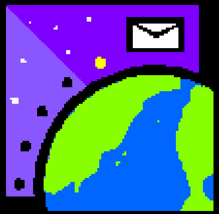
Stopping Email Abuse

– An Engineer’s Perspective

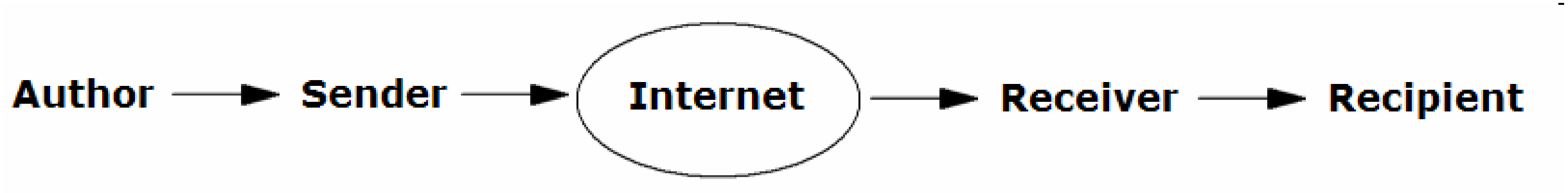
Dr. David MacQuigg, President
Open-mail.org

University of Arizona
ECE 596c
August 2006



- How the Email System Works
  - Actors, Agents, Terminology
  - Email Identities, Authentication Methods
- Reputation/Accreditation Systems
  - Registry of Public Email Senders™
  - Receiver Setup
  - Border Patrol™ MTA
  - Reputation Statistics
- Social Factors
  - Barriers to Adoption
  - Economics of Email Abuse

Simple Mail Transfer



Actors include Users and Agents
Users include Authors and Recipients
Agents include Senders, Receivers and Forwarders

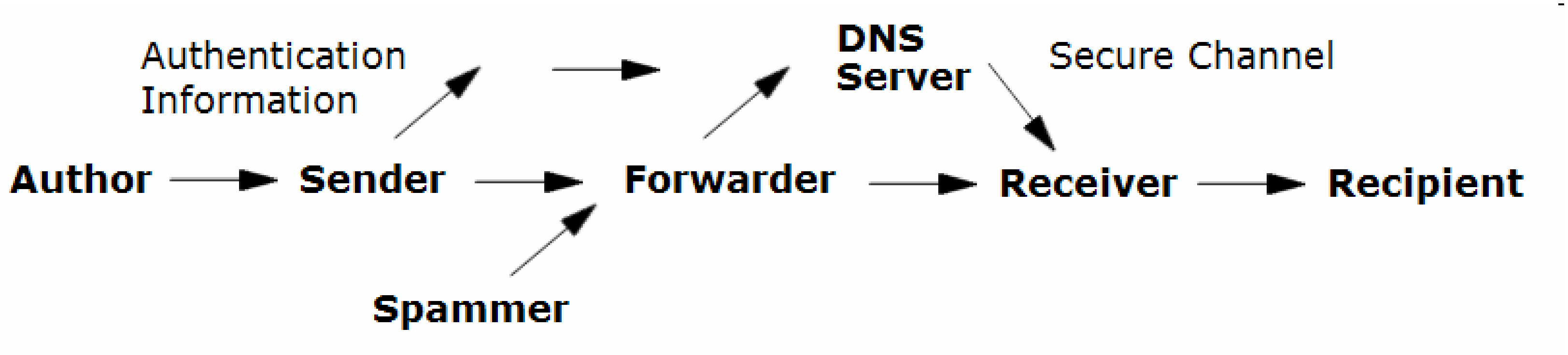
Forwarders include:

Recipient's Forwarders (most common)

Sender's and Receiver’s Forwarders
Open Relays (banned)

Routers are Invisible to Email – We depend on them only to preserve IP source and destination addresses.

Forgery is the Critical Factor in Email Abuse

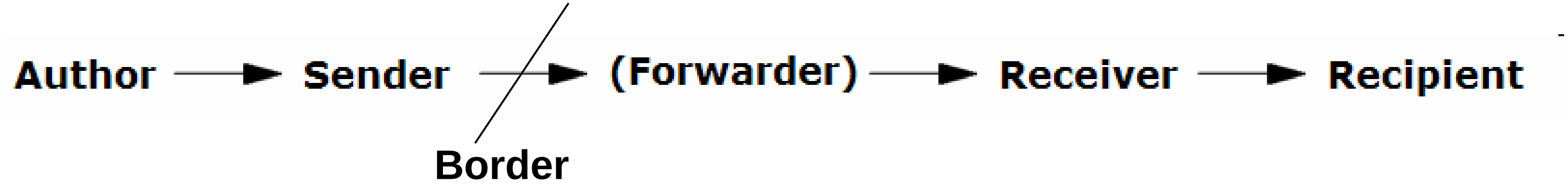


Authentication stops forgery.

IP-based Authentication (SPF, SenderID, CSV, PTR):
Domain owner provides a list of authorized IP addresses.
Fast, minimum mail-transfer overhead.

Signature-based Authentication (DKIM):
Domain owner provides a Public Key via a secure channel.
Messages are signed with the related Private Key.
End-to-end protocol allows arbitrary forwarding.
High security.

Precise Terminology


Author → Sender → (Forwarder) → Receiver → Recipient

Border

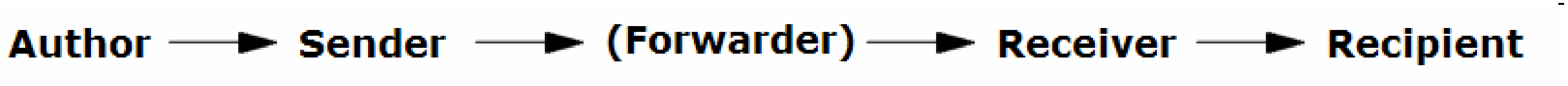
The **Border** is the only interface with no established trust relationship.

"Mail Transfer Agent (**MTA**)" is a commonly-used term for a mail-handling program. A typical mailflow involves mutliple MTAs for each Agent. We will use "**Agent**" to mean an individual or organization, and "**MTA**" to mean a program or process.

"**Border MTAs**" include "**Transmitters**" and "**Receiving MTAs**" or "receivers". Transmitters have a special role in limiting spam and abuse in outgoing mail, and in ensuring valid identities associated with that mail. Receiving MTAs have a special role in rejecting mail with forged identities.

Other programs with special roles include the Sender's MSA (Mail Submission Agent), the Receiver's MDA (Mail Distribution Agent), and the User's MUA (Mail User Agent). Again, we will use the acronyms to avoid confusion over the word Agent.

Identities in an Email Session



Author → Sender → (Forwarder) → Receiver → Recipient

```
  $ telnet open-mail.org 25
  220 open-mail.org ESMTP Sendmail 8.13.1/8.13.1; Wed, 30 Aug 2006 07:36:42 -0400
1 HELO mailout1.phrednet.com
  250 open-mail.org Hello ip068.subnet71.gci-net.com [216.183.71.68], pleased to meet you
2 MAIL FROM:<macquigg@box67.com>                          6 Network Owner
  250 2.1.0 <macquigg@box67.com>... Sender ok
3 RCPT TO:<jman@box67.com>
  250 2.1.5 <jman@box67.com>... Recipient ok
  DATA
  354 Enter mail, end with "." on a line by itself
4 From: Dave\r\nTo: Test Recipient\r\nSubject: SPAM SPAM SPAM\r\n\r\nThis is message 1 from our test
  script.\r\n.\r\n
  250 2.0.0 k7TKIBYb024731 Message accepted for delivery
  QUIT
  221 2.0.0 open-mail.org closing connection
```

RFC-2821

1 Helo Name

Envelope Addresses:

2 Return Address

3 Recipient Addresses

RFC-2822

Header Addresses:

4 From Address

5 Reply-To Address

Registry of Public Email Senders™

ID Owner publishes:

```
_auth.example.com.  TXT  "method=SPF,DK helo=192.168.92.216-8"
```

The Registry publishes:

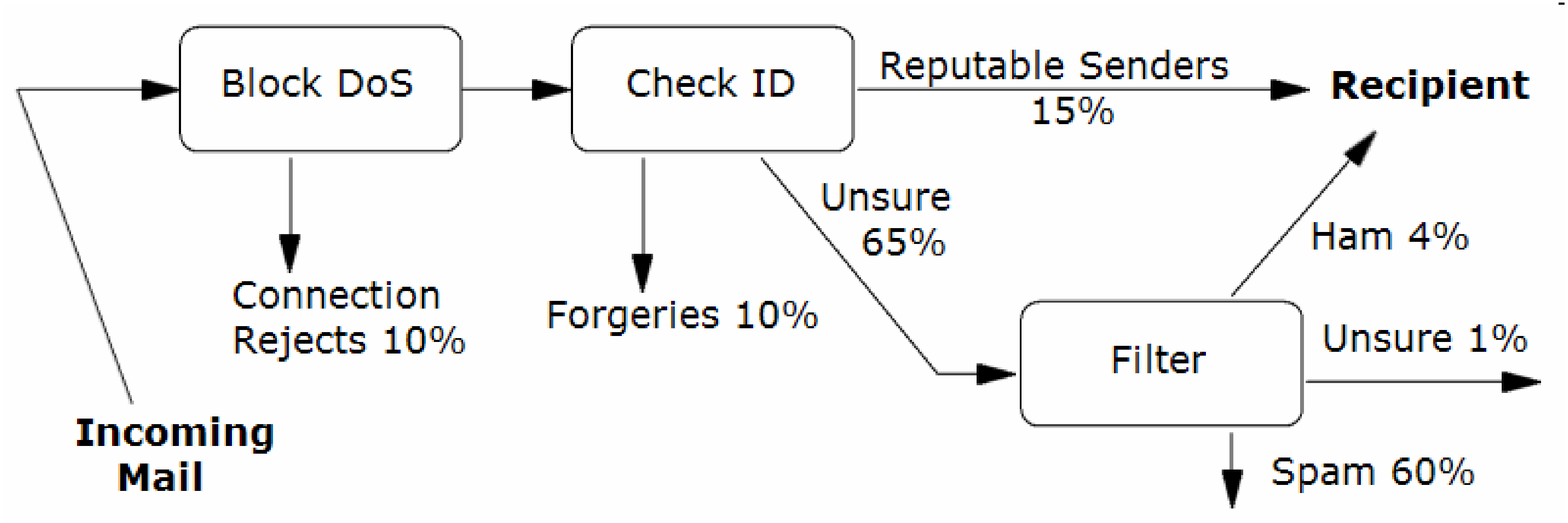
```
example.com.s-id.net. TXT "svc=X1:A,S2:A mth=SPF+5,DK+3 ip4=192.168.92.216-8"
```

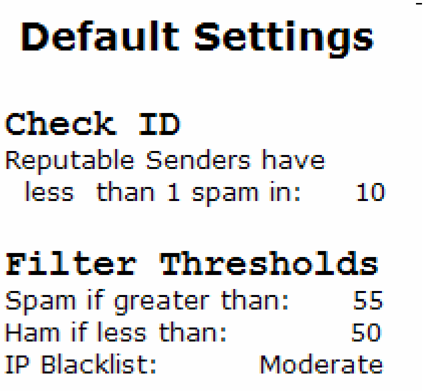
The ID owner has complete control of the Registry record, except for data from the Rating Services, and the numbers showing how many DNS queries it took to run the method.

Which authentication methods are used depends on what the Sender offers, and what the Receiver will accept. The Registry has no favorite method.

HELO addresses can be checked without any authentication method.

Border Patrol™ MTA





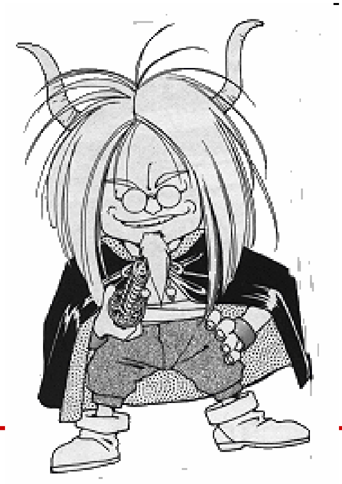
Default Settings

Check ID

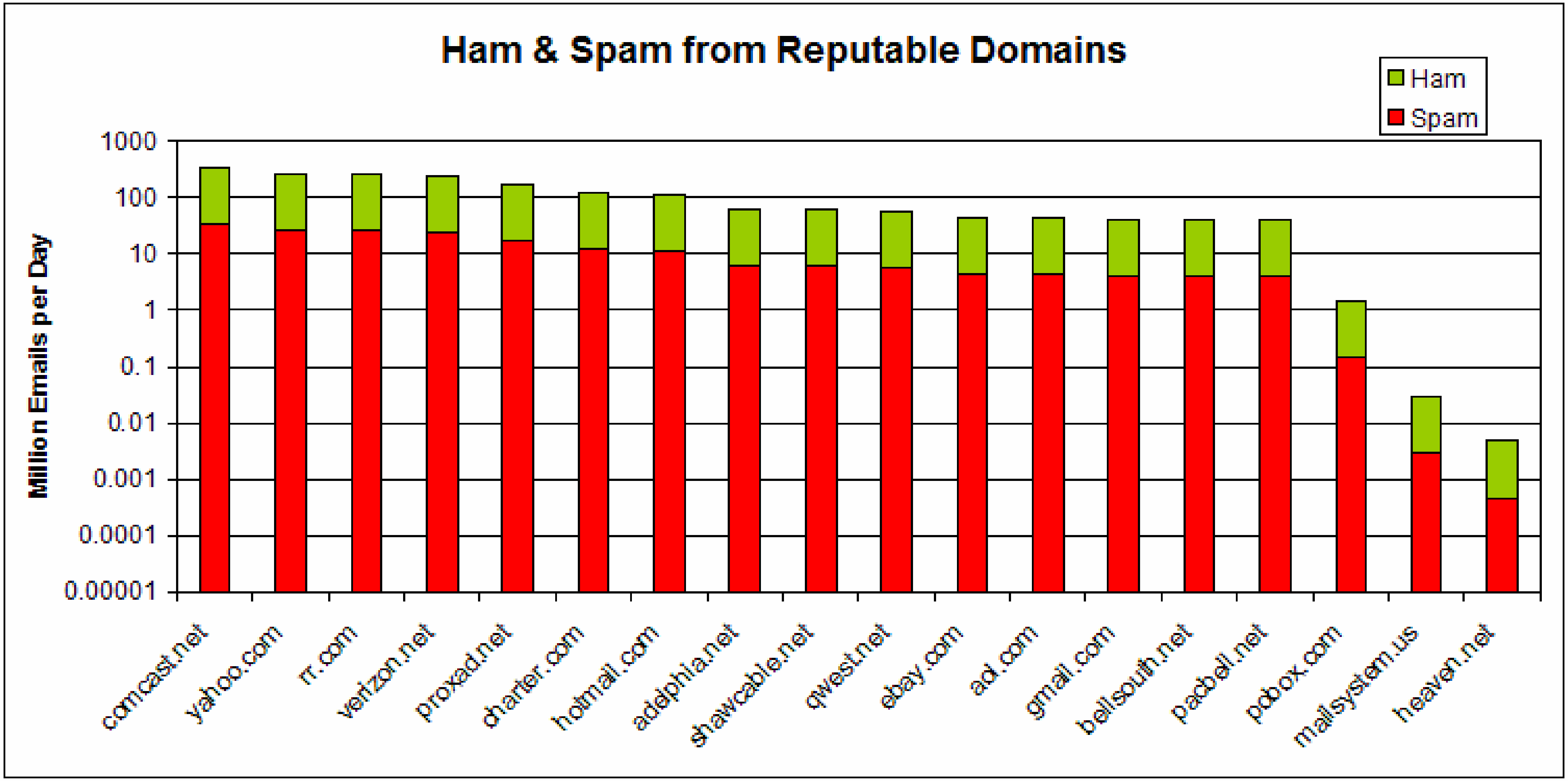
Reputable Senders have less than 1 spam in:	10

Filter Thresholds

Spam if greater than:	55
Ham if less than:	50
IP Blacklist:	Moderate



Reputation Statistics



Need real data !!

Barriers to Adoption

Hurdles that anti-spam systems must avoid or overcome,
in order of decreasing severity:

1) Required simultaneous upgrades in software or setup. (Flag Day)

2) Required widespread adoption by Agents before any benefit is realized by Recipients. (By June 30th, all senders will ...)

3) Required widespread adoption of one company's method or service. (Microsoft patent)

4) Changes that cause a temporary degradation in service. (Turn off your spam filters and ...)

5) Changes in current practices.
   a) A well-established and standards-compliant practice.
   b) A widespread but non-standardized practice. ("Misuse" of Return Address)
   c) A widespread but non-compliant practice. (bad HELO name)
   d) An already unacceptable practice. (open relays)

6) Costs to senders.
   a) Loss of mail due to mistakes by others. (SPF "forwarding problem")
   b) Registration fees or administrative costs.

Economics of Email Abuse

$200B	annual benefit of email
$20B	cost of abuse
	100M users x ($.25/day deleting spam + $100/yr false rejects)
$2B	benefit to anti-spam industry
	100 companies x $20M/yr
$0.2B	benefit to spammers
	10K spammers x $20K/yr
$0.02B	cost of an effective authentication/reputation system
	10M users x $2/yr
	100K companies x $200/yr (90% internal, 10% external services)

Bibliography

A short list of the most useful books and articles on the technology underlying email.

- **TCP/IP Illustrated, vol. I, The Protocols,** W. Richard Stevens, 1994. Very thorough, yet readable. Good illustrations.
- **"Internet Mail Architecture",** D. Crocker, http://tools.ietf.org/html/draft-crocker-email-arch-06 (work in progress) - a much more detailed description of the current email system with references to the relevant RFC standards.
- **Pro DNS and BIND,** Ron Aitchison, 2005. – Excellent book on the Domain Name System and the most popular DNS server.
- **"CircleID",** http://www.circleid.com – a "Collaborative Intelligence Hub for the Internet's Core Infrastructure & Policies" – current articles by top industry experts.

Project Links

- https://open-mail.org – Current status of our project.
- http://purl.net/macquigg/email – Articles and notes from early development.