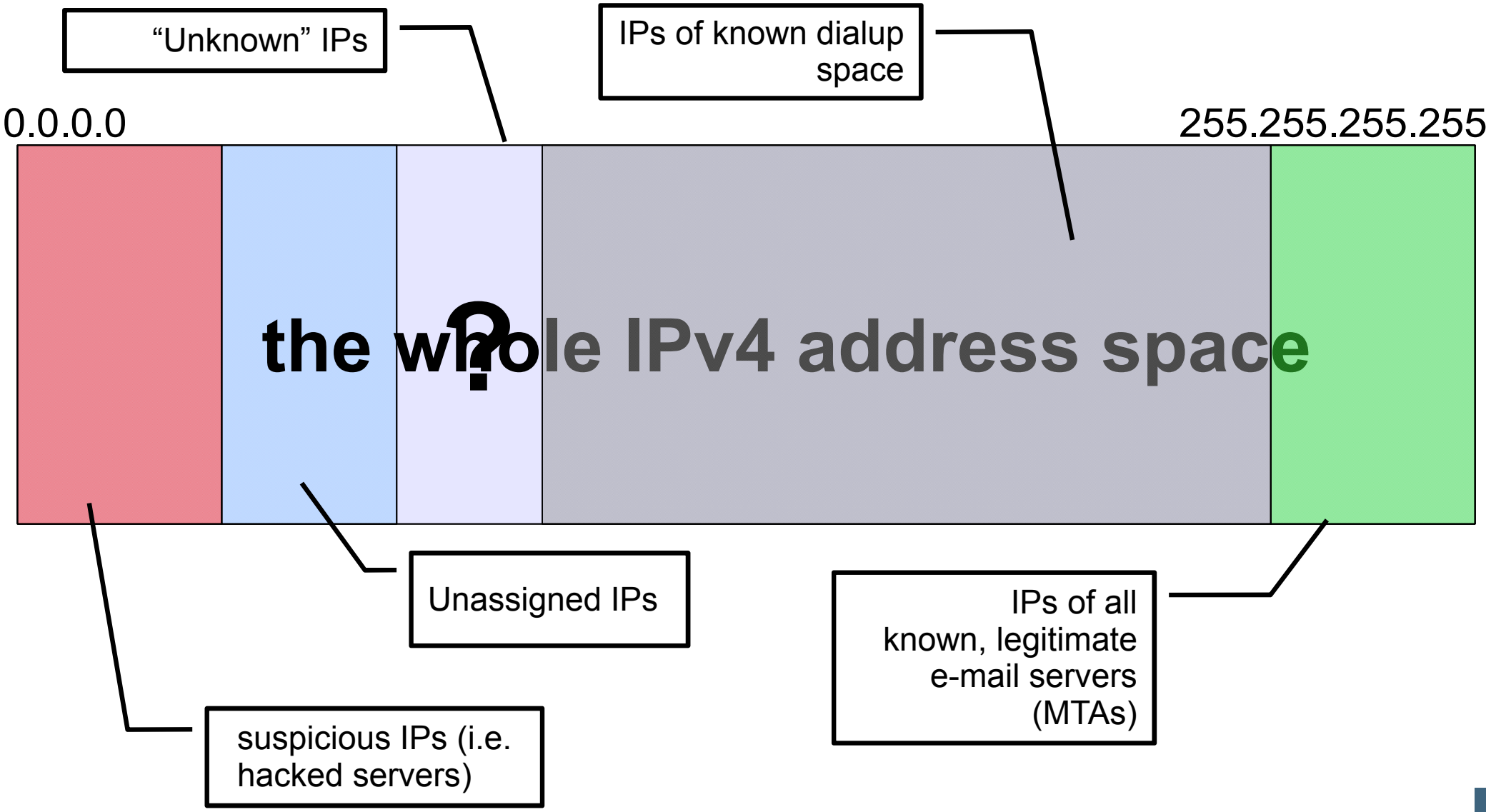
Internal e-mail server

IP Reputation
→ Idea

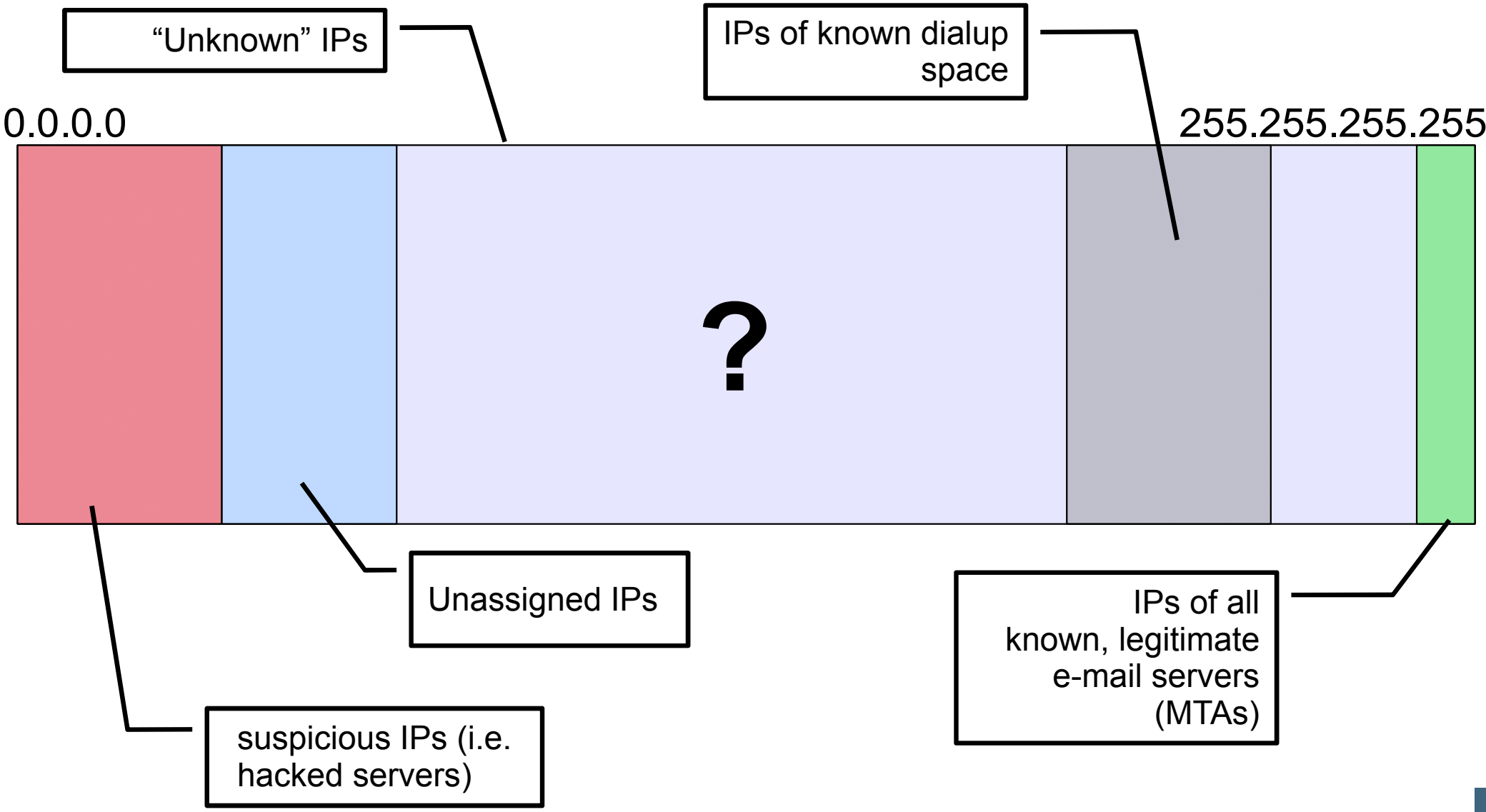
- Combining black und white listing is one of the most efficient anti spam mechanisms
- ***However***
  - High dependency on black/white list providers
- **Aggregation of the most important black lists**
  => only 19% of advertised IPv4 addresses can be judged concerning e-mail reputation!
- **More IP reputation attributes and IP space are needed!**
- **Less dependency on single Provider is also important.**



IP Reputation
→ The IP map (possible attributes/space)



IP-Reputation
→ The IP map (attributes/space today)



E-mail infrastructure
→ Some figures

- Port 25 state analysis (incoming)
- German research „ISP“ - DFN (Deutsches Forschungsnetz)
- 0.08% of all IP addresses respond to a connection attempt on port 25
  - Every 1250th IP address „is“ a mail server (open port 25)

- **Challenges**
  - (every) open port 25 = SMTP
  - How many different IP addresses belong to one host?
    (timing measurement problems, honeypots/honeynets, …)

E-mail infrastructure
→ Some thoughts

- **Fact:**
  - 1.752 billion IPv4 addresses advertised (as of 2007-08)
- **Assumption:**
  - 0.08% of all IPv4 addresses speak SMTP (incoming)
- **Result:**
  - ~1.4 million IPv4 addresses that speak SMTP (incoming)

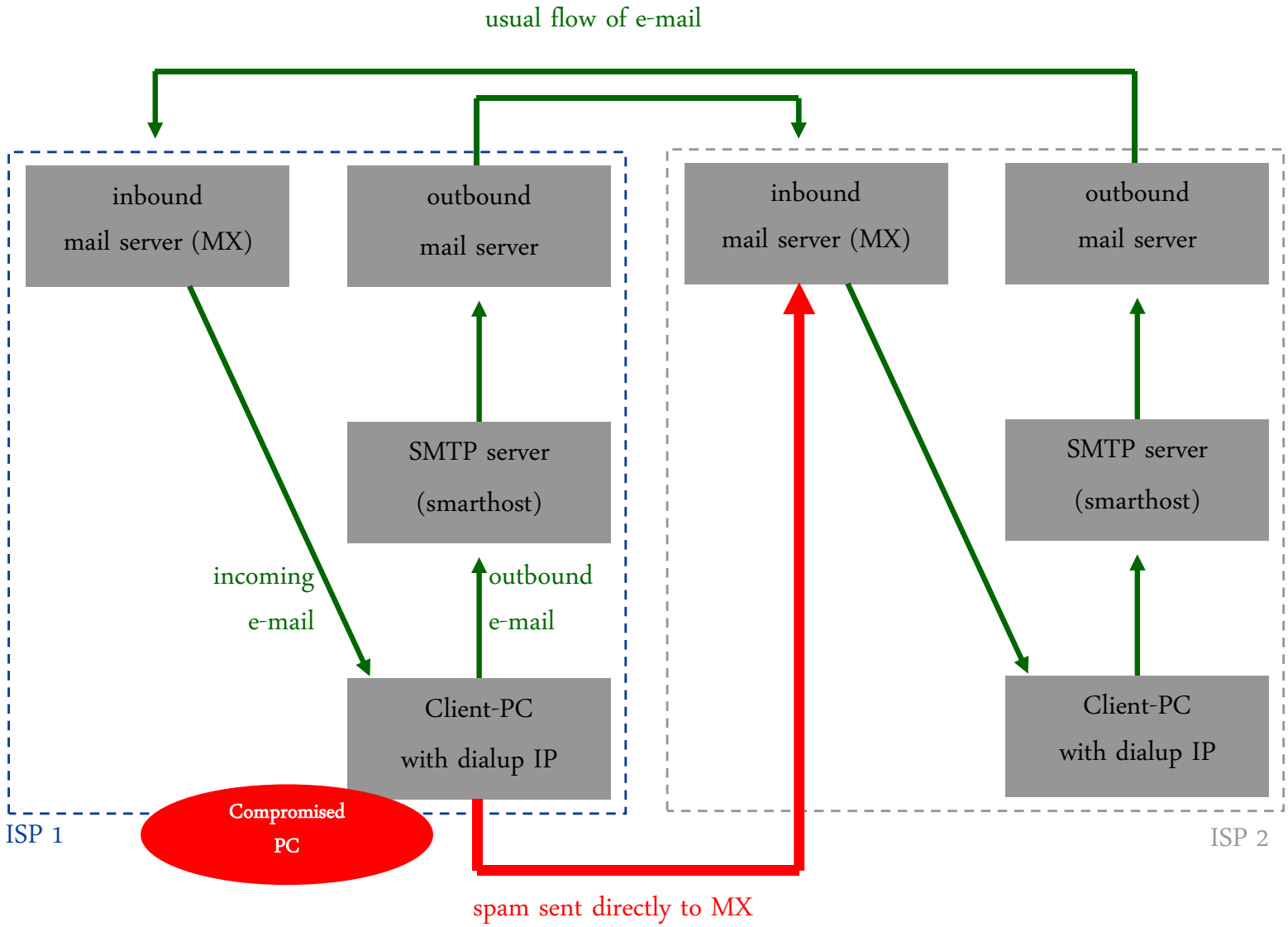
➔ **~1.4 million legitimate e-mail servers**

The main source of spam
→ Dialup IPs

- Over 90% of all spam originates come from dialup IP addresses (bots)
- Bots send spam on a large scale to the inbound e-mail servers (MX) of e-mail service providers
- Smart hosts are omitted
- PCs get a (dynamic) dialup IP address when connecting to the internet

- **Conclusion**
  - **Dialup-IPs never send legitimate e-mail to inbound e-mail servers (MX)**
  - **Blocking dialup IP addresses has no major drawback!**

Spam from dialup IPs
→ Spam sent directly to MX

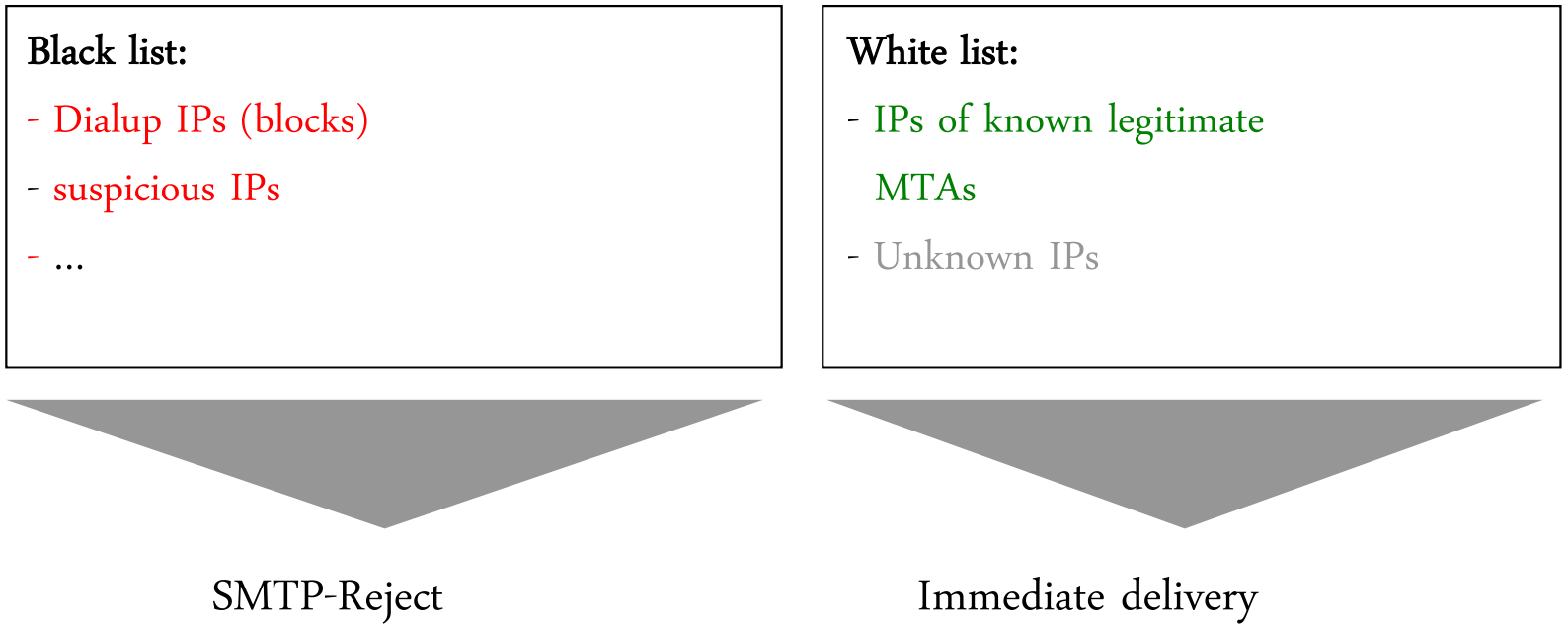


Content

- IP Reputation (general Idea)
- **Current best practice**
- IP Reputation Exchange (Idea, Approach, Results)
- Summary

Current best practice (1/4)
→ Black & white list

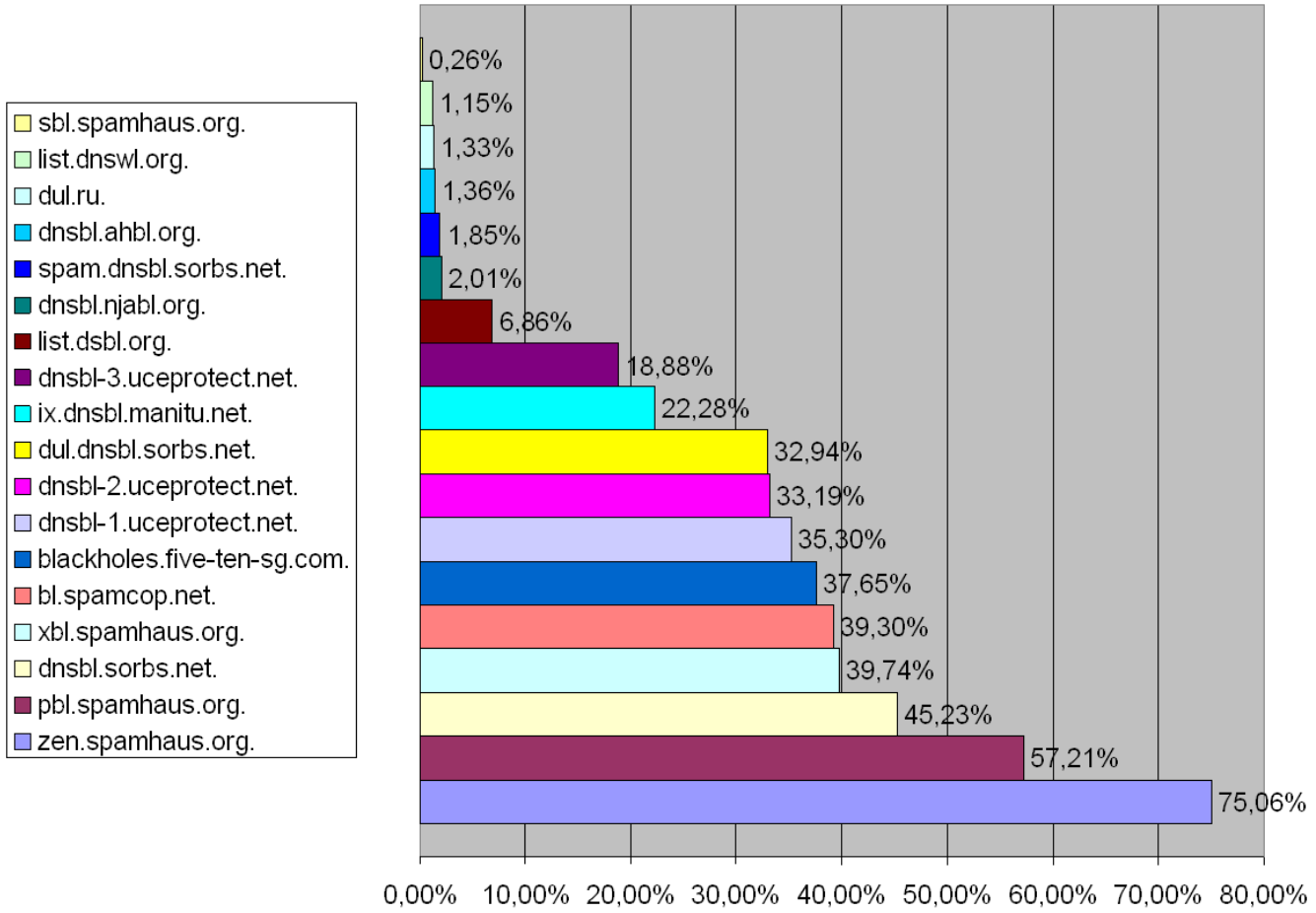
- E-mail service providers categorize IP addresses (Mail-Gateways) into black and white lists



Current best practice (2/4)
→ IP maps of Mail-Gateways

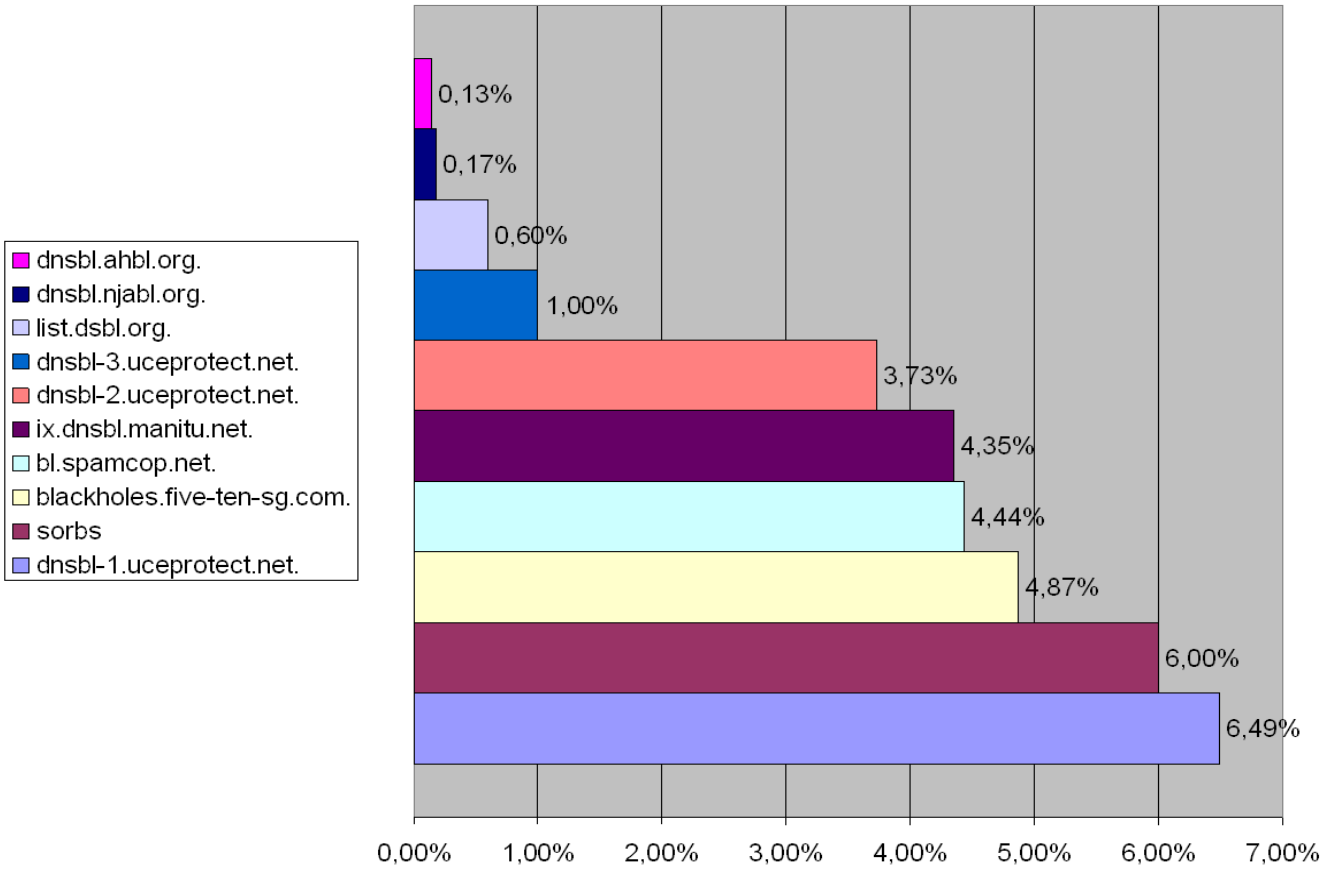
- Known e-mail gateways IP addresses are based on experience or observation of the ISP landscape
- Connections from unknown or non-suspicious IP addresses are allowed (e-mails are accepted)
- An entry on the black list depends on monitored spam activity (user complaints, amount of e-mails, frequency analysis, valid e-mail addresses, etc.)

Current best practice (3/4)
→ Combining multiple (black) lists



- One black list alone blocked 75%
- Others block less than 75%
- What is the gain in terms of blocking spam by using multiple lists?

Current best practice (4/4)
→ Combining multiple (black) lists



- Gain in blocking spam using multiple black lists
- Using a second list blocks +6.5%, a third +6%, a fourth +4.8%
- **Result: Combining multiple black lists makes sense!**

Potential of IP maps

- The rate of detected spam mails must be enhanced
- Spamming IP addresses should be identified much quicker than today
- A European or even international IP map should be established in order to fight spam in general and for long term

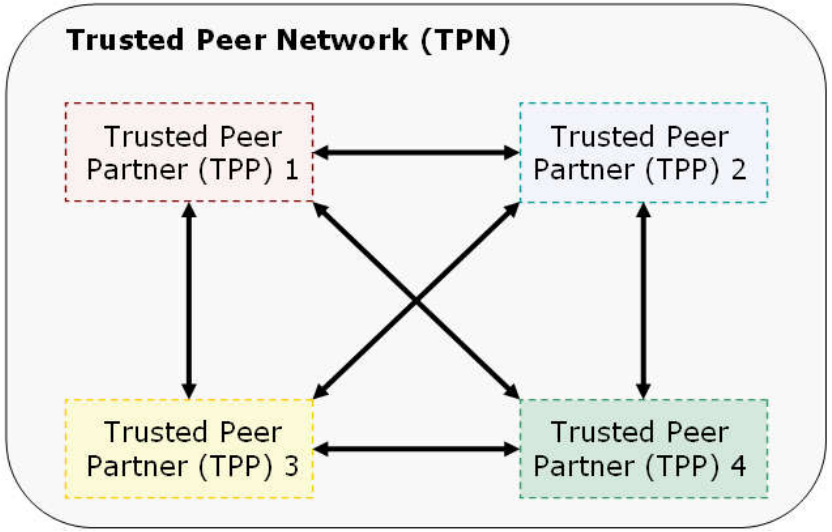
- **Action**
  - **Exchange of IP maps between ISPs world-wide**

Content

- IP Reputation (general Idea)
- Current best practice
- **IP Reputation Exchange (Idea, Approach, Results)**
- Summary

Distributed IP reputation system → Idea

- The distributed IP reputation system consists of a **network of participants** (**Trusted Peer Network**), which helps to get **describing attributes of IP addresses**.
- Therefore it is based on participants **sharing their view on the whole internet**, expressed in categorizing IP addresses.
- The **idea** of the distributed IP reputation system is to **share information held by many different providers** (**Trusted Peer Partner – TPP**).
- Sharing in detail means to pool single IP lists of the participants between other participants and to **achieve a most detailed and complete IP list** by aggregating this information.
- The working time of providers would be shared and **suspicions about spam sources** could be **amplified** or **weakened** by other parties.



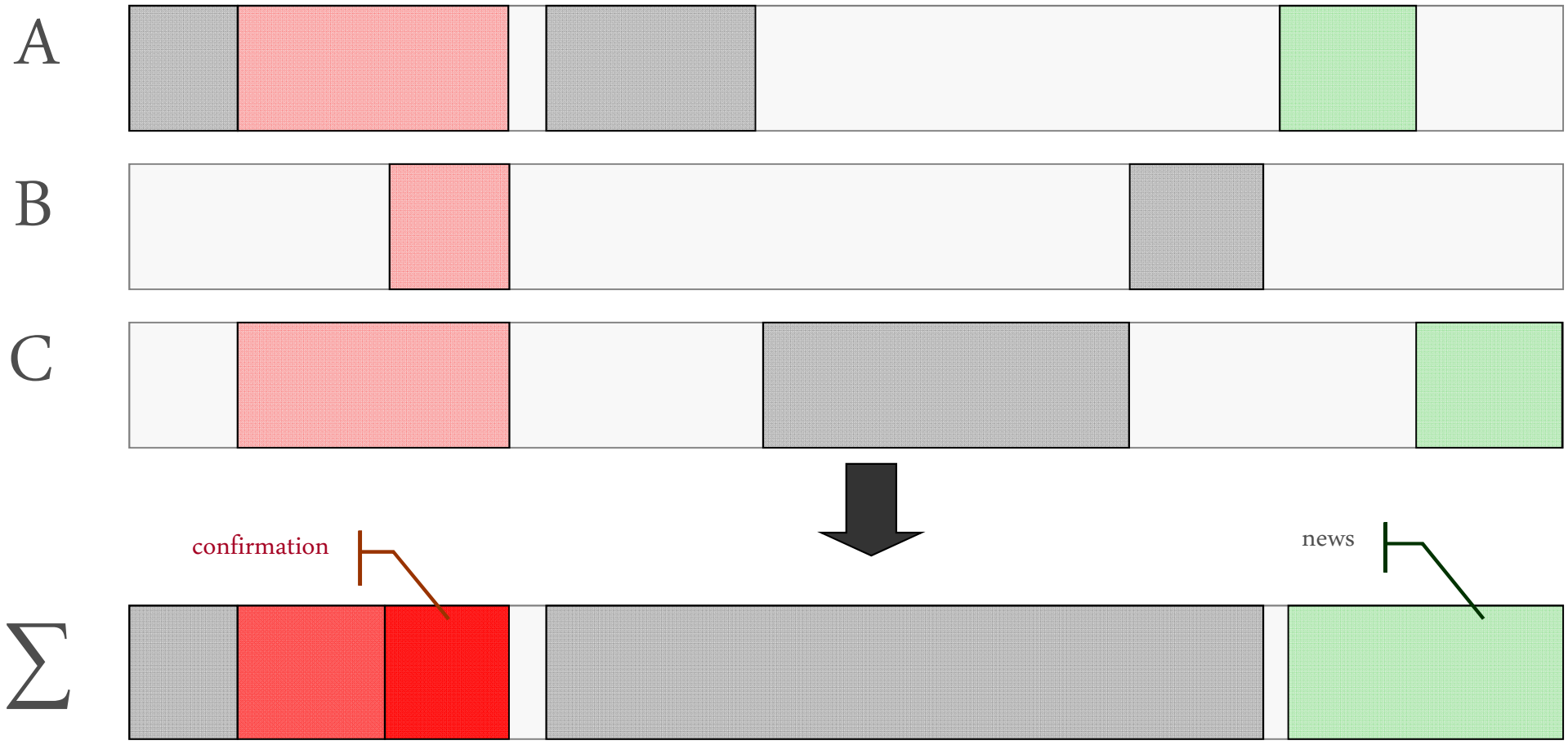
Distributed IP reputation system
→ Self-declaration data / observation

- ISPs exchange self-declaration information as well as observation regularly.
- In fact, these are lists of IP addresses with describing attributes (IP reputation).

Self-declaration data	Observation
- IPs of outbound mail servers - Dialup-IPs (blocks) in addition maybe: - Static IPs, ...	- suspicious IPs - IPs of non-maintained mail servers - ...

- The self-declaration data may be checked against routing information.
- What are the advantages to exchange this kind of information?

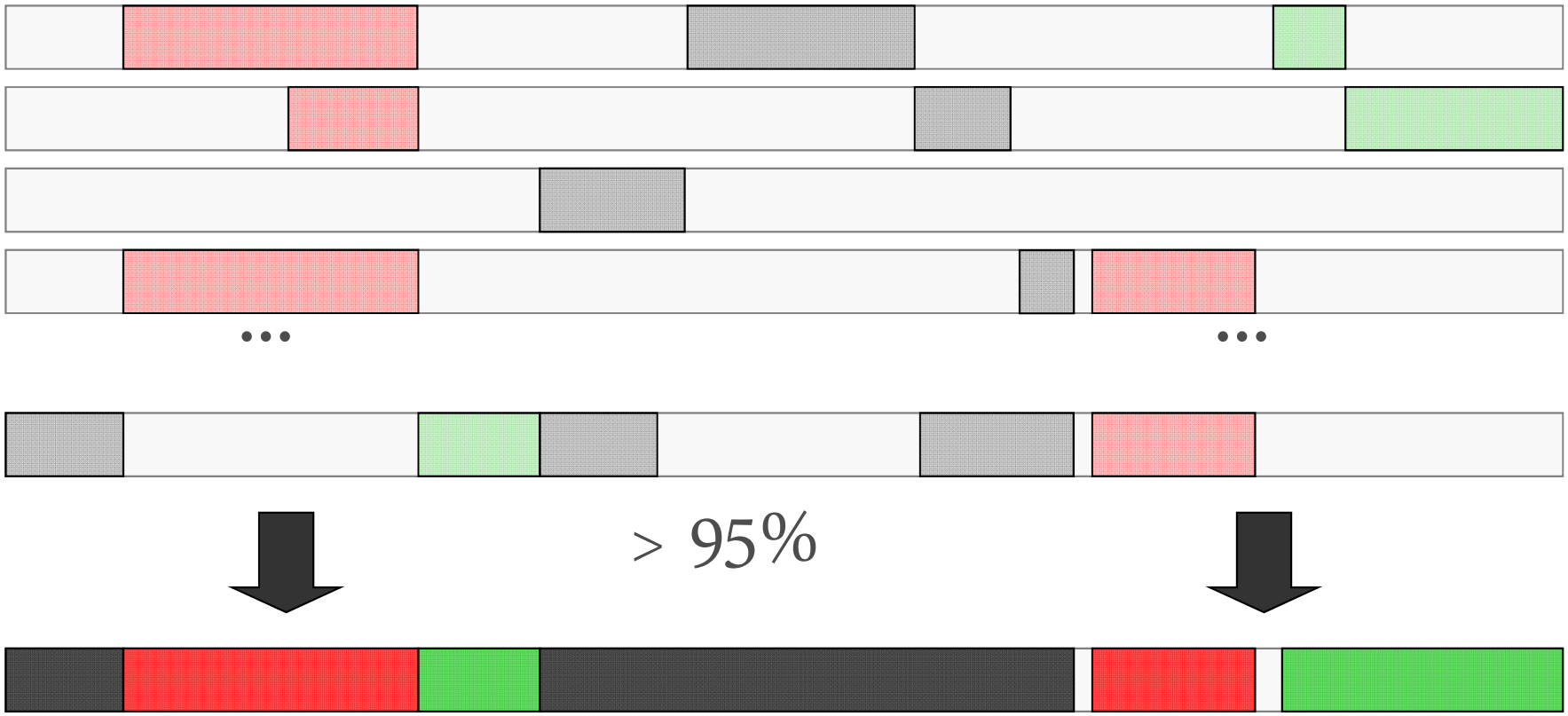
Distributed IP reputation system
→ Interpretation of „IP maps“ (1/2)



- Assessing the IP maps results in a confirmation of possible spam sources or reduce own observations (false positives)
- Shows new potential spam sources

Distributed IP reputation system
→ Interpretation of „IP maps“ (2/2)

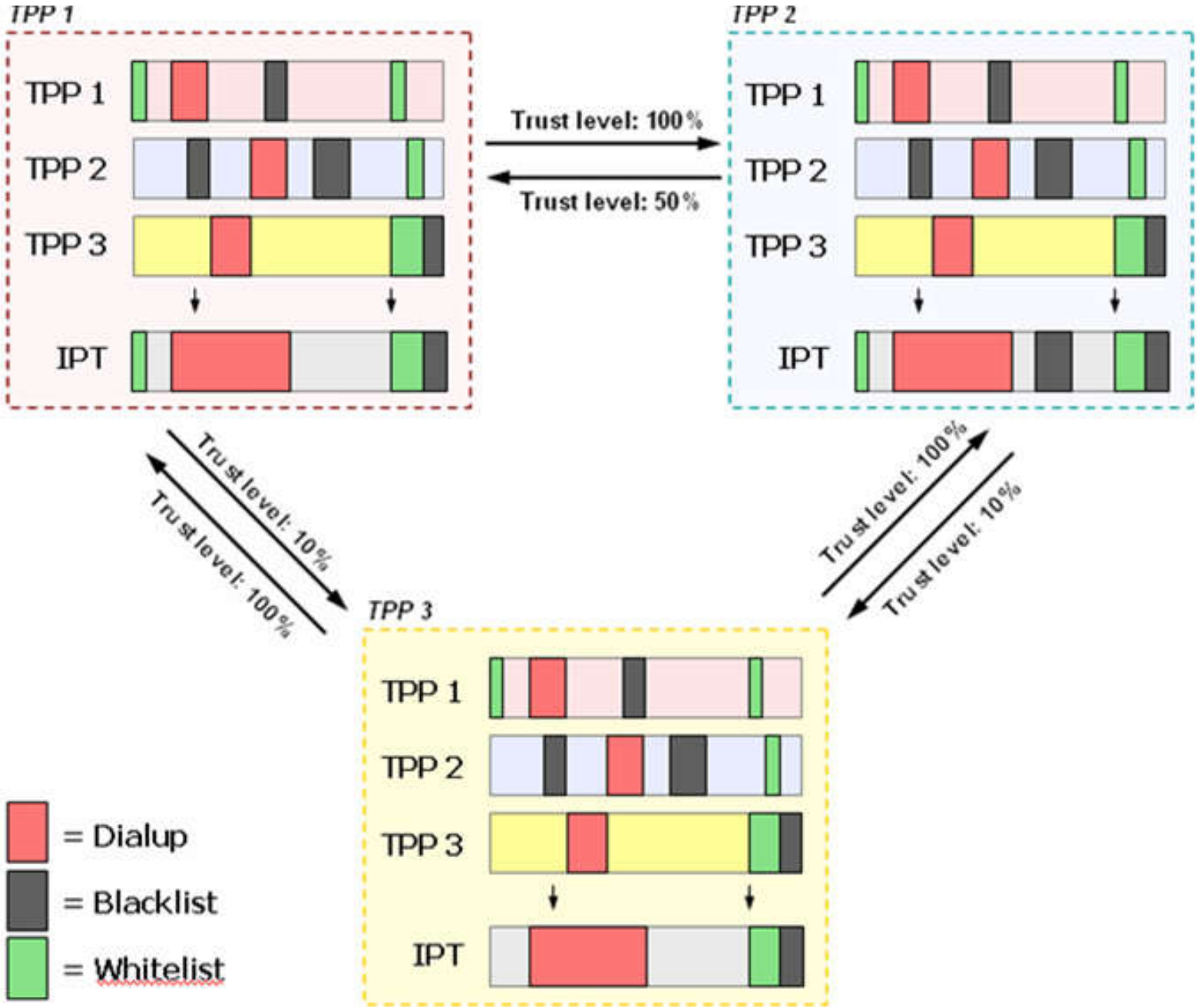
- Incoming self-declaration information as well as observations are aggregated into a composite IP map, with a better reputation of IP addresses.
- The higher the participation, the better for all users!
- **Aim: (nearly) complete IP map for the whole IP address space.**



Types of information
→ Describing attributes

- **Black list - attribute**
  - Describes IP addresses to be blocked permanently (i.e. > 1 week)
- **White list - attribute**
  - Describes legitimate outbound e-mail servers
  - Valid until withdrawn …
- **Spam activity - attribute**
  - Short-dated (i.e. less than 1 week)
  - Reasons: unexpected high traffic, high bounce rate
  - Many spam activity statements from several nodes of the network may lead to blocking the IP address in question
- **Dialup - attribute**
  - IP address blocks used for dialup
- **Neutralization / Withdrawal**
  - Statements can be corrected/withdrawn

Example: Distributed IP reputation
→ 3 partner with different trust level



Distributed IP reputation system
→ Benefits

- As a **Semi-Closed User Group** the IP map is open to all ISPs
- Even with a small number of participants, a high amount of suspicious IP addresses are detected and thus a quick and effective identification of spam sources is in place.
- Self-declaration information mitigates the risk of false positives.
- Every participant is free concerning the use of data
  (not only to block spam, but also spam over internet telephony (spit)?)

- **Distributed IP reputation system:**
  - **no central point of failure** prevent from misuse by single participants
  - **enhances availability** of the distributed IP reputation system

Content

- IP Reputation (general Idea)
- Current best practice
- IP Reputation Exchange (Idea, Approach, Results)
- **Summary**

Summary

- **Spam mail is a complex problem of the global internet.**
- **The new concept of distributed IP reputation system**
  - **makes black and white listing robust, trustworthy and manageable**
  - **will help to reduce the spam problem and prevent from damage**
- **What is needed**
  - **International cooperation will be very effective**
  - **More Analysis of communication behavior** of e-mail senders helps to detect and optimize reputation of IP addresses concerning e-mail
- Only together we can solve the spam problem!
- **So let us work together …**

Further information: www.if-is.net, www.internet-sicherheit.de (German)

Fachhochschule Gelsenkirchen

IP Reputation Exchange
→ e-mail security research ...

Thank you for your attention!
Questions?

Prof. Dr. Norbert Pohlmann

Institute for Internet Security – if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Institute for Internet Security
→ e-mail security research topics

- E-mail security in the context of internet security
- Survey (German Government, ENISA)
- Focus on anti spam
- **Current research activities**
  - IP reputation system
  - IP black list analysis for e-mail (RBLDNS)
  - Spamtraps
  - Hamtraps
  - Harvesting
  - E-mail infrastructure throughout the internet
  - Applied Antispam – next generation research MTA
  - Visualization tools for IPv4 address space

Institute for Internet Security
→ Other research topics

- **Internet Early Warning System**
  - Internet Analysis System (IAS)
  - Internet Availability System (IVS)
  - Internet Research
  - Log-Data-Analysis, Intrusion Detection, … for real time analysis

- **Trusted Computing**
  - Turaya (Security Platform based on TPM)
  - Trusted Network Connect (TNC)

- **Other actual topics:**
  - VoIP QoS/Security, Mobile Security, …