

# Combating Spam – Latest Trends

THE *Open* GROUP

**Mike Lambert**

A Fellow of The Open Group  
Director, Messaging Forum

GSM +44 7770 451167

[m.lambert@opengroup.org](mailto:m.lambert@opengroup.org)

79, Camrose Way  
Basingstoke  
Hants, RG21 3AW  
United Kingdom

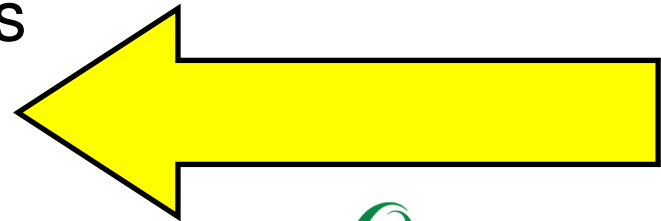
Tel +44 1256 414513  
Fax +44 20 7691 7868  
[www.opengroup.org](http://www.opengroup.org)

THE *Open* GROUP

# What can we do about Spam?

---

- ❑ Current state of the art is Spam filtering
- ❑ Each mail is scored against a number of criteria and mail that exceeds a certain score is treated as Spam
- ❑ Criteria includes
  - Examination of the header
  - Examination of the contents
  - Examination of the source



# Examination of Source

---

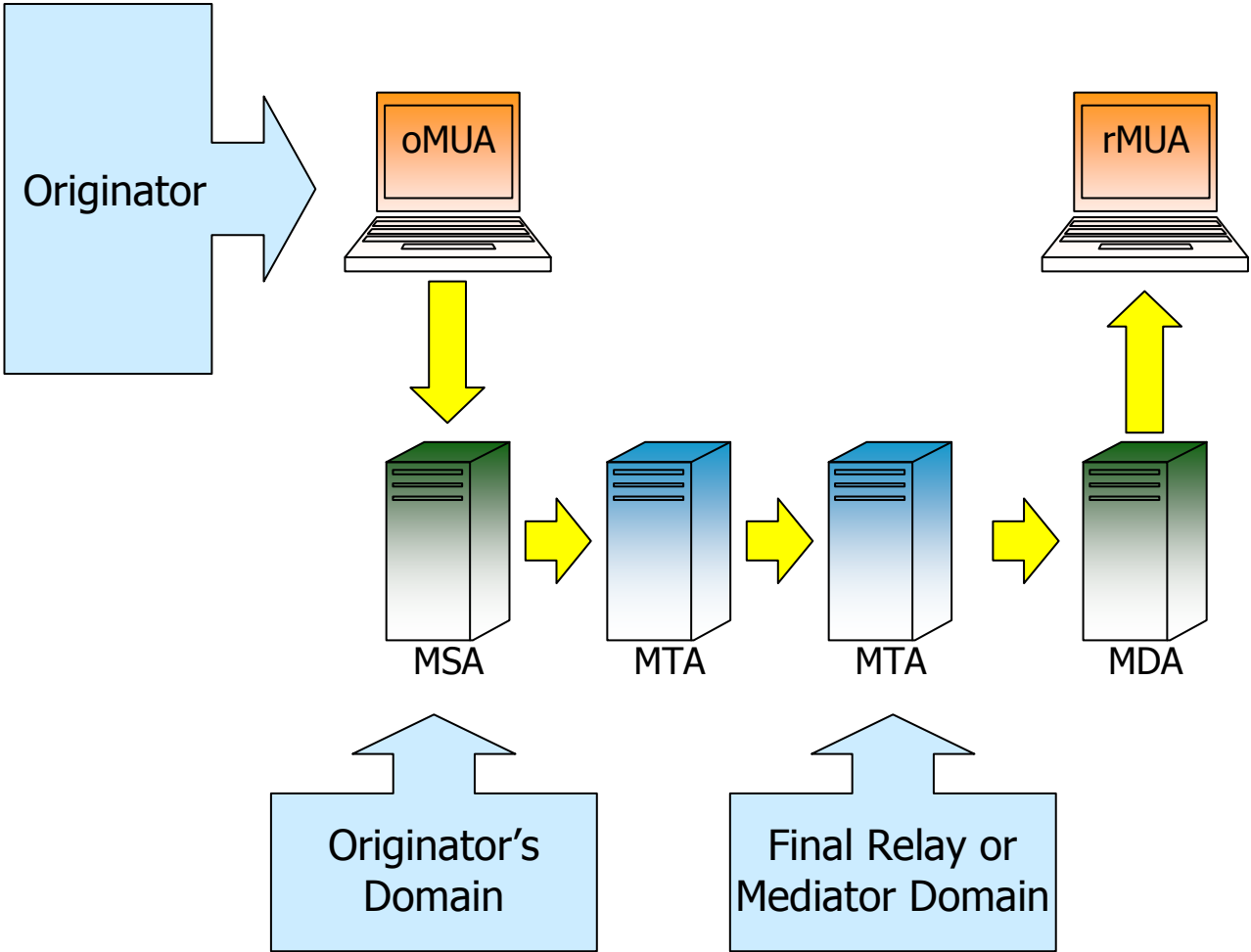
- ❑ Information currently available:
  - IP address of sending MTA (reliable)
  - Identities from the mail headers (easily forged)
  
- ❑ New authentication initiatives are improving the reliability of the sender identity from the mail headers

# Context

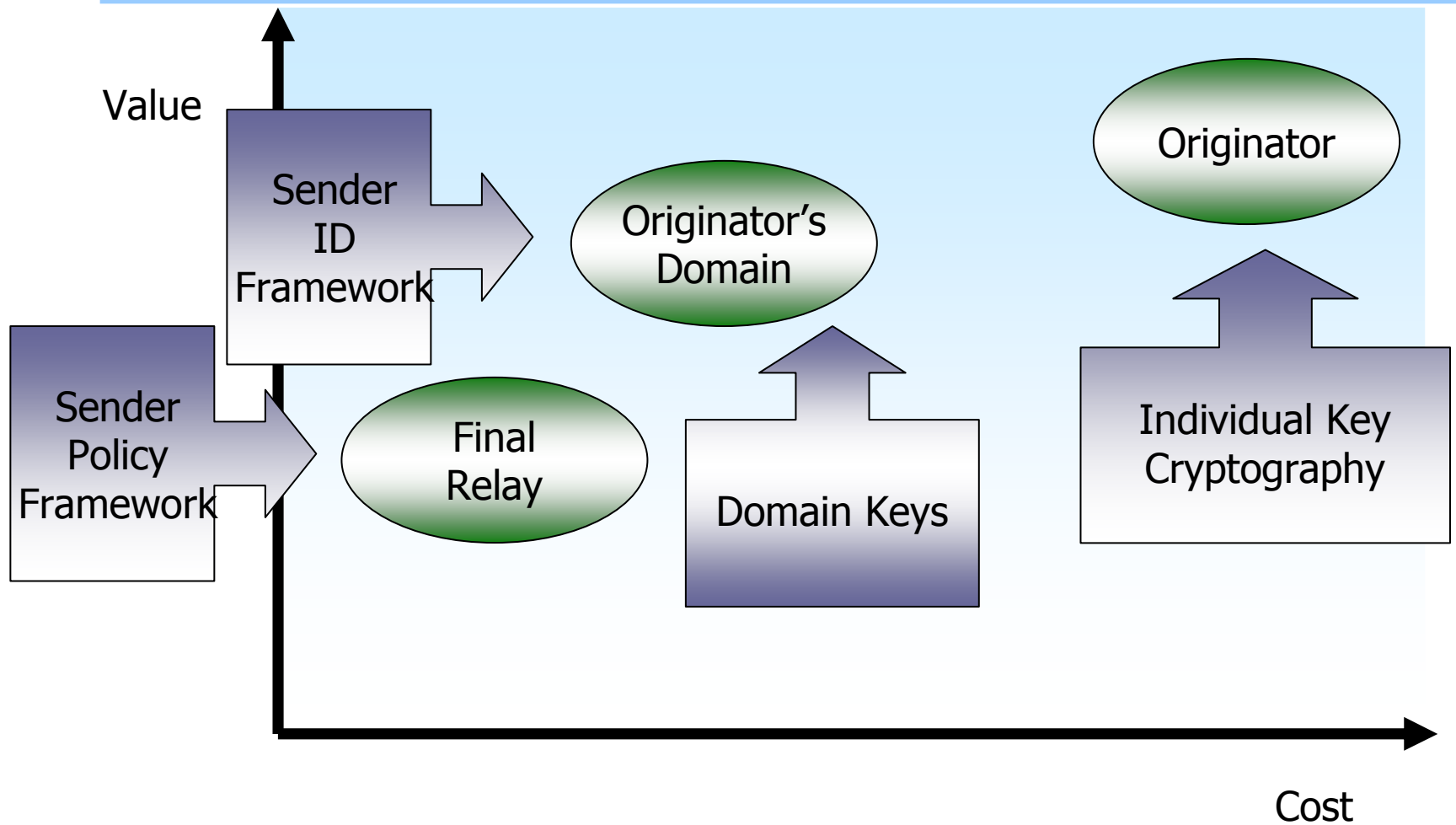
---

- ❑ The Internet Mail System has no reliable/usable form of authentication of
  - The sender
  - The domain from which the mail originated
  - Intermediate domains through which the mail passed
- ❑ All identities in e-mail messages are held in plain text header lines
  - Can be edited with any text editor
  - It is hard to detect forged headers

# Authentication Options

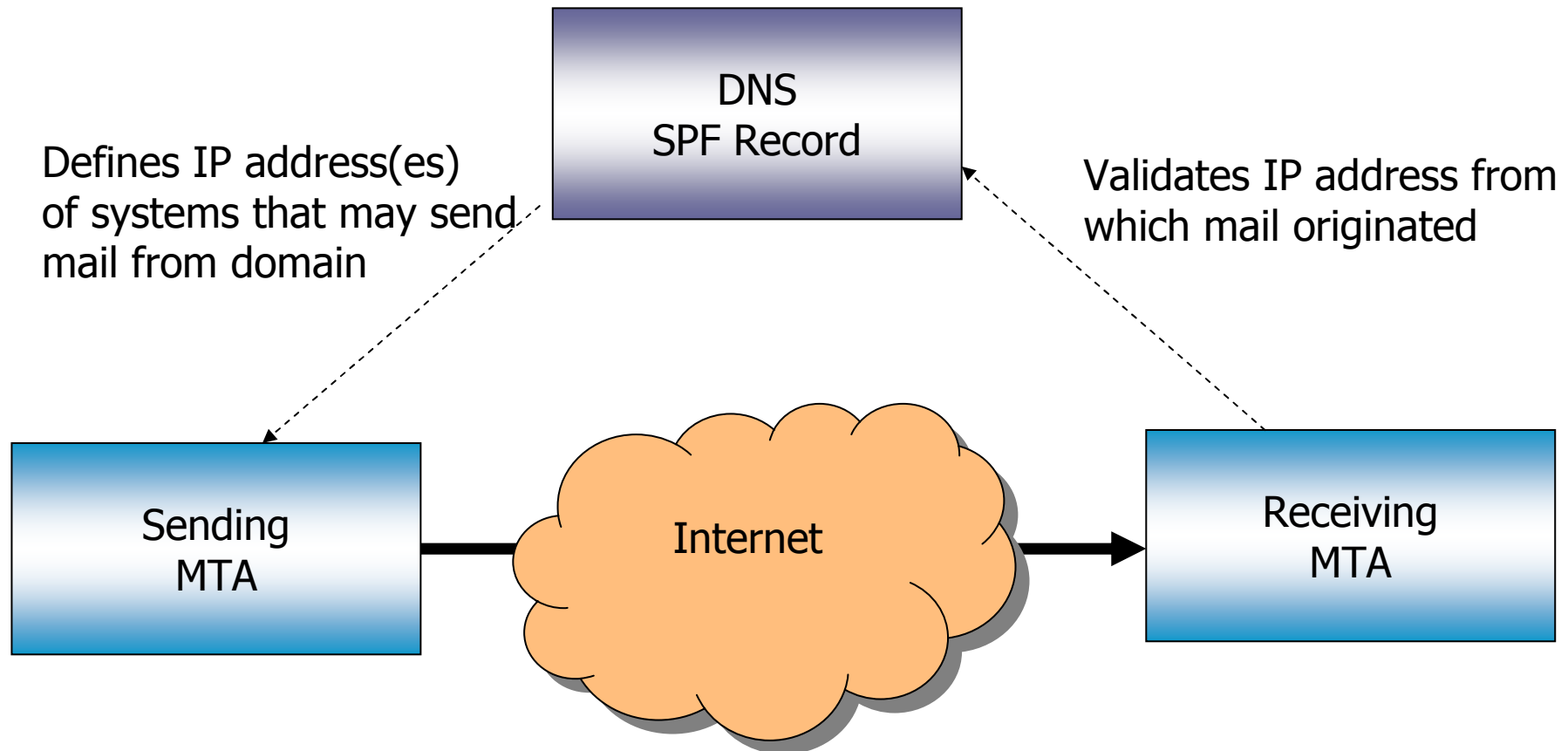


# Value/Cost Balance



# Sender Policy Framework

---

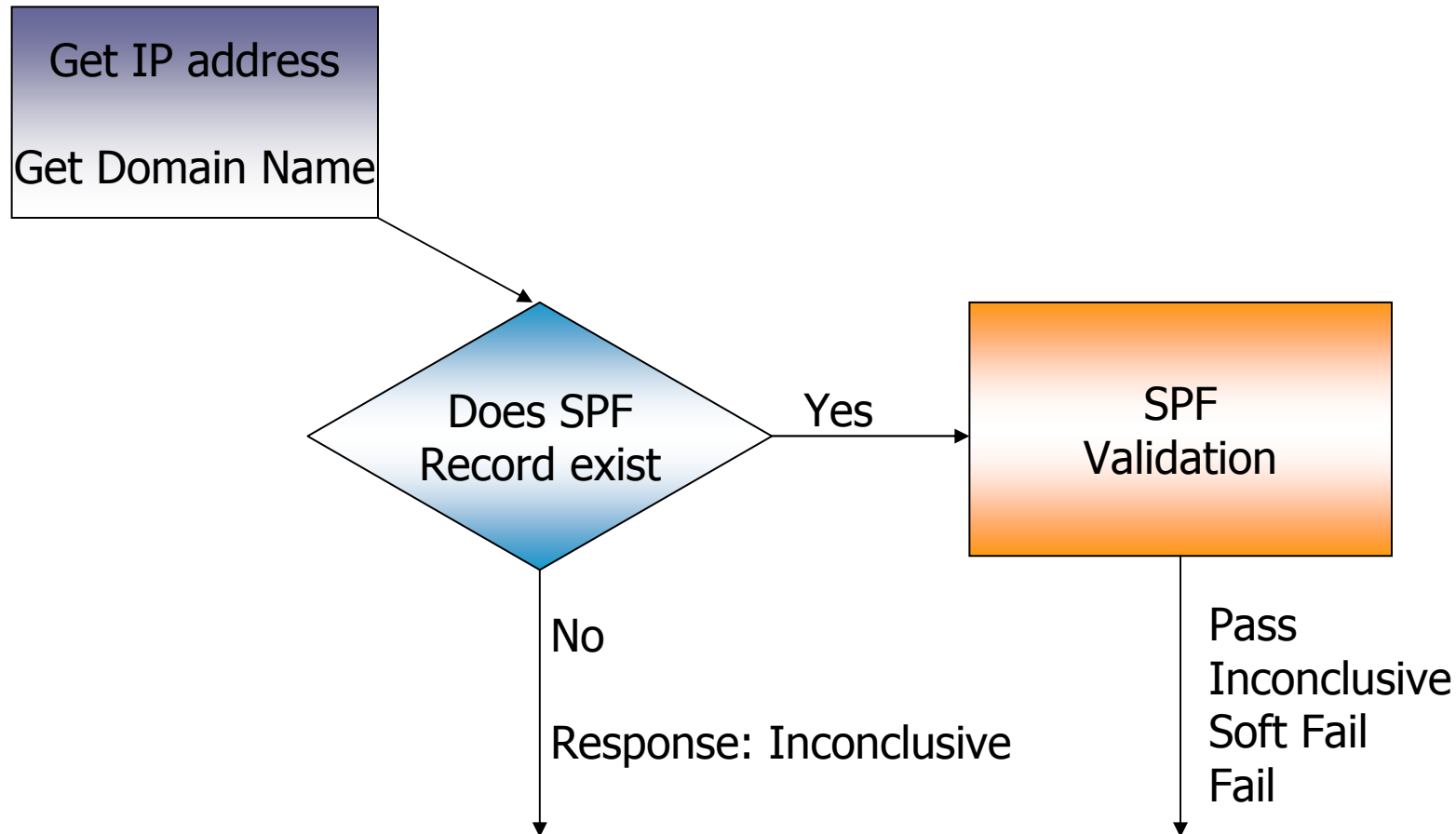


# SPF Record at DNS

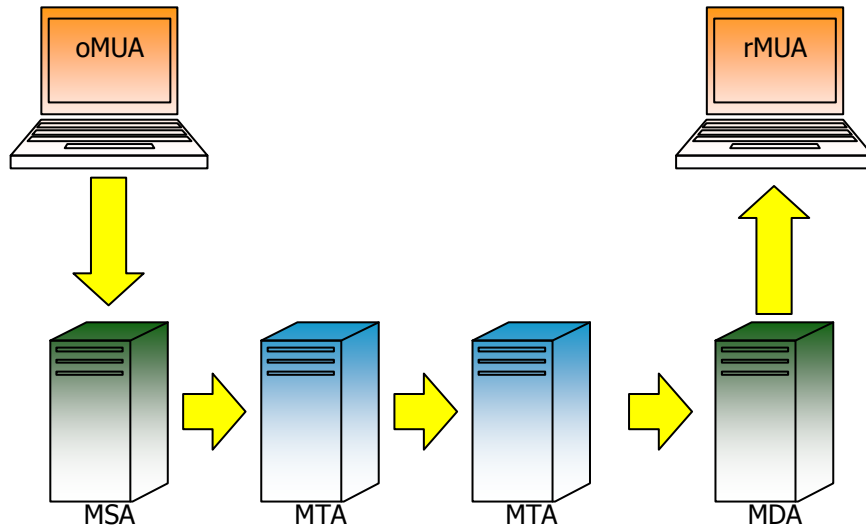
---

- ❑ Declare which hosts are, and are not, authorised to use a domain name to originate mail
- ❑ Linked to domain name to which it relates
- ❑ Simple text string format and/or special SPF record type

# SPF Validation (in MTA)



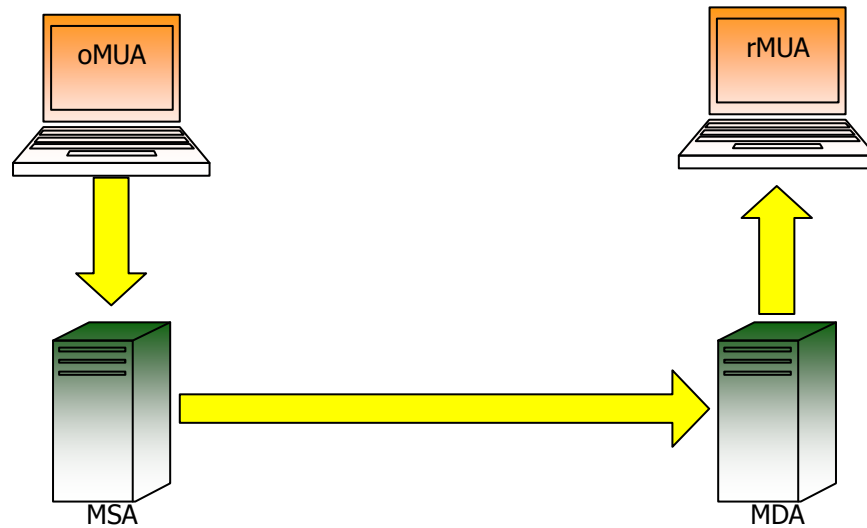
# Applicability of SPF



- ❑ Operates at the SMTP level
- ❑ Validates the previous sender
- ❑ Does not work in the generalised example shown
  - IP address of forwarding machine will not match the MAIL FROM line

# Applicability of SPF

---



- >80% of mail goes directly from MSA to MDA without intervening relays or mediators

# What have we achieved

---

- ❑ Validation of the originating domain of an e-mail
- ❑ Necessary in order to implement an e-mail policy, but not sufficient
  - Spammers can create SPF records
- ❑ E-Mail can be rejected on the basis of the address “on the envelope”
  - Very efficient
  - Legal

# Sender-ID Framework

---

- ❑ Microsoft development of SPF
- ❑ Uses the same mechanism to (SPF record) to define permitted senders of e-mail
- ❑ Uses a different mechanism to identify the sending domain
  - One option via SMTP envelope
  - One option via headers of e-mail message itself

# Sender-ID

---

- ❑ Adds new mail headers to allow mediators to pass on both the original sender details and information about the relay to enable SPF checking
  - Resent-Sender
  - Resent-From
- ❑ Adds a new SUBMITTER parameter to SMTP to support
- ❑ Needs changes to MTAs to handle this
- ❑ Algorithm allows for the way that the mail system works

# SMTP Changes

---

- New SUBMITTER parameter to define the system that is acting as relay or mediator
  - MAIL FROM: <mike@swimbluefins.org>  
SUBMITTER: <postman@reading.ac.uk>

# What does Sender-ID Add

---

- ❑ Better handling of relaying and mediation
  - At the expense of extra processing time
- ❑ Does need MTA software changes
- ❑ Backwards compatible, so does not break the internet mail system

# “Edge cases”

---

- There are lots of “edge cases” that need to be examined to determine whether SPF and/or Sender-ID still works
  - Message Forwarding
  - List Handling
  - Outsourced mailshots
  - Mail proxies (greeting card services)
  - .....

# SPF/Sender-ID Status

---

- Both SPF and Sender-ID are now being deployed
  - 2.5 million domains now have SPF records
    - 34% of Fortune-50
    - 22% of Fortune-100
  - Significant proportion of mail now from domains with SPF record
    - 25% to Hotmail/MSN
    - 37% to Earthlink
    - 33% to Ironport
- Hotlink statistics
  - 40% pass
  - 40% fail [Mostly soft fail]
  - 20% indeterminate
- SPF checking is implemented in a number of Commercial products
  - Open source MTA implementation available from SendMail
- Hotmail now checks SPF
  - Result visible to user via client
- Bank of America now checks SPF
- Major filter vendors now include results of SPF checking as weighting factor

# Recommendations

---

- ❑ Companies should create an SPF record defining the systems that they use to send email now. The cost is low, the risk is low, and there is an immediate reduction in the amount of bounced mail arising from mail sent from imposters.
- ❑ Companies should consider upgrading their Message Transfer Agents to check SPF records now that the major vendors have shipping software.
- ❑ Simple domain authentication based on IP address validation is now available
- ❑ Will authenticate between 80% and 90% of existing e-mail
- ❑ Low cost, low risk of disruption to the existing mail system.

# Digital Signatures

---

- ❑ Digital signatures have two fundamental objectives
  - To authenticate the originator of a message
  - To ensure that the contents of a message are not tampered with
  
- ❑ The signature is unique to the combination of the originator and the message being transmitted

# Authentication

---

- ❑ Digital Signatures use Asymmetric Key encryption to encrypt part or all of a message
- ❑ The originators PRIVATE key is used to encrypt
- ❑ When the originators PUBLIC key is used to decrypt the message it can only have been created with the associated PRIVATE key
- ❑ The challenge .. prove the relationship between the PUBLIC key and the originator
- ❑ Done by obtaining the PUBLIC key from someone who can be trusted
  - e.g. In a certificate issues by a trusted Certificate Authority

# Authentication using Digital Signatures

---

- ❑ Two prototype approaches developed
  - DomainKeys (Yahoo)
  - Internet Identified Mail (Cisco)
  
- ❑ They have now been integrated into a single approach (DKIM)
  - Submitted to IETF early July 2005

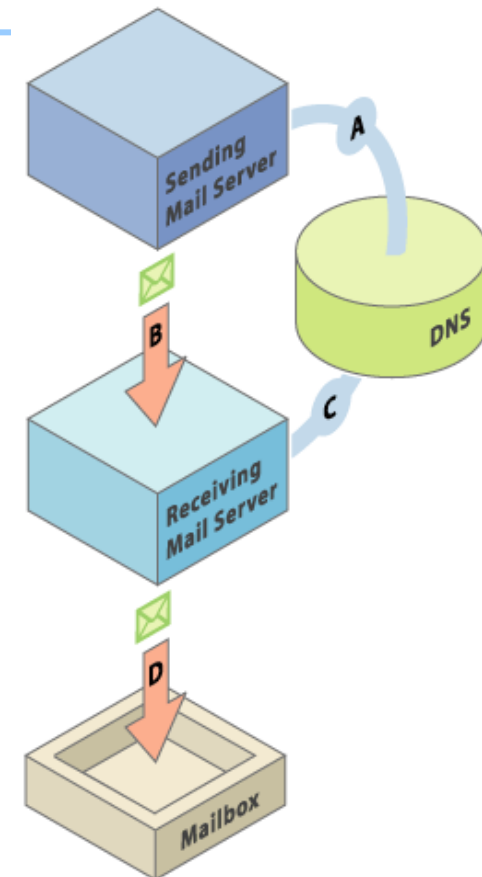
# DKIM Summary

---

- ❑ Domain owner generates PRIVATE/PUBLIC key pair
  
- ❑ Domain owner publishes public key in new DNS txt record
  - Revocation under control of domain owner
  - Multiple key pairs per domain
    - Can have separate key pair for outsourced E-Mail Service Provider, or for a specific contract

# DKIM – How it Works

- ❑ Outbound e-mail is signed by the originating domain using the PRIVATE key
  - Hash selected headers
  - Hash (part of) the body
  - Generate signature from resulting hash
  - Signature stored in the e-mail header
- ❑ Receiving system
  - Finds domain from From: header
  - Retrieves PUBLIC KEY from DNS
  - Verifies signature in e-mail



Graphic: Yahoo !

# Crypto Approaches and Sender-ID Framework

---

- Work together
  - Sender-ID effectively validates the path
  - DK/IIM effectively validates the content

# What problem does this solve

---

- ❑ Authentication of the originators domain
- ❑ Preserves signature through mediation and relays
- ❑ Does not ensure that e-mail is good

# Recommendations

---

- ❑ Domain Keys is deployed. DKIM is work in progress
- ❑ It is probably worth holding off on implementation of cryptography-based approaches until DKIM work is stable
  - Likely to happen in 1H 2006

# The Role of Reputation

---

- The identity of the originator is of little use without additional information about the originator
  - Are they known to you
  - Do they have a reputation of good behaviour
  - Are they known to be a source of Spam
  
- Reputation services are an unreliable tool, especially when the identity is purely an IP address
  - Filters use this information as a weighting factor, rather than an absolute yes/no indicator

# (Real-Time) Black List

---

- ❑ Sometimes called Block lists
- ❑ List of sites that are alleged to be source of Spam
- ❑ Spam filters may
  - Either download the list for local processing
  - Or make a real-time query relating to a single address
- ❑ Black lists are dangerous
  - There are many of them
  - Criteria for inclusion are not generally clear
  - Criteria for removal are generally time consuming
- ❑ Most companies find themselves on black lists from time to time

# White Lists

---

- ❑ Sometimes called “Allow Lists”
- ❑ List of sites that you can trust
  - Accreditation services
  - Reputation services
  - “Bonded sender”
- ❑ May be maintained by an enterprise as part of its e-mail policy
- ❑ May be a service from a third party
- ❑ Will become more important with more reliable authentication

# Accreditation Service

---

- ❑ E-Mail Sender signs up to a code of practise for mail handling
- ❑ Processes are audited by a third party, who publishes a list of accredited mail senders
- ❑ Sanctions available if the sender fails to abide by the code of practise
  - Bonded sender – Sender loses bond

# Reputation Service

---

- ❑ Third party monitors the behaviour of an e-mail sender
- ❑ Generates a rating based on the ratio of alleged Spam to total mail volume
- ❑ Rating is available for real-time retrieval by Filter vendors

# Greylisting

---

- ❑ A simple mechanism implemented at the receiving MTA
- ❑ When the first message is received from an unknown MTA, it is rejected
  - Well behaved MTAs will attempt to retransmit a failed message
  - At that point the receiving MTA adds the site to its grey list and accepts the mail
- ❑ This works because most Spam originators get so many message failure messages that they do not attempt to retransmit

# Recommendation

---

- ❑ Companies should start to worry about their email reputation now, making sure that policies are in place to prevent events that would generate a negative reputation, such as an ill-managed direct marketing campaign.

# Summary

---

- ❑ Spam is a big problem
  - Spam is cheap to originate and expensive to prevent
  
- ❑ Spam filters use a combination of approaches to
  - Examine the contents
  - Examine the source of mail
  
- ❑ Spam filtering is not reliable
  - There will always be a combination of false positives and false negatives
  
- ❑ The combination of Authentication and Reputation Services represents the major breakthrough

# Summary of Recommendations

---

- ❑ Companies should create an SPF record defining the systems that they use to send email now. The cost is low, the risk is low, and there is an immediate reduction in the amount of bounced mail arising from mail sent from imposters.
- ❑ Companies should consider upgrading their Message Transfer Agents to check SPF records "soon". The major vendors have software just about ready to ship.
- ❑ It is probably worth holding off on implementation of cryptography-based approaches until DKIM is stable.
- ❑ Companies should start to worry about their email reputation now, making sure that policies are in place to prevent events that would generate a negative reputation, such as an ill-managed direct marketing campaign.
- ❑ Deployment of DNS SEC is now an urgent requirement.

# Combating Spam – Latest Trends

THE *Open* GROUP

**Mike Lambert**

A Fellow of The Open Group  
Director, Messaging Forum

GSM +44 7770 451167

[m.lambert@opengroup.org](mailto:m.lambert@opengroup.org)

79, Camrose Way  
Basingstoke  
Hants, RG21 3AW  
United Kingdom

Tel +44 1256 414513  
Fax +44 20 7691 7868  
[www.opengroup.org](http://www.opengroup.org)

THE *Open* GROUP