

Spam Prevention using Access Code (AC)

Akhtar H Khalil, David J. Parish

a.h.khalil@lboro.ac.uk , d.j.parish@lboro.ac.uk

High Speed Networks Group



**MSN 2008, Coseners
July 10-11, 2008**

Introduction

➤ Spam

- Unsolicited message (Informally)
- No single technical definition
- SPIT (Spam over Internet Telephony)

Problems Caused

- ***Worldwide financial losses caused by spam in 2005 were \$50 billion [Ferris Research Analyzer]***
- **Impacts on business communication**
- **Exposure to Malware, Spyware, Adware**
- **Loss of Corporate Assets**
- **The Legal Risk of Spam**
- **Spam exceeds 4 times legitimate messages** [Johnston and Piscitello, *Understanding Voice over IP Security*]

Impacts of the SOA Anti-spam measures

- **No effective solution against address spoofing, dictionary attacks, sybil attacks etc**
- **May prevent legitimate messages**
- **Example: Members of the British parliament did not receive messages related to “Sexual Offences Bill” under discussion. Assumed to be porn, these messages were filtered by Anti-spam filters.**



**“There is no panacea for the
spam problem, as all
approaches come with some
drawbacks”**

*(Rainer Baumann, St´ephane Cavin and Stefan Schmid,
"Voice over IP - security and SPAM," page 10, September
8, 2006)*

Access Code Mechanism

➤ Two Main Entities

- ❖ User ID (ID)

- ❖ Access Code (AC)

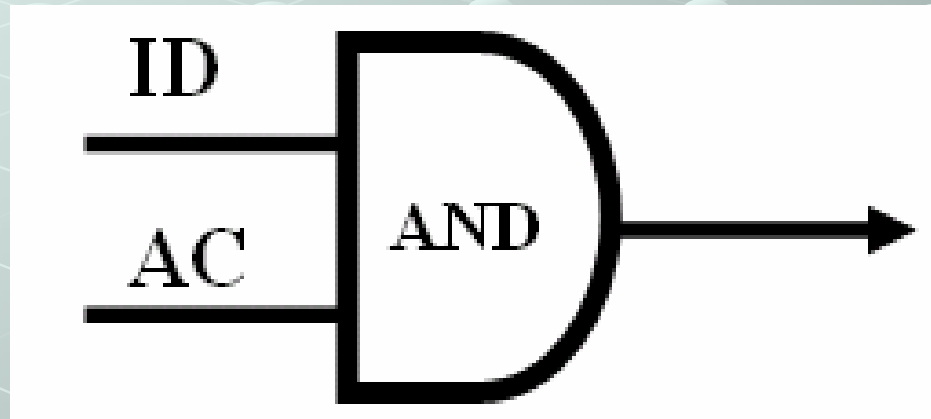


Fig: Basic operation

- User ID:

- ❖ Unique

- ❖ Can be accessed by anyone

Access Code (AC)

- **A 5 digit changeable number**
- **Accessible by legitimate clients**
- **Impossible or so unpleasent for a spammer to access it that he skips and goes away**
- **Changing AC will not affect the legitimate clients**
- **Required by legitimate clients only at the first time**

Spammer Vs Legitimate Client

- A legitimate client has some knowledge about the recipient
- Transmission Cost of spam is almost zero
- Spams are sent to thousands of users within a short time
- It is typically impossible to call a spammer back

Data Base of a User on the Server

Contains three types of lists:

- Trusted Persons List (TPL)
- Blocked Persons List (BPL)
- New Persons List (NPL)

TPL
David

BPL
Eve

NPL

Fig: Data Base of a User on the Server

Call from an Unknown Legitimate Client

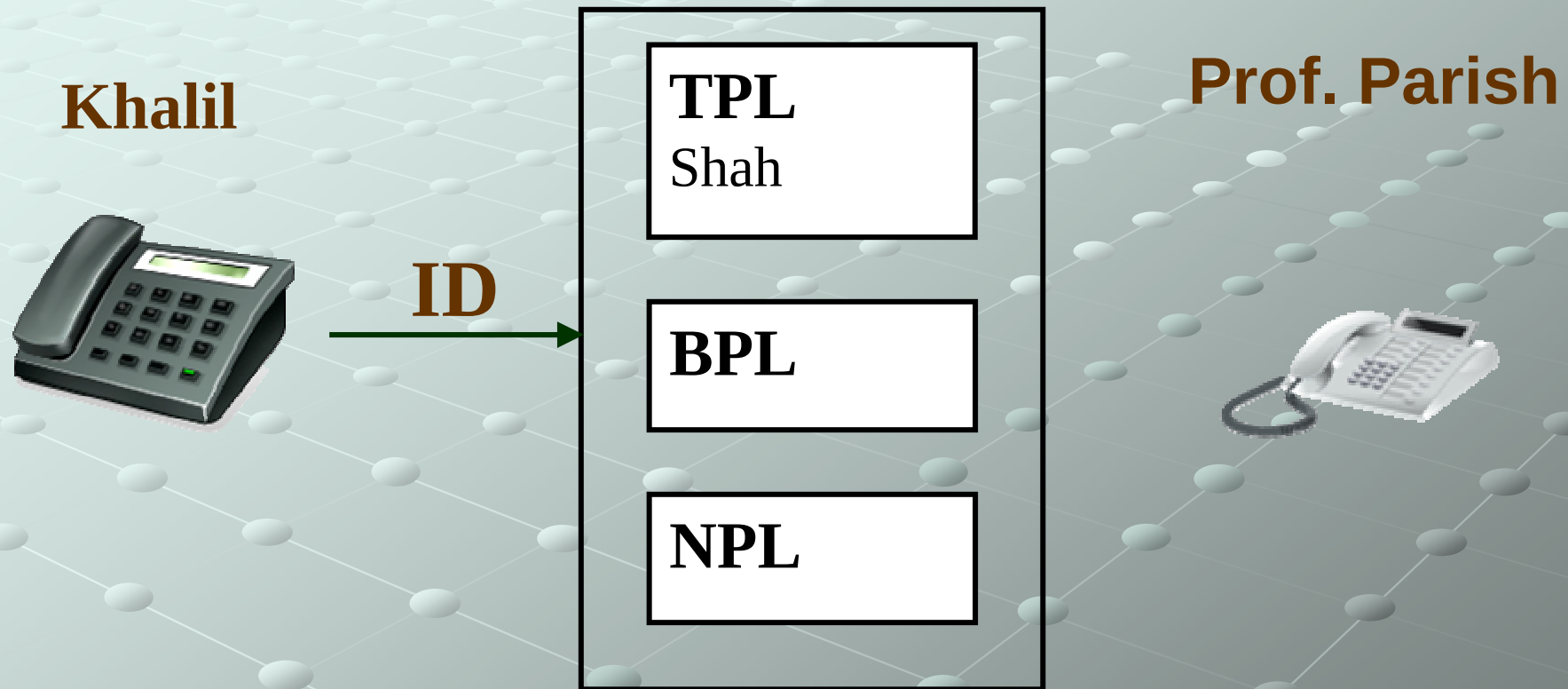


Fig. An unknown person wants to make a call

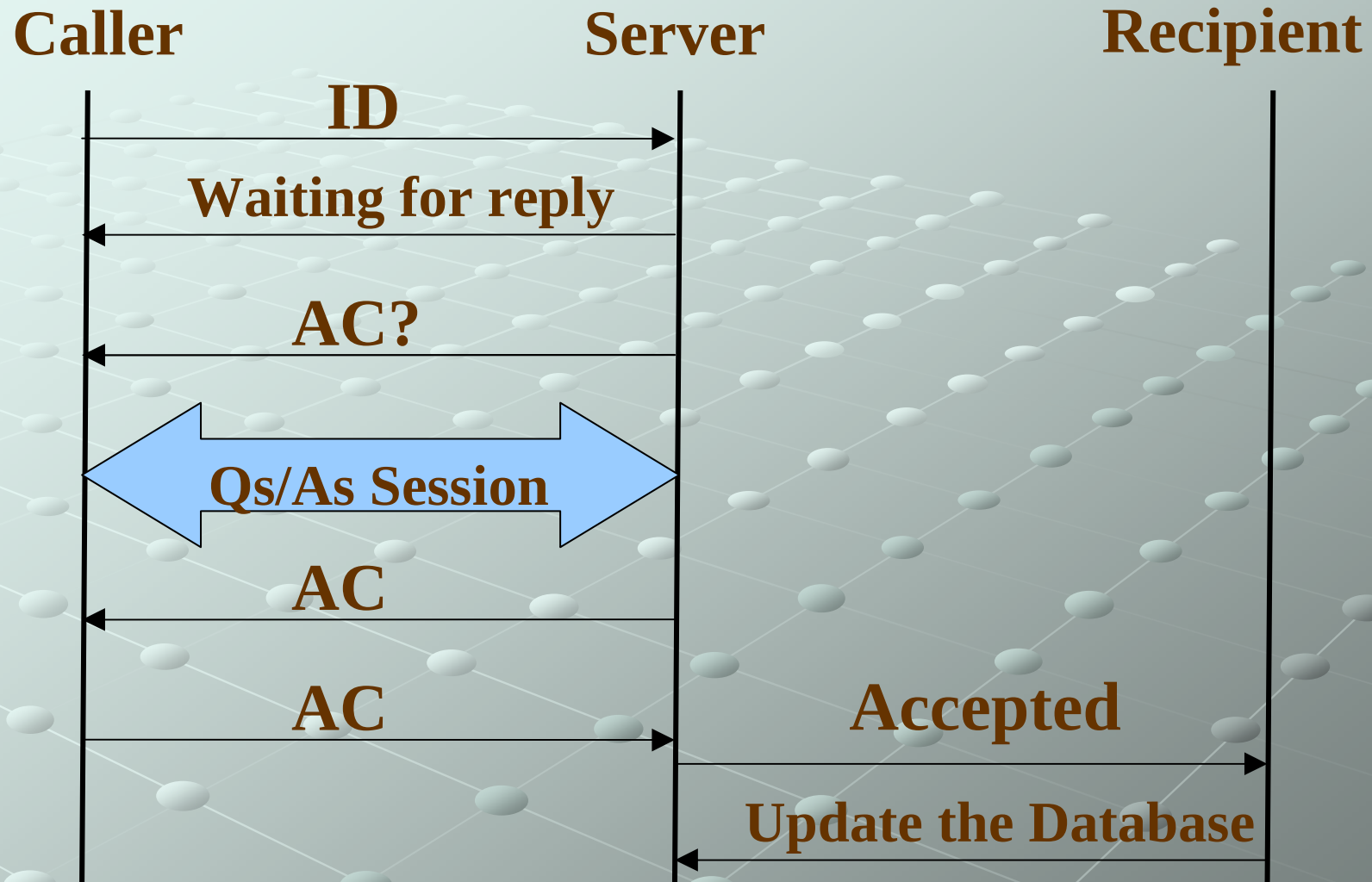


Fig. Accessing AC from the server

Spammer who Accesses the AC

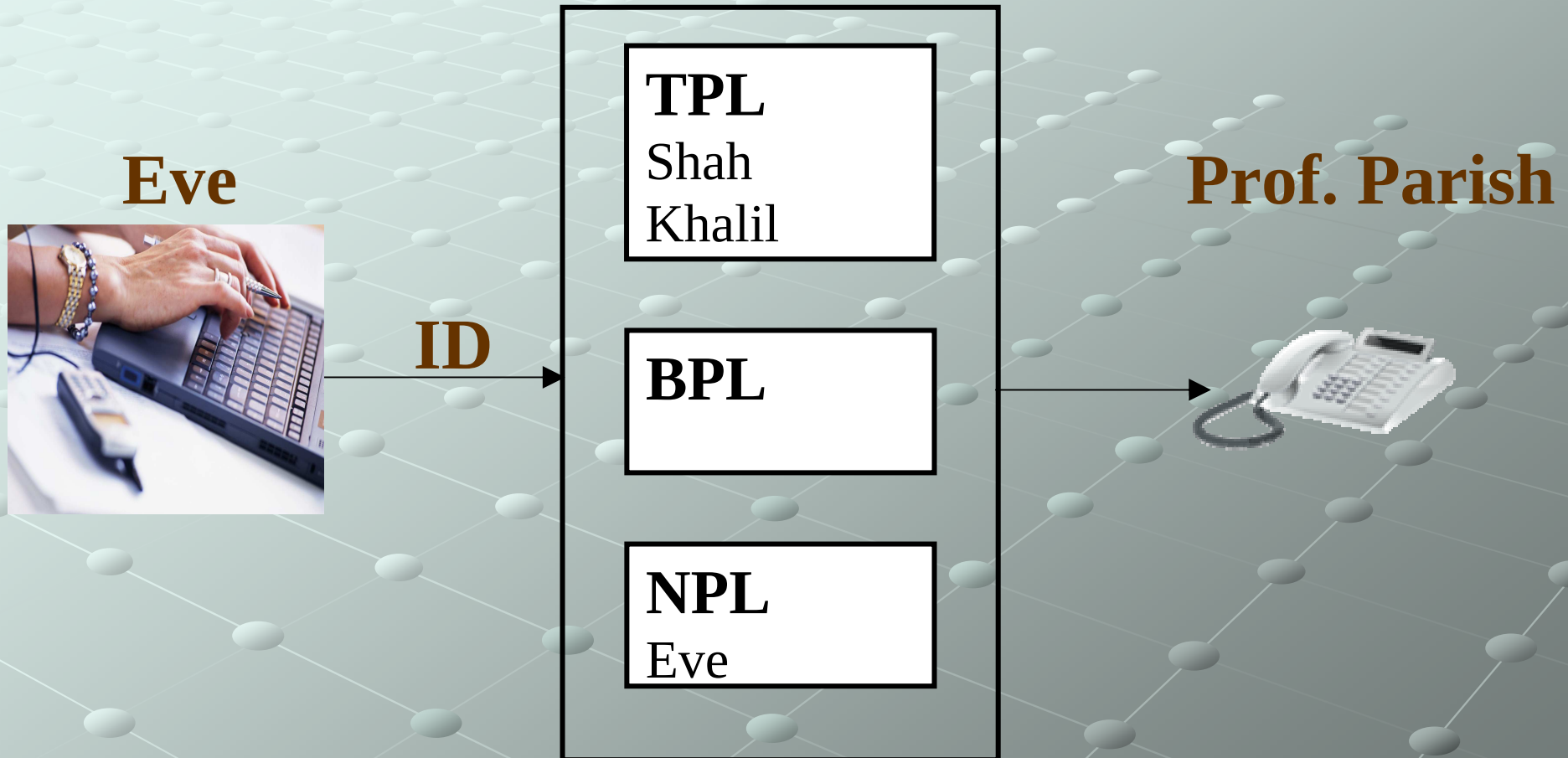


Fig. Eve successfully accesses the AC

Eve Gives Up and Goes Away

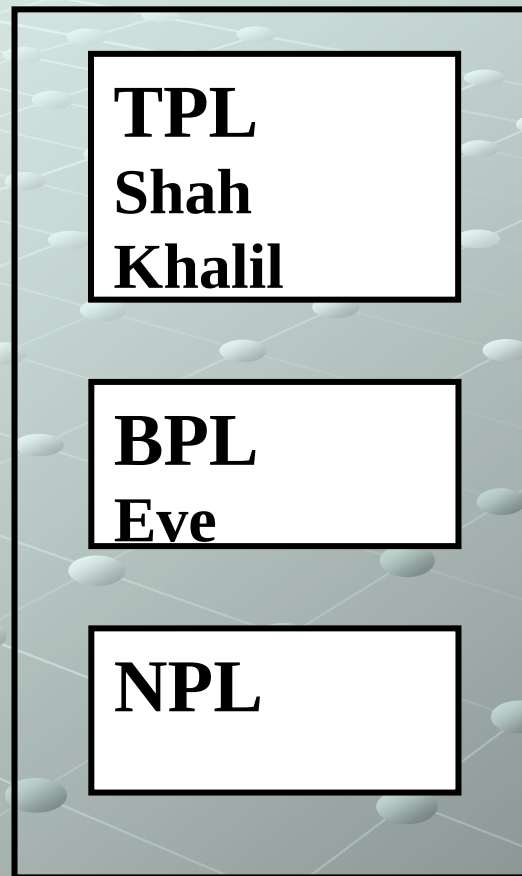


Fig. Data Base of Prof. Parish after receiving spit

Analysis

➤ Charging Mechanism

- ❖ Free tokens to each user
- ❖ Enough for legitimate clients
- ❖ For obtaining AC from the server one token is subtracted
- ❖ If sender is not added to BPL list then the token is returned

Dealing With Address Spoofing

Two cases of Address Spoofing

➤ Spoofed Address not in the TPL

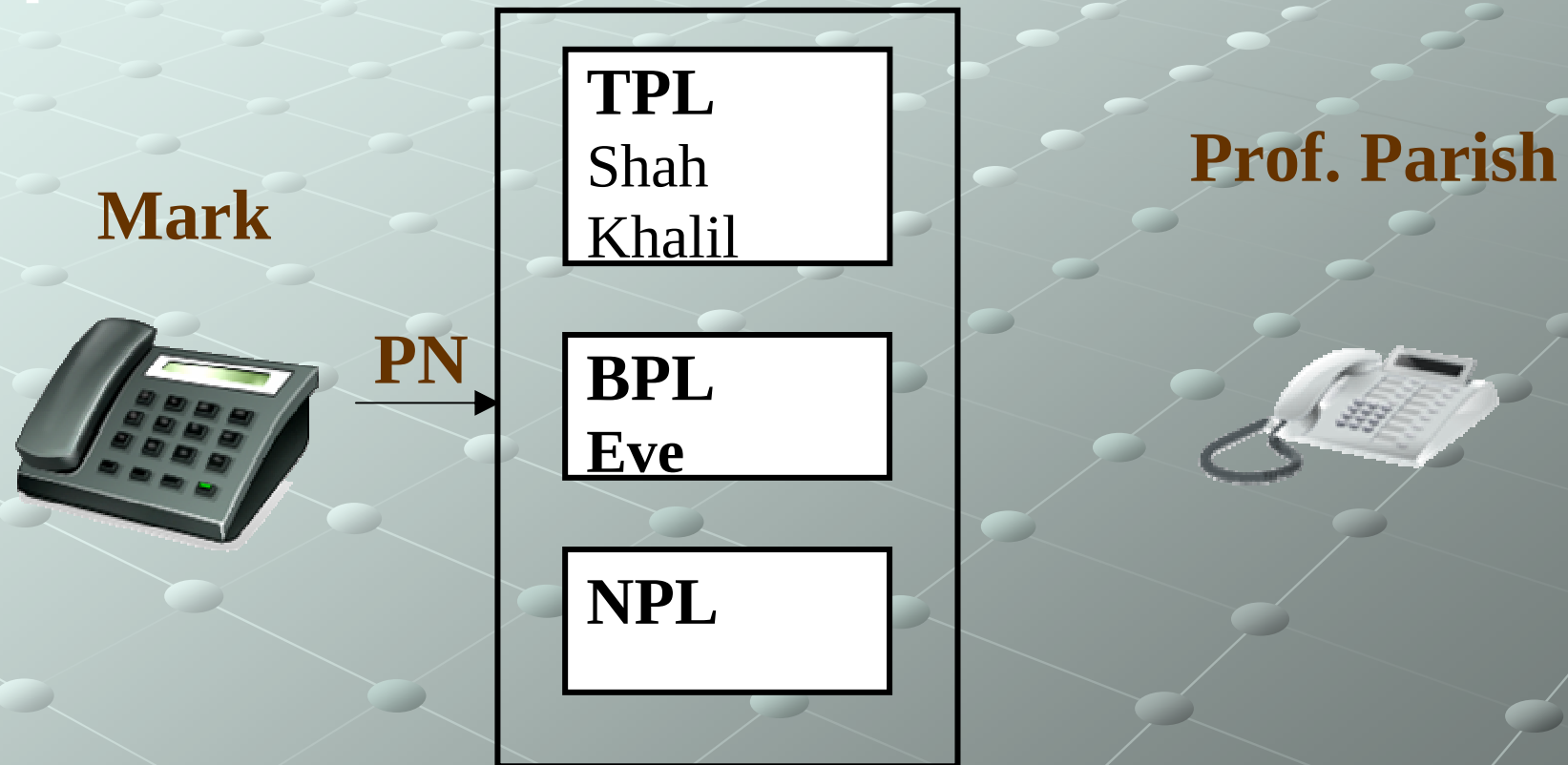


Fig: Server functions as for unknown persons

Spoofed Address is in the TPL

- Knowledge about the TPL list of the recipient
- Time factor

Khalil



PN

TPL

Khalil
Shah

BPL

Eve

NPL

Prof. Parish

TPL

Jin
Wang

BPL

Mev

NPL

Akhtar

TPL

Kostas
Yaqoob

BPL

Eve

NPL

John

Conclusion

- **The only Anti-spam mechanism that prevents all types of spam attacks**
- **The only technique that prevents spam in all its forms (spam email, spit, spim etc).
The most suitable for converged networks**
- **No introduction problem of new callers/users**
- **Does not show any false positive or false negative**
- **Provides the desired degree of convenience to legitimate clients**

QUESTIONS

AND

ANSWERSS

