The Sender ID Framework

An Approach to Email Authentication

Presentation to the Federal Trade Commission Email Authentication Summit

Washington, D.C.
November 9, 2004

Harry Katz
Program Manager
Safety Technology & Strategy Team
Microsoft Corp.

Microsoft

Agenda

- Microsoft's anti-spam strategy
- Why we need email authentication
- Sender ID Framework
- Implementation considerations
- Benefits

Why Authentication?

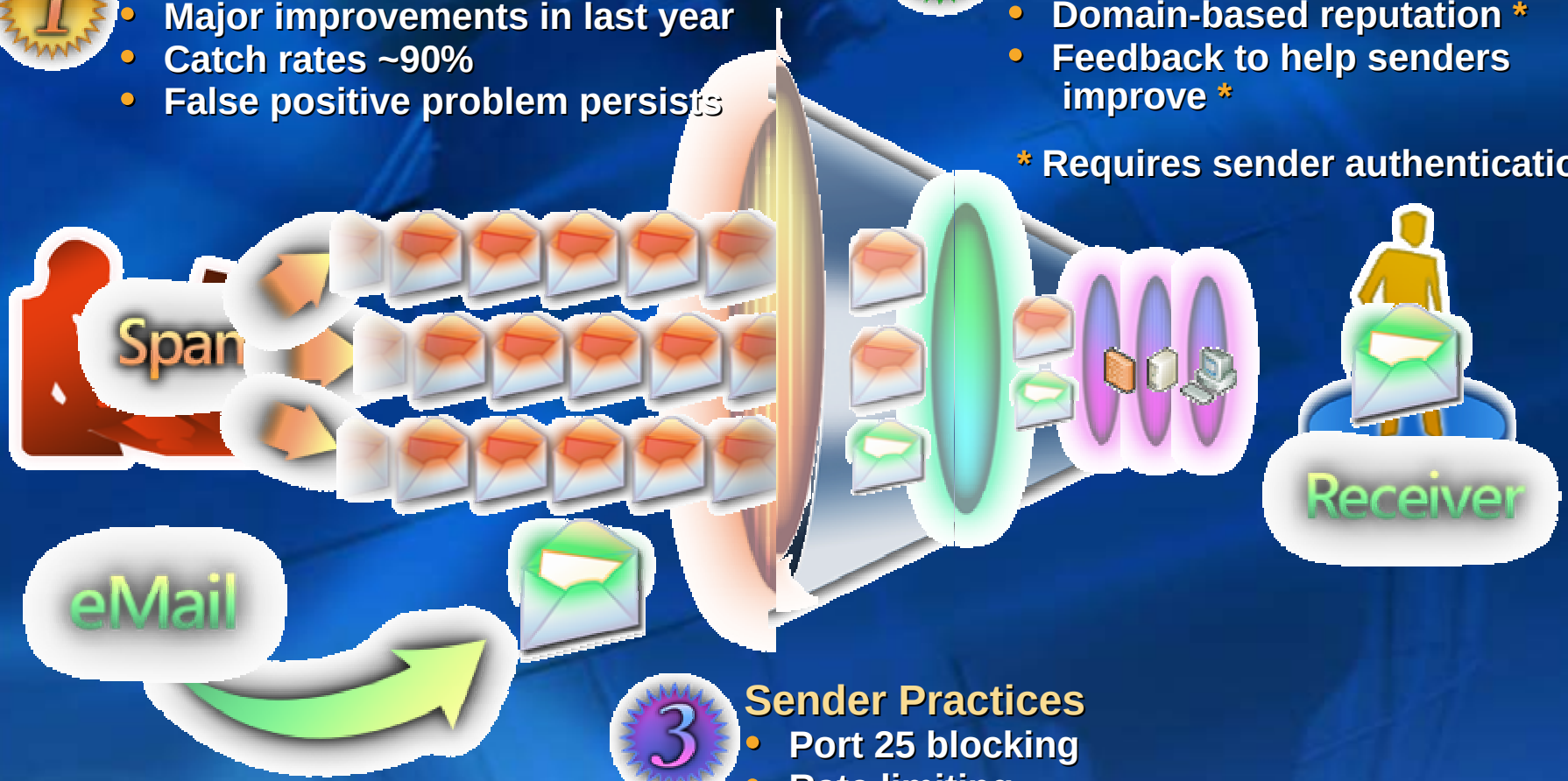
1 Content Filtering

- Major improvements in last year
- Catch rates ~90%
- False positive problem persists

2 Sender Reputation

- IP-based reputation
- Domain-based reputation *
- Feedback to help senders improve *

* Requires sender authentication



3 Sender Practices

- Port 25 blocking
- Rate limiting
- Publish SPF record
- Digital signatures
- Proof of work

Sender ID Framework
An Emerging Standard

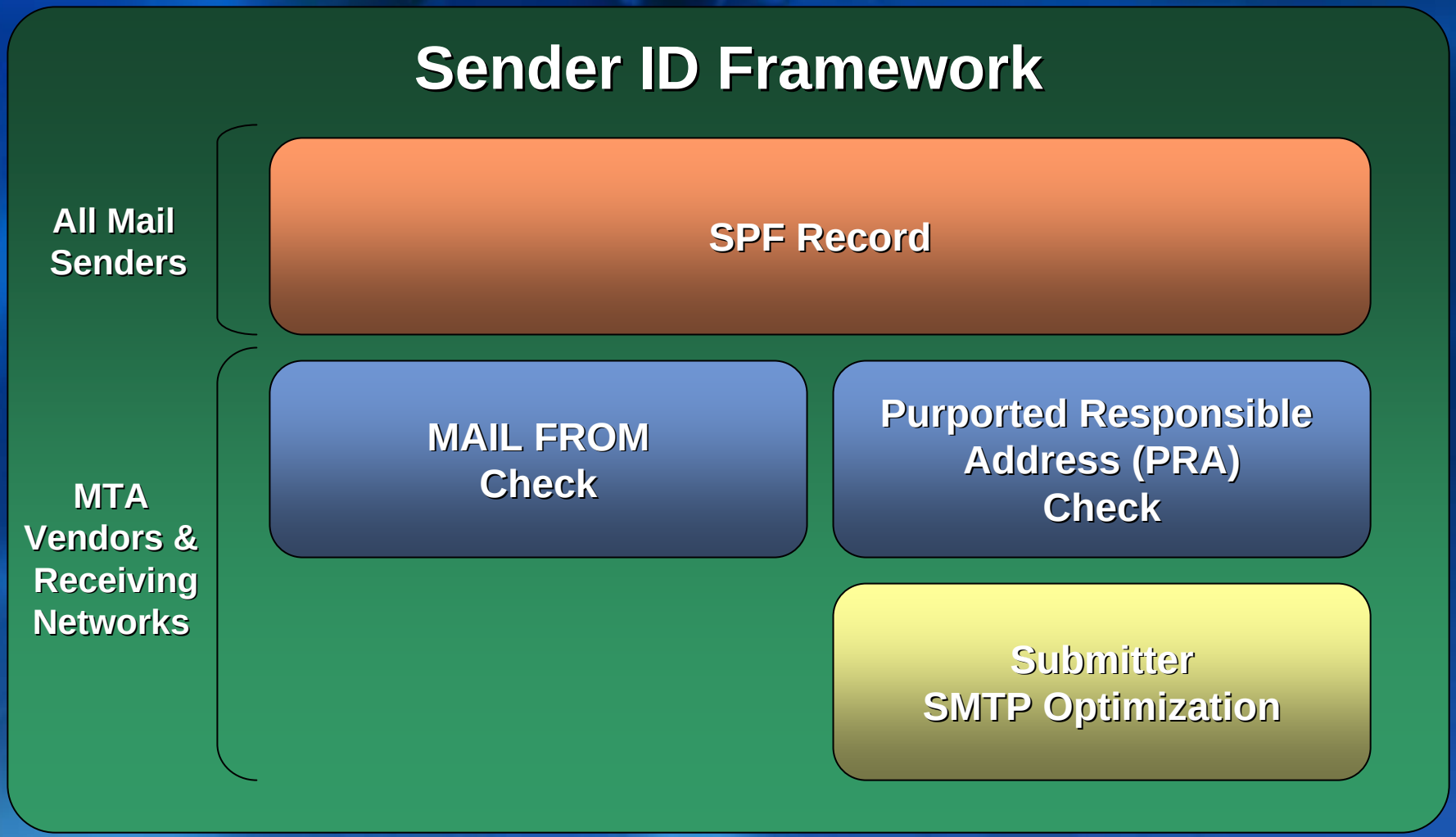
- A merger and refinement of proposals
  - SPF (Sender Policy Framework)
  - Microsoft Caller ID for Email
  - IETF MARID working group feedback
- Industry collaboration including
  - AOL, Bell Canada, Cisco, Comcast, IBM, Interland, Port25, Sendmail, Symantec, Tumbleweed, VeriSign….
  - Email Service Providers Coalition, Opengroup Messaging Forum, TRUSTe….
- A first step and on a fast track….

Design Goals & Tradeoffs

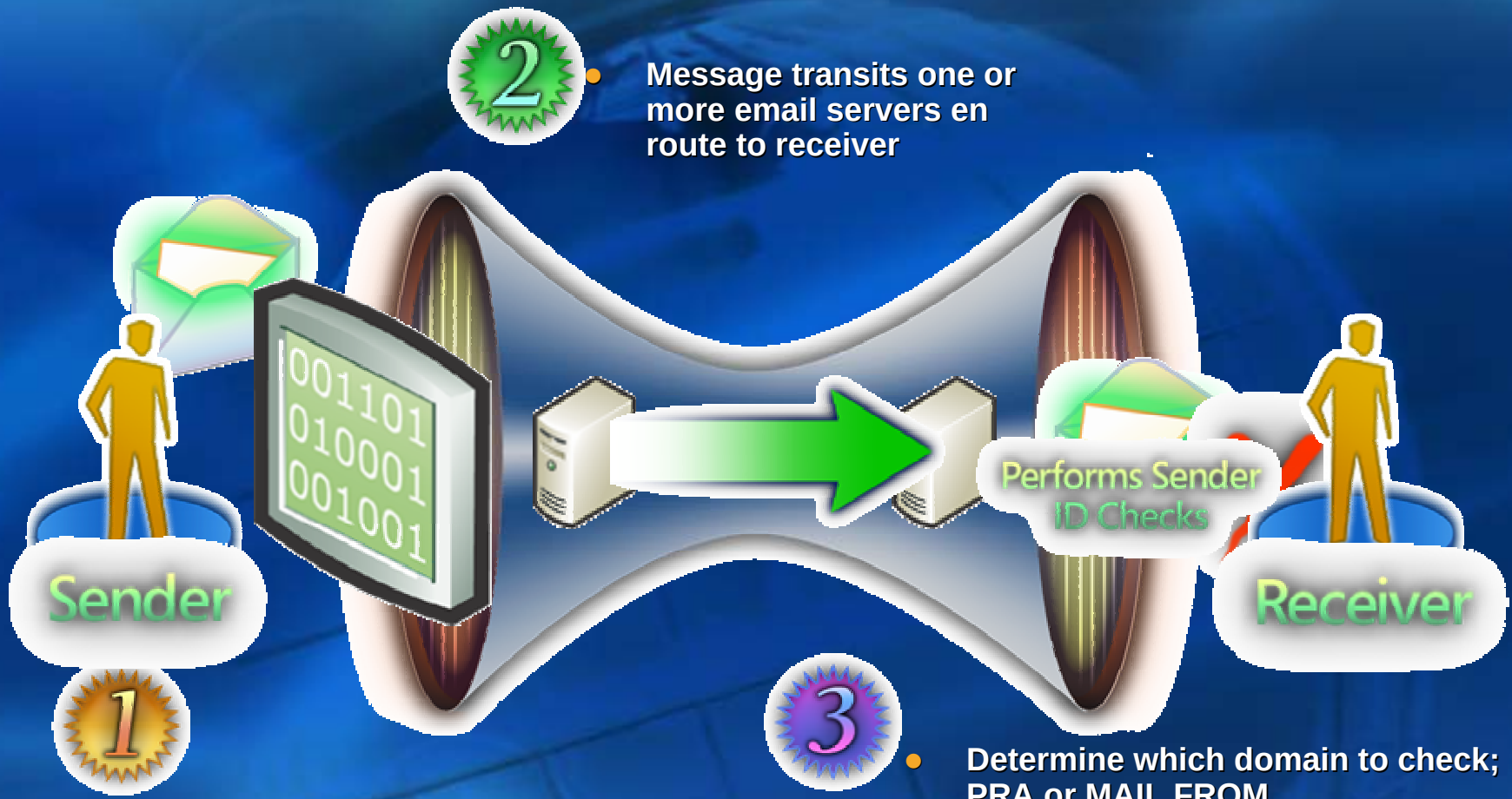
- Protection
  - Senders can take immediate steps to protect their brand & domain names
- Accountability
  - Senders can be held accountable for mail they send
- Ease of adoption
  - No software changes required for most senders
  - Openly published specification that can be broadly adopted
- Scalability
  - From small businesses to largest ISPs
- Non-Goals
  - Silver bullet for spam & phishing
  - Solve all email authentication problems
  - Zero cost

What Is Sender ID?

A framework of technical specifications



How Does Sender ID Work?



- One time: Publish SDIF record in DNS using SPF text format
- No other changes required
- Email sent as normal

- Determine which domain to check; PRA or MAIL FROM
- Look up sender's SPF record in DNS
- Compare connecting IP address to authorized list from SPF record
- Match → positive filter input
- No match → negative filter input

PRA and Mail From Checks

PRA	MAIL FROM
• Derived from RFC2822 message headers ➢ Resent-Sender, Resent-From, Sender, From • Identity most often seen by users	• RFC2821 “bounce” address
• Helps reduce phishing • Easier adoption for email forwarders	• Helps reduce “joe jobs” • Checking can begin before message data is received
• Headers can be spoofed • Headers must be received and parsed	• Headers seen by users are not validated • More difficult for forwarders

Interpreting the Results

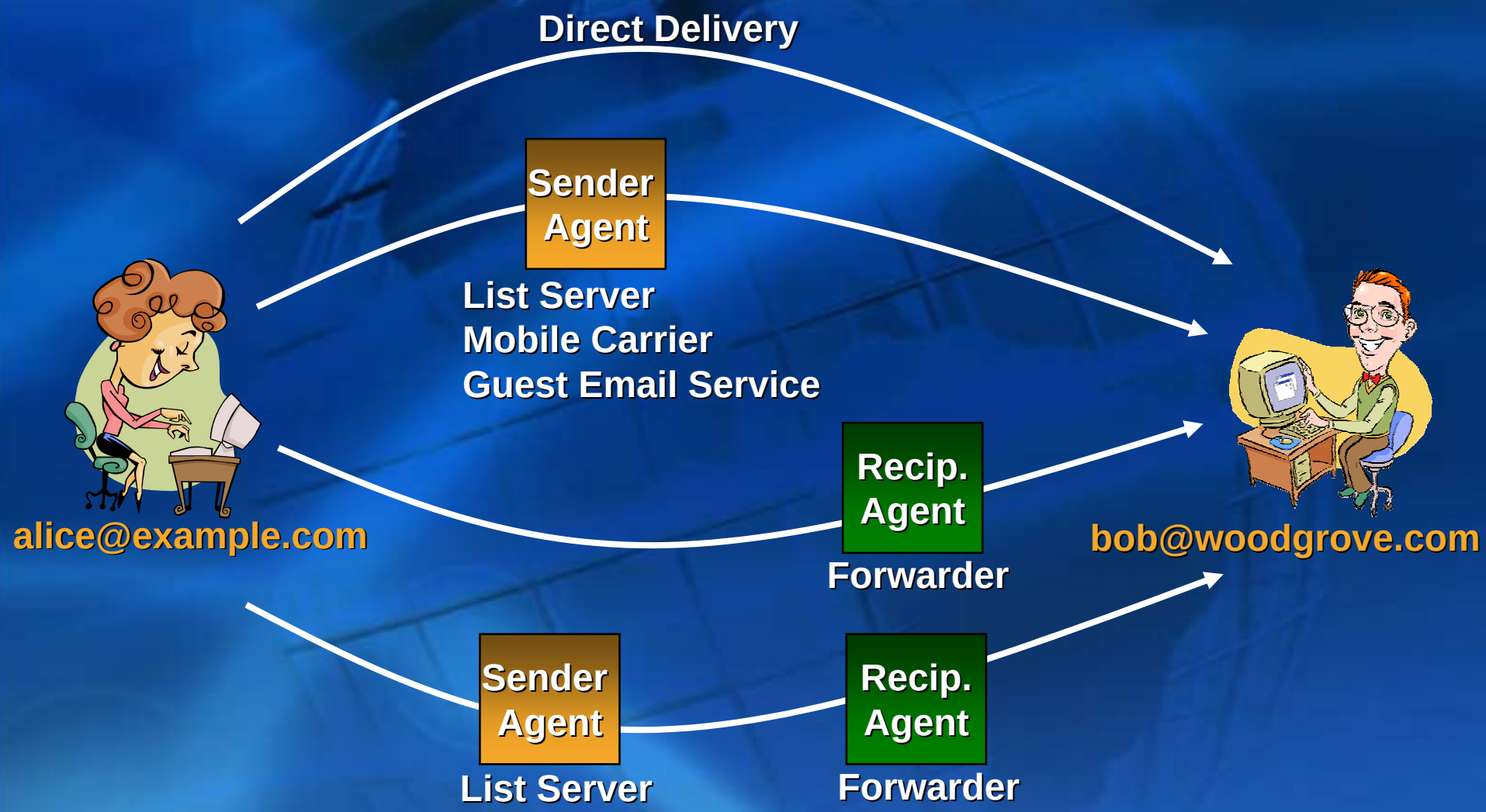
- Range of actions based on check results:
  - Accept message
  - Reject message
  - Use result as input into spam filters
  - Indicate result to end users
- "Pass" does not mean "good mail"
  - Sender could be a spammer with a domain
- Increasing adoption will enable stricter tests
  - Domains with no Sender ID records will have their mail subject to increased scrutiny
  - Increase weighting in filtering algorithms

Sample SPF Records

- example.com TXT “v=spf1 -all”
  - This domain never sends mail
- example.com TXT “v=spf1 mx -all”
  - Inbound email servers also send outbound mail
- example.com TXT “v=spf1 ip4:192.0.2.0/24 –all”
  - Specify an IP range
- example.com TXT “v=spf1 mx include:myesp.com –all”
  - Outsourced email service
- example.com TXT “spf2.0/pra ip4:192.0.3.0/24 –all”
  - Different configuration for PRA checking

Mail Delivery Scenarios

What Must Senders Do?



Direct Delivery

alice@example.com

bob@woodgrove.com

- Publish outbound server records in DNS using the SPF format
- Optional: Transmit SUBMITTER parameter on MAIL command

Direct Delivery

S: 220 woodgrove.com ESMTP server ready
C: EHLO example.com
S: 250-woodgrove.com
S: 250-DSN
S: 250-AUTH
S: 250-SUBMITTER
S: 250 SIZE
C: MAIL FROM:<alice@example.com>
S: 250 <alice@example.com> sender ok
C: RCPT TO:<bob@woodgrove.com>
S: 250 <bob@woodgrove.com> recipient ok
C: DATA
S: 354 okay, send message
C: From: alice@example.com
C: (message body goes here)
C: .
S: 250 message accepted
C: QUIT
S: 221 goodbye

SUBMITTER extension advertised in EHLO response

RFC2821 MAIL FROM = RFC2822 From

Mailing List

alice@example.com

List Server

owner-list1@listexample.com

bob@woodgrove.com

1. Publish outbound server records in DNS
2. Ensure “list-owner” style address is present in the message
   - E.g. Sender: owner-list1@listexample.com
   - Vast majority of mailing list servers do this today
3. Optional: Transmit SUBMITTER parameter on MAIL command

Mailing List

S: 220 woodgrove.com ESMTP server ready
C: EHLO listexample.com
S: 250-woodgrove.com
S: 250-SUBMITTER
S: 250 SIZE
C: MAIL FROM:<owner-list1@listexample.com>
SUBMITTER=owner-list1@listexample.com
S: 250 <owner-list1@listexample.com> sender ok
C: RCPT TO:<bob@woodgrove.com>
S: 250 <bob@woodgrove.com> recipient ok
C: DATA
S: 354 okay, send message
C: Received By: ...
C: From: alice@example.com
C: Sender: owner-list1@listexample.com
C: To: list1@listexample.com
C: (message body goes here)
C: .
S: 250 message accepted
C: QUIT
S: 221 goodbye

SUBMITTER extension advertised in EHLO response

SUBMITTER parameter added to MAIL command

Sender header added to message

Mail Forwarder

alice@example.com

Mail Forwarder

bob@alumni.almamater.edu

bob@woodgrove.com

1. Publish outbound server records in DNS
2. Ensure forwarding address is present in the message
   - E.g. Resent-From: bob@alumni.almamater.edu
3. Optional: Transmit SUBMITTER parameter on MAIL command indicating forwarding address

Mail Forwarder

S: 220 woodgrove.com ESMTP server ready
C: EHLO alumni.almamater.edu
S: 250-woodgrove.com
S: 250-DSN
S: 250-AUTH
S: 250-SUBMITTER
S: 250 SIZE
C: MAIL FROM:<alice@example.com>
SUBMITTER=bob@alumni.almamater.edu
S: 250 <alice@example.com> sender ok
C: RCPT TO:<bob@woodgrove.com>
S: 250 <bob@woodgrove.com> recipient ok
C: DATA
S: 354 okay, send message
C: Resent-From: bob@alumni.almamater.edu
C: Received By: ...
C: (message body goes here)
C: .
S: 250 message accepted
C: QUIT
S: 221 goodbye

SUBMITTER extension advertised in EHLO response

SUBMITTER parameter added to MAIL command

Resent-From header added to message

Implementation Considerations

- Senders
  - Administrative (immediate): Publish DNS records identifying authorized outbound email servers
    - On-going maintenance of same
    - Coordination of e-mail marketing initiatives
    - No hard costs or technical overhead
- Receivers
  - Software (near term): Upgrade inbound email gateway servers to perform Sender ID checks
  - Software (optional - medium-long term): Upgrade client software to display results of Sender ID check
- Mail forwarders and other “intermediaries”
  - Software (near term): Upgrade outbound email servers to identify their own domains in messages

Sender ID vs. Cryptographic Email Authentication

Sender ID	Crypto Approaches
• Validates "last hop"	• Validates end-to-end ➢ If signature survives
• Validates domain	• Validates domain & potentially user
• Asymmetric deployment ➢ Most senders don't need software upgrades	• Symmetric deployment ➢ Requires software changes by both sender and receiver
• Input to reputation systems ➢ Senders can register own domains	• Input to reputation systems ➢ Spammers can sign messages
• Forged header attacks	• Replay attacks

Benefits of Sender ID

- Protect senders' brand and domain names from spoofing and phishing
- Rapid adoption
  - Senders can publish SPF records today
  - Most senders require no software upgrades
- A foundation for the reliable use of domain names in accreditation, reputation systems & safe lists
  - Receivers validate the origin of mail
- Input into more aggressive spam filtering with reduced false positives
- The first step industry will need to take together – there will be more to come including signing solutions

Summary

- All e-mail senders and domains should publish their SPF records today
- MSFT will initiate checking by year-end
- Network administrators should contact their ISP / MTA Vendors for Sender ID Framework integration
- Resources
  - www.microsoft.com/senderid
    - Specs, resources, record wizard
  - www.microsoft.com/spam