

CS 4235 - Internet Security Group I Project

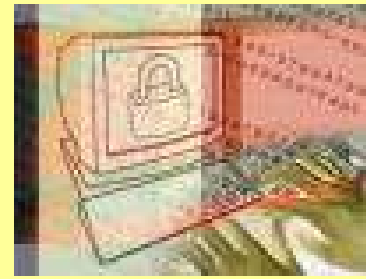
Comparison and Evaluation of E-Mail Sender Authentication Technologies

Leo
Singleton



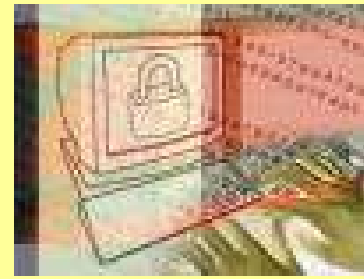
Wednesday, November 10, 2004.

Presentation Topics



- Overview
- Three Technologies
 - Sender Policy Framework
 - DomainKeys
 - Sender ID
- Industry Adoption of Technologies
- Empirical Statistics
- Evaluation: Real-World Application
- Threats / Vulnerabilities Associated with Technologies
- Examination: Comparison of Technologies
- Conclusions

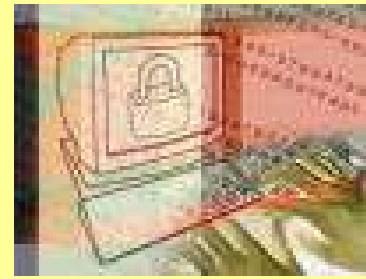
Overview



Why is E-mail Sender Authentication so important ?

- Spammers forge the sender domain to deceive internet e-mail users.
- E-mail sent using such malicious methods, provoke users in relinquishing their private information.
- An estimated loss of US \$20.5 billion was reported in 2003 due to spoofed e-mails.
- Sender authentication can substantially reduce these losses.

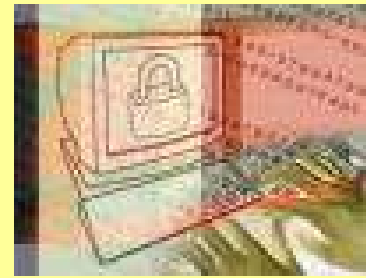
Sender Policy Framework



Background of SPF:

- DNS based open standard E-mail sender authentication scheme.
- Proposed by Meng Weng Wong of pobox.com.
- Improves on “Reverse Mail Exchange” and “Designated Mailer Protocol” concepts.

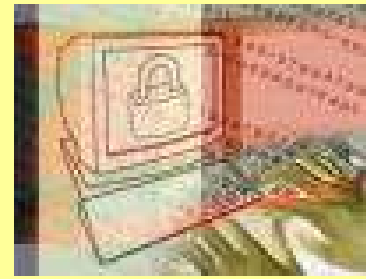
SPF (*contd.*)



Steps in the Process:

- Policy Framework:
 - Domains responsible for outbound E-mail traffic publish SPF records in their DNS.
- Authentication Scheme:
 - The receiver E-mail server verify the incoming messages with those published in the DNS.

SPF (*contd.*)



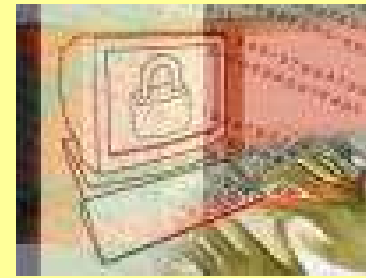
SPF Records:

- Defines attributes of legitimate E-mail messages sent by publishing domains.
- Uses textual symbols as defined by SPF technology.

Sample SPF Record:

```
v=spf1 +mx +a:mail.gatech.edu +ip4:130.207.0.0/16 -all
```

SPF (*contd.*)

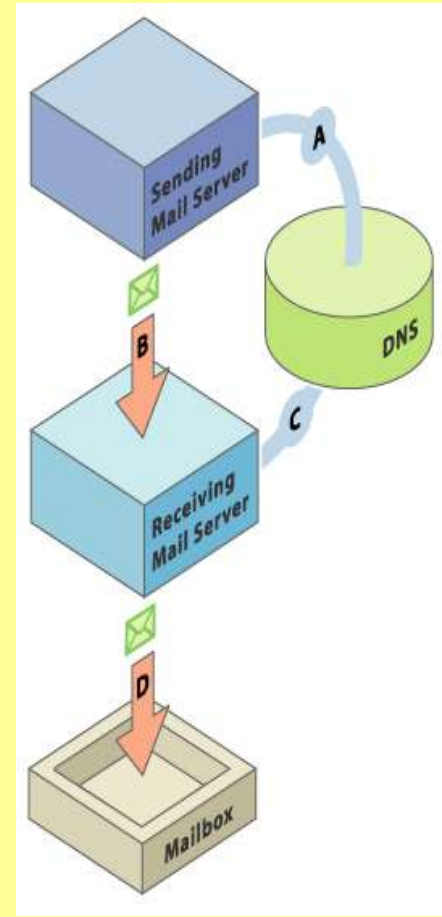


Sender Authentication:

- SPF Records are published in DNS as a TXT record.
- These TXT records can be cached by DNS resolvers to reduce computational overhead.
- E-mail receiver server verifies the attributes of the incoming messages to determine its authenticity.

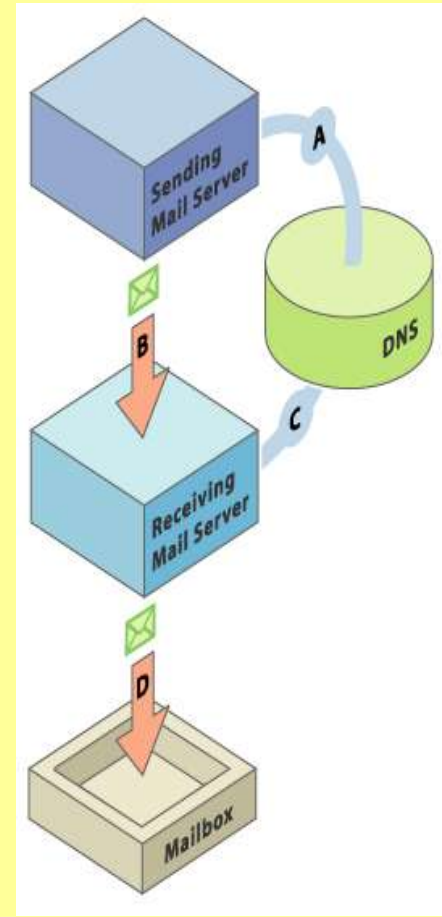
DomainKeys

- Four Steps in the process:
 - Public / Private encryption keys created. Public key published in DNS
 - Outgoing mail signed using a private key
 - Receiving mail servers check incoming mail's signature
 - Authenticated mail delivered to end-user

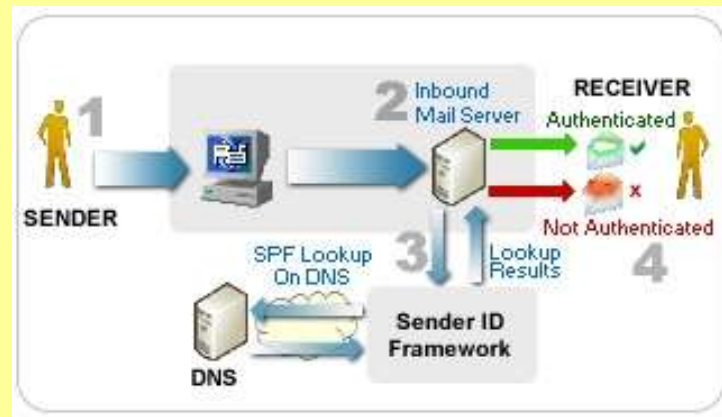


DomainKeys (*contd.*)

- Most robust of all technologies in what it enables
- Most taxing on hardware
- Least “adopted” so far, which may change as processing costs become cheaper
- Yahoo! developed but claims no license to and is open-source for all to use and improve
- The RSA encryption algorithm used by DomainKeys may need to be licensed



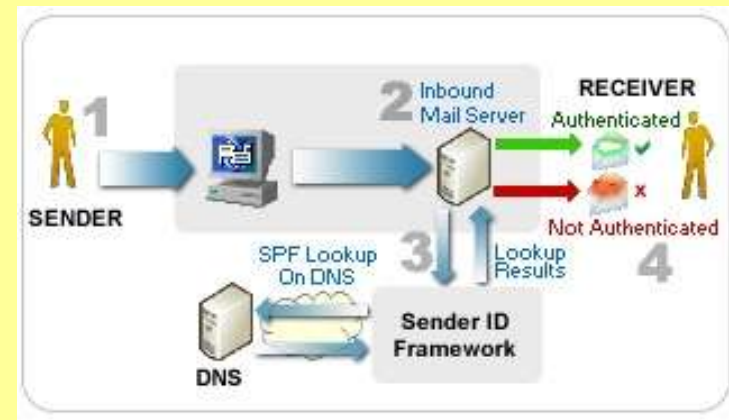
Sender ID



- **Four Steps in the process:**

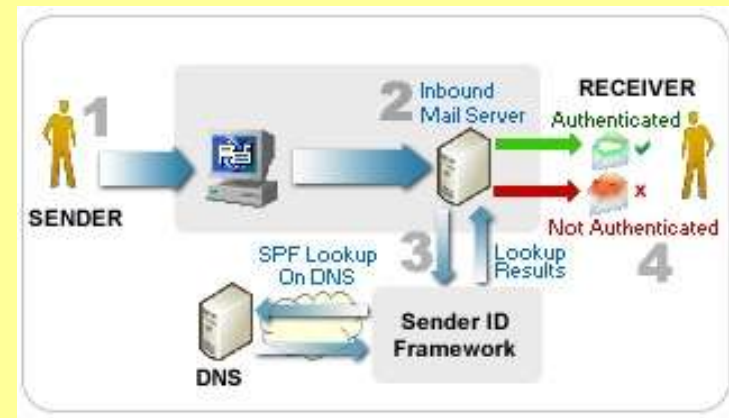
1. Sender sends an e-mail message to Receiver.
3. Receiver's inbound mail server receives mail.
5. Receiver's server checks for the SPF record of the sending domain published in the Domain Name System (DNS) record.
7. Inbound e-mail server determines if the sending e-mail server's IP address matches the IP address published in the DNS record.

Sender ID (*contd.*)



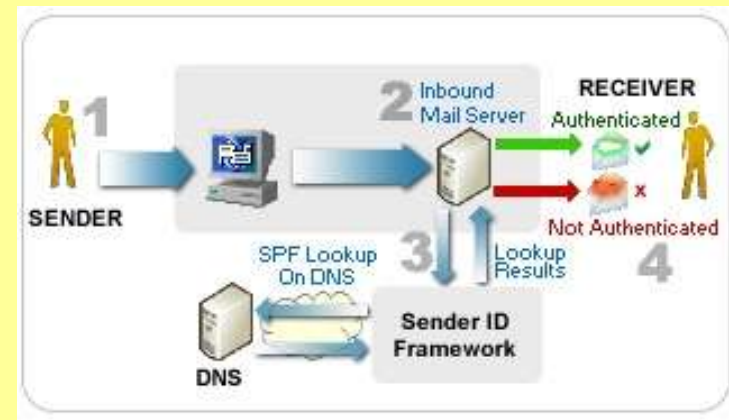
- Two methods will be used to identify senders:
 - PRD: Purported Responsible Domain
 - SPF: Sender Policy Framework
- Implementation of two methods provides full functionality.
- Result: causes senders to create two sets of references in DNS to accommodate both types of receiving e-mail servers.

Sender ID (contd.)



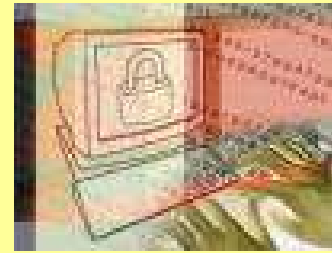
- Sender ID under intense review by IETF since Sept. 2004
 - Undergoing licensing process
 - Difficulty: elements of Sender ID conflict with user preferences
- Microsoft revamping Sender ID to resubmit to IETF
 - IETF: hints that new version will still “fall short” in appealing to all users
- Intellectual Property Rights Conflict
 - Scott Deaver, of Failsafe Designs, claims to have invented e-mail authentication technology
 - Possible lawsuit against Microsoft could result

Sender ID (*contd.*)

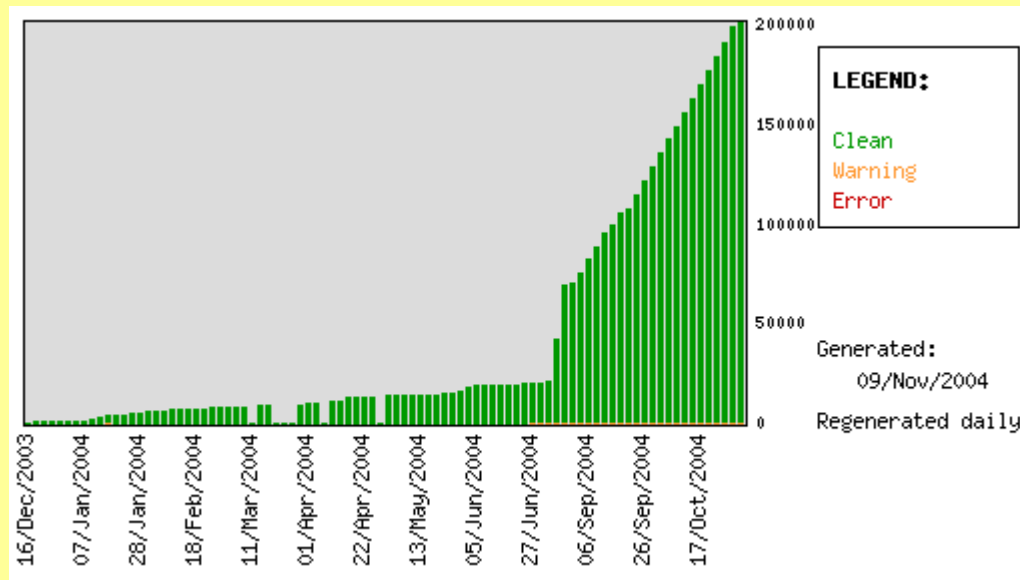


- AOL has been back and forth in its decision to support Microsoft's Sender ID:
 - September 2004: AOL rejected Sender ID
 - October 2004: AOL accepted Sender ID
- AOL realized importance of working with Microsoft to encourage sender authentication over its own e-mail servers for better business practices
- AOL has now confidently joined Microsoft to promote Sender ID technology.

Industry Adoption – SPF

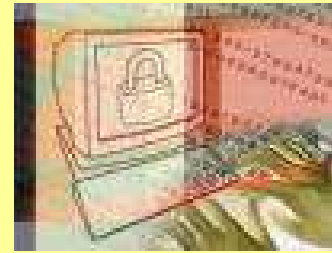


- Dramatic increase during the period July-September 2004
- As of November 9, 2004, 203,653 domains have adopted SPF in some form.
- Amazon, Earthlink, Red Hat, Verizon etc.



Source: <http://spftools.infinitepenguins.net/register.php>

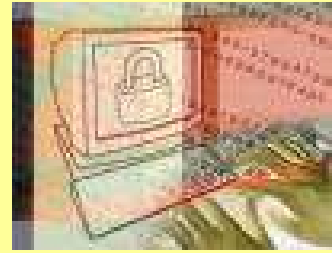
Industry Adoption – Sender ID



- Companies that either currently use products that support Sender ID, have plans to implement Sender ID or are in process of upgrading to Sender ID.

COMPANIES WITH PRODUCTS THAT SUPPORT SENDER ID			
AOL	Barracuda Networks	CipherTrust	Cloudmark
ESPC	GoDaddy.com	Hotmail (will implement Sender ID)	IronPort Systems
Microsoft Exchange (upgrading to Sender ID)	MSN Services (will implement Sender ID)	Port25 Solutions, Inc.	Sendmail (upgrading to Sender ID)
Symantec	Trust-e	Tumbleweed Communications	VeriSign

Industry Adoption - DomainKeys



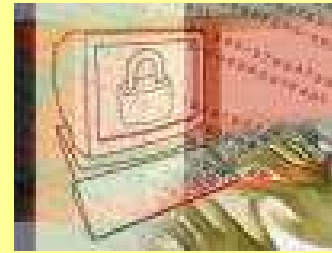
- Yahoo! Inc.
- Very few other domains have actually implemented DomainKeys

Empirical Statistics

- 100 Top Domains Queried
- SPF deployed by 19%
- Many of these companies publish SPF records, but do not check them for incoming mail

EXPERIMENT RESULTS	
DOMAIN TESTED	SENDER AUTHENTICATION TECHNOLOGY(IES) SUPPORTED
about.com	SPF v1
advertising.com	SPF v1
altavista.com	SPF v1
amazon.com	SPF v1
aol.com	SPF v1
apple.com	SPF v1
craigslist.org	SPF v1
doubleclick.com	SPF v1
ebay.com	SPF v1 / SPF v2
excite.com	SPF v1
google.com	SPF v1
lycos.com	SPF v1
match.com	SPF v1
myway.com	SPF v1
netzero.com	SPF v1
nytimes.com	SPF v1
real.com	SPF v1
symantec.com	SPF v1
xanga.com	SPF v1

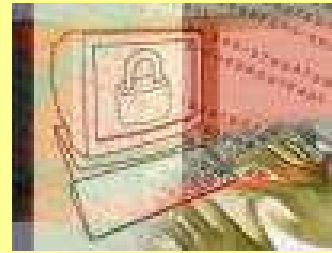
Evaluation: Real-World Application



Effectiveness/Performance Aspects:

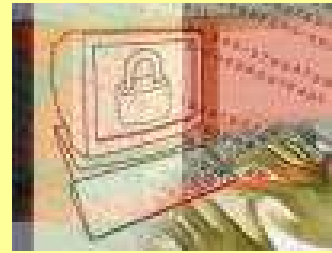
- SPF – Easy to implement, low resource overhead, vulnerable to threats.
- Sender ID – Slightly difficult to implement, low resource overhead, vulnerable to threats
- DomainKeys – Fairly complex implementation, high resource overhead, less vulnerable.

Threats/Vulnerabilities



- All proposals do what they claim
- Principle of Easiest Penetration
- Implementation Vulnerabilities

Threat #1:



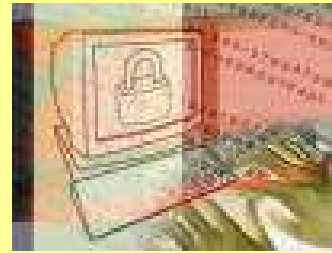
DNS Hijacking

SPF: **Vulnerable**

Sender ID: **Vulnerable**

DomainKeys: **Not Vulnerable**

Threat #2:



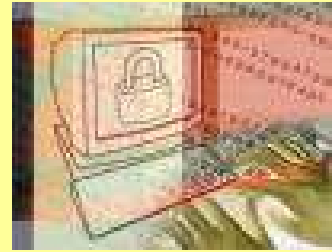
Spoofting the username portion of an e-mail address

SPF: **Vulnerable**

Sender ID: **Vulnerable**

DomainKeys: **Vulnerable**

Threat #3:



Password Cracking

SPF: **Vulnerable**

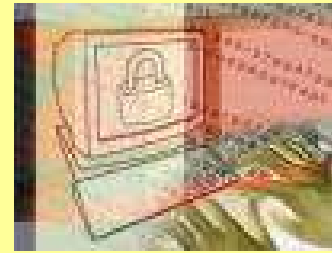
Sender ID: **Vulnerable**

DomainKeys: **Vulnerable**

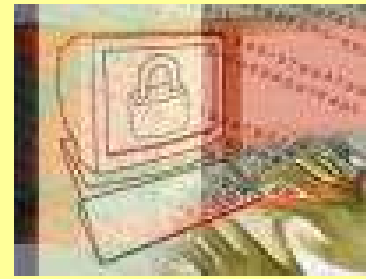
Examination: Comparison

METRIC	SPF	SENDER ID	DOMAINKEYS
“DOES IT WORK?”	10 It does what it claims to do	10 It does what it claims to do	10 It does what it claims to do
TRANSPARENCY TO END-USERS	10 The user does not need any new mail applications or any new settings	10 The user does not need any new mail applications or any new settings	10 The user does not need any new mail applications or any new settings
SIMPLICITY OF INITIAL CONFIGURATION	8 Only requires receiving SMTP server modifications and intuitive additions to DNS records	7 Only requires receiving SMTP server modifications and slightly more complicated additions to DNS records	4 Requires sending and receiving SMTP server modifications, public/private encryption key generation and maintenance, and public key published in DNS records
COMPLEXITY / PERFORMANCE	8 Simple DNS record additions and low overhead on part of receiving SMTP servers	7 Slightly more complicated DNS additions and low overhead on part of receiving SMTP servers	4 Require processor-intensive encryption/decryption at sending/receiving SMTP servers. Also, have to maintain the security of the private key(s)
ADOPTION RATE	8 Already have the necessary DNS entries on multiple internet servers	5 Superset of SPF. Has backing from Microsoft	3 Very few servers have public keys published in DNS records. More relatively new to the scene compared to SPF
IMMUNITY TO THREATS	5 Vulnerable to DNS highjacking and sender-authenticated message contents can be modified in transit	5 Vulnerable to DNS highjacking and sender-authenticated message contents can be modified in transit	10 Authenticates sending domain and digitally signs entire message. Technically speaking, more secure
TOTALS:	49	44	41

Conclusion



- SPF scored the highest overall
- Microsoft's Sender ID improves upon SPF, but patents have hurt its adoption
- DomainKeys is the most technically sound proposal, but is a latecomer, and requires significant hardware upgrades
- Any of the 3 proposals will significantly improve SMTP, but will not eliminate the SPAM / phishing problem



Questions ?

References

- [1] Conry-Murray, Andrew. "E-Mail Authentication Via Sender ID." 27 Sept. 2004. Desktop Pipeline. 03 Nov. 2004 <<http://www.desktoppipeline.com/trends/47903288>>.
- [2] "DomainKeys: Proving and Protecting Email Sender Identity." 2004. Yahoo! 01 Nov. 2004 <<http://antispam.yahoo.com/domainkeys>>.
- [3] "Email Sender ID: The Hype and the Reality." 24 Aug. 2004. NewsForge: The Online Newspaper for Linux and Open Source. 02 Nov. 2004 <<http://www.newsforge.com/article.pl?sid=04/08/26/1326244>>.
- [4] Wong, Meng and Mark Lentzner. "Sender Policy Framework." May 2004. IC Group, Inc. 18 Oct. 2004 <<http://spf.pobox.com/spf-draft-200406.txt>>.
- [5] "Microsoft Is Committed to Help End the Spam Epidemic." 23 June 2004. Microsoft. 31 Oct. 2004 <<http://www.microsoft.com/mscorp/twc/privacy/spam.mspx>>.
- [6] "Sender ID Framework at a Glance." 30 Sept. 2004. Microsoft. 07 Oct. 2004 <http://www.microsoft.com/mscorp/twc/privacy/spam_senderid.mspx>.
- [7] Wagner, Jim. "Exposed Sender ID Patents Up Debate." 20 Sept. 2004. InternetNews.com. 31 Oct. 2004 <<http://www.internetnews.com/dev-news/article.php/3409971>>.
- [8] "Sender ID Framework." 06 Oct. 2004. Microsoft. 31 Oct. 2004 <http://www.microsoft.com/mscorp/twc/privacy/spam_senderid_itpro.mspx>.
- [9] InfinitePenguins.Net. 27 Oct. 2004. InfinitePenguins.Net. 03 Nov. 2004 <<http://spftools.infinitepenguins.net/register.php>>.
- [10] "Betamax." 18 Sept. 2004. Wikipedia: The Free Encyclopedia. 03 Nov. 2004 <<http://en.wikipedia.org/wiki/Betamax>>.
- [11] "Sender ID Framework Industry." 30 Sept. 2004. Microsoft. 07 Oct. 2004 <http://www.microsoft.com/mscorp/twc/privacy/spam_senderid_providers.mspx>.
- [12] "Whither Sender ID?" 17 Sept. 2004. Computer Business Review Online. 02 Nov. 2004 <http://www.cbronline.com/article_feature.asp?guid=B1721863-ECB3-4644-A270-A978BAA179EA>.
- [13] Wagner, Jim. "Microsoft Faces Lawsuit Over Caller ID for E-Mail" 11 Aug. 2004. InternetNews.com. 02 Nov. 2004 <<http://www.internetnews.com/security/article.php/3393891>>.
- [14] Wagner, Jim. "AOL Dumps Sender ID." 15 Sept. 2004. InternetNews.com. 31 Oct. 2004 <<http://www.internetnews.com/xSP/article.php/3408601>>.
- [15] Wagner, Jim. "Microsoft, AOL Resurrect Sender ID." 25 Oct. 2004. InternetNews.com. 31 Oct. 2004 <<http://www.internetnews.com/security/article.php/3426291>>.
- [16] Regan, Keith. "Microsoft Revises Sender ID, AOL Signs On." 26 Oct. 2004. E-Commerce Times. 03 Nov. 2004 <<http://www.ecommercetimes.com/story/37616.html>>.
- [17] Roberts, Paul. "Spammers using sender authentication too, study says." 31 Aug. 2004. Infoworld. 31 Oct 2004 <http://www.infoworld.com/article/04/08/31/HNspammerstudy_1.html>.
- [18] Knight, Will. "RSA Security site defaced." 13 Feb 2000. ZDNet. 31 Oct. 2004 <<http://zdnet.com.com/2100-11-518535.html?legacy=zdn>>.
- [19] Edwards, Mark. "Something Old, Something New: DNS Hijacking." 16 Feb. 2000. Windows IT Pro Magazine. 31 Oct 2004 <<http://www.winnetmag.com/Article/ArticleID/8170/8170.html>>.
- [20] German, Bob. "New mail blocks result of Ralsky's latest attacks?" Online posting. 10 Oct 2003. 31 Oct. 2004 <<http://www.merit.edu/mail.archives/nanog/200310/msg00569.html>>.
- [21] Mitchell, Anne P. "Google's Gmail Adopts Yahoo's Domain Keys Authentication Technology." 19 Oct. 2004. thespamweblog. 03 Nov. 2004. <<http://spam.weblogsinc.com/entry/3081199343254187/>>.
- [22] "Sender Policy Framework." IC Group, Inc. 14 Oct. 2004 <<http://spf.pobox.com/howworks.html>>.
- [23] Danisch, Hadmut. "The RMX DNS RR and method for lightweight SMTP sender authorization: draft-danisch-dns-rr-smtp-04.txt." May 2004. Internet Engineering Task Force. 20 Oct. 2004 <<http://www.ietf.org/internet-drafts/draft-danisch-dns-rr-smtp-04.txt>>.
- [24] Fecyk, Gordon. "Pan-Am Internet Services, Computer and Internet Consulting in Winnipeg Manitoba Canada." Dec. 2003. Pan-Am Internet Services. 20 Oct. 2004 <<http://www.pan-am.ca/dmp/draft-fecyk-dmp-01.txt>>.
- [25] "Wikipedia: The Free Encyclopedia." 27 Mar. 2004. Wikipedia Foundation, Inc. 1 Nov. 2004 <http://en.wikipedia.org/wiki/Sender_Policy_Framework#Limitations_and_controversies>.
- [26] Wong, Meng W. Interview with CircleID Reporter. 29 June 2004. CircleID. 30 Oct. 2004 <http://www.circleid.com/article/634_0_1_0_C/>.
- [27] "Sender Policy Framework." IC Group, Inc. 14 Oct. 2004 <<http://spf.pobox.com/faq.html>>.
- [28] "Sender Policy Framework." IC Group, Inc. 14 Oct. 2004 <<http://spf.pobox.com/adoption.html>>.