Future Approaches to Stop Spam: Certification Services for Everyone

The Internet Days, Stockholm, Sweden
October 24, 2006

Eric Thomas
Inventor of LISTSERV®
L-Soft Founder and CEO

Agenda

- Overview of current ”remedies”
- Our big hope – DomainKeys, SPF, Sender ID and pay-to-send schemes
- But why short-term solutions are doomed to fail?
- Spam free email – utopia?
- A workable solution in the long term

Bad methods

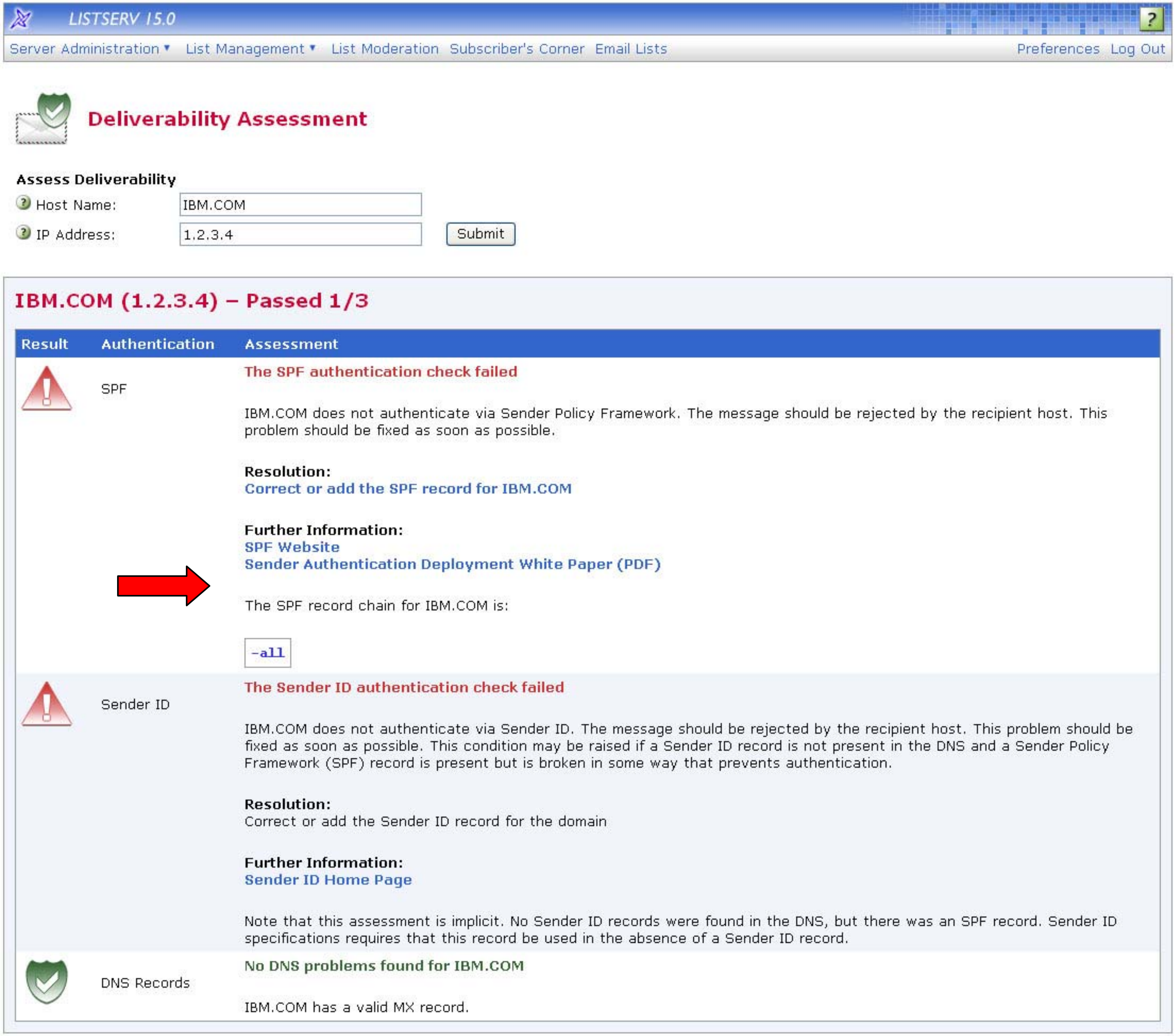
- Content filtering (e.g. Outlook’s)
- Black lists
- Closing of port 25 for all homes
- All regular spam filters
- Etc …

Even worse methods

- Volume filters
- ”If you want me to receive your message, please fill out this form”
- Honey pots
- …

Our big hope – DK, SPF, SID

- SPF/SID became a political mess
  - ✓ Considered dead as AOL has abandoned SPF
  - ✓ No one runs SPF live – no effect
- DomainKeys
  - ✓ Used diligently – by spammers!
  - ✓ Does not solve anything even if everybody would use them



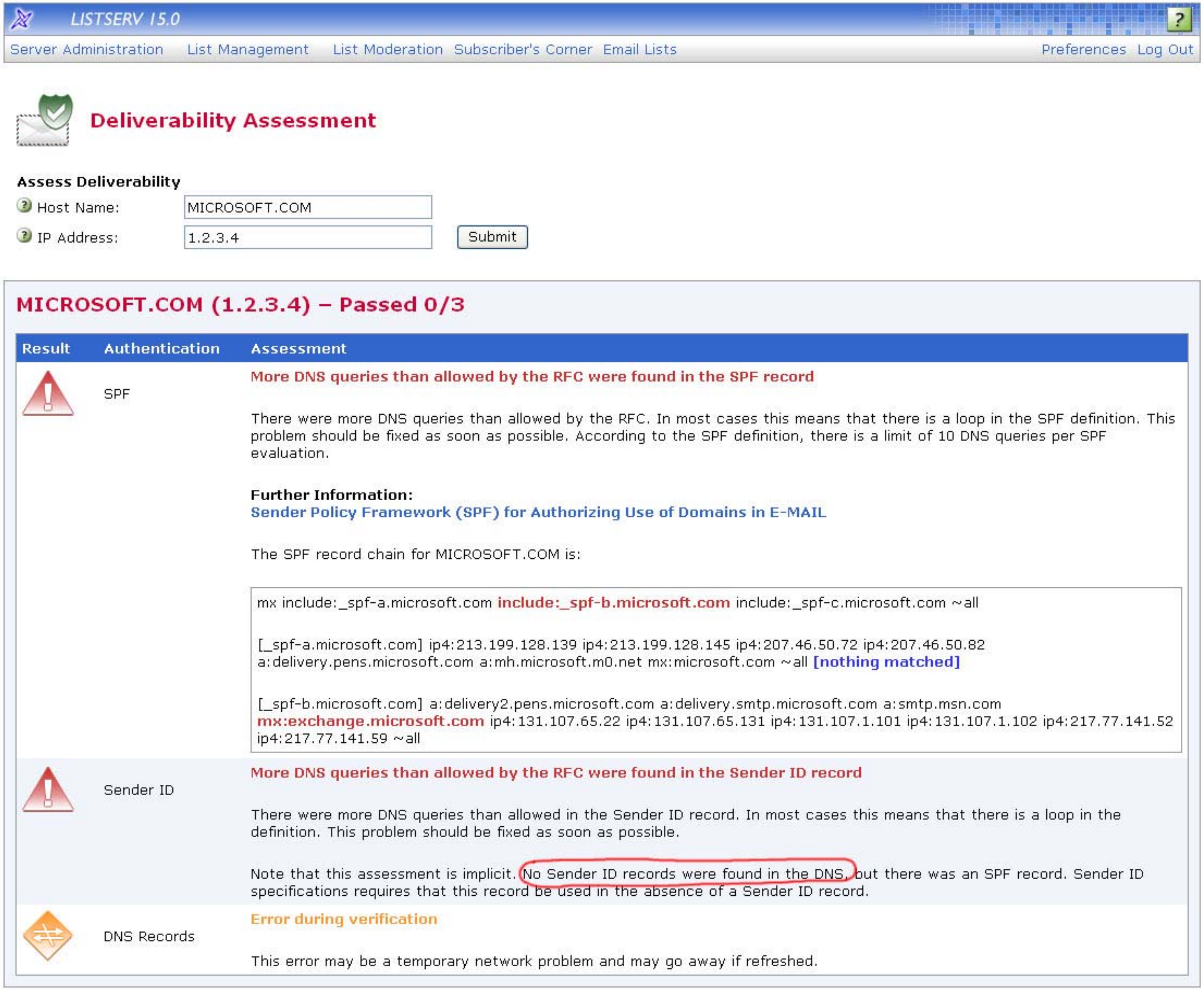
Deliverability Assessment

Assess Deliverability

Host Name:	IBM.COM
IP Address:	1.2.3.4

IBM.COM (1.2.3.4) – Passed 1/3

Result	Authentication	Assessment
⚠	SPF	**The SPF authentication check failed** IBM.COM does not authenticate via Sender Policy Framework. The message should be rejected by the recipient host. This problem should be fixed as soon as possible. **Resolution:** Correct or add the SPF record for IBM.COM **Further Information:** SPF Website Sender Authentication Deployment White Paper (PDF) The SPF record chain for IBM.COM is: `-all`
⚠	Sender ID	**The Sender ID authentication check failed** IBM.COM does not authenticate via Sender ID. The message should be rejected by the recipient host. This problem should be fixed as soon as possible. This condition may be raised if a Sender ID record is not present in the DNS and a Sender Policy Framework (SPF) record is present but is broken in some way that prevents authentication. **Resolution:** Correct or add the Sender ID record for the domain **Further Information:** Sender ID Home Page Note that this assessment is implicit. No Sender ID records were found in the DNS, but there was an SPF record. Sender ID specifications requires that this record be used in the absence of a Sender ID record.
✓	DNS Records	**No DNS problems found for IBM.COM** IBM.COM has a valid MX record.



Deliverability Assessment

Assess Deliverability

Host Name:	MICROSOFT.COM
IP Address:	1.2.3.4

MICROSOFT.COM (1.2.3.4) – Passed 0/3

Result	Authentication	Assessment
⚠	SPF	**More DNS queries than allowed by the RFC were found in the SPF record** There were more DNS queries than allowed by the RFC. In most cases this means that there is a loop in the SPF definition. This problem should be fixed as soon as possible. According to the SPF definition, there is a limit of 10 DNS queries per SPF evaluation. **Further Information:** Sender Policy Framework (SPF) for Authorizing Use of Domains in E-MAIL The SPF record chain for MICROSOFT.COM is: mx include:_spf-a.microsoft.com **include:_spf-b.microsoft.com** include:_spf-c.microsoft.com ~all [_spf-a.microsoft.com] ip4:213.199.128.139 ip4:213.199.128.145 ip4:207.46.50.72 ip4:207.46.50.82 a:delivery.pens.microsoft.com a:mh.microsoft.m0.net mx:microsoft.com ~all **[nothing matched]** [_spf-b.microsoft.com] a:delivery2.pens.microsoft.com a:delivery.smtp.microsoft.com a:smtp.msn.com **mx:exchange.microsoft.com** ip4:131.107.65.22 ip4:131.107.65.131 ip4:131.107.1.101 ip4:131.107.1.102 ip4:217.77.141.52 ip4:217.77.141.59 ~all
⚠	Sender ID	**More DNS queries than allowed by the RFC were found in the Sender ID record** There were more DNS queries than allowed in the Sender ID record. In most cases this means that there is a loop in the definition. This problem should be fixed as soon as possible. Note that this assessment is implicit. No Sender ID records were found in the DNS, but there was an SPF record. Sender ID specifications requires that this record be used in the absence of a Sender ID record.
◆	DNS Records	**Error during verification** This error may be a temporary network problem and may go away if refreshed.

Reemerged idea: charge for email

- Very strong support for this ”solution”; media convinced the public that spam would disappear once and for all
- Much money to make!
- Strong commercial interests, e.g. AOL/Goodmail
- Tax on email has been mentioned too …

Goodmail

- Corporation in California with a strong connection to AOL (ownership)
- Media storm in the U.S.
- Senate hearing in April 2006 in the U.S.
- AOL had to back down
- Completely unknown in many non-English speaking countries

The spammers have money

- The spammers have enough money to afford to pay for better email deliverability
- If the price for sending email gets too high to get rid of spammers, then we also get rid of small companies, clubs and associations

To pay for email = more spam

- The spammers can afford to pay with the money of others (hacked computers)
- Such a system makes the life easier for the spammers!

Status

- Spammers gain ground
- DomainKeys, SPF/SID and email charges won’t help
- The battle against spammers is lost because:
  - ✓ We demand results at once…
  - ✓ … even if we know that spammers move quicker than we do

Solution: open certification

- Certification is available today (Goodmail, Return Path, Habeas, among others) and it works but costs too much
- No open certification system available today
- Imagine if everyone could afford to certify themselves!

The inbox of the future

- The main, primary, inbox:
  - ✓ 99.x % spam free
  - ✓ No spam filtering = no lost messages, no false positives
- The side, secondary, inbox:
  - ✓ A few important messages
  - ✓ More aggressive filtering than today
  - ✓ You read when you have the time

The business model

Two models which can be combined:

- Companies such as D&B or main business and credit information agencies can sell information about a company’s “spam factor”
- Companies such as Return Path, among others, and community sites can review and certify those who wish certification

Technology available today can be developed further

- DomainKeys: ”I’m who I claim to be and here is the proof”
- Certification: ”And, in addition, I have been reviewed by nospam.org and here is the proof”
- The certification key can be taken away within minutes if the sender would start to spam

Resources

DomainKeys:
http://antispam.yahoo.com/domainkeys

Sender ID:
http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx

Sender Policy Framework:
http://www.openspf.org

Spam Laws:
http://www.spamlaws.com

About Spam:
http://www.lsoft.com/resources/spamorama.asp