SENDMAIL®

DomainKeys Identified Mail (DKIM): Introduction and Overview

Eric Allman

Chief Science Officer

Sendmail, Inc.

The Context

- Traditional Content Scanning is reaching its limits

- Increasing interest in making life better for good players (in addition to penalizing bad players)
  - Messages from good senders can be delivered without spam scanning to reduce load and avoid false positives
  - Messages from known bad senders should be slowed down, carefully scanned, greylisted, challenged, or rejected outright

- Good senders want an ability to demonstrate their goodness, either by Accreditation (3rd party assurance) or Reputation

“Identity-Based” Filtering

- For most people, 90–99% of their legitimate email comes from people or entities they know
  - Notable exceptions: help desks, inquiry addresses, “info@” addresses, etc.
  - Allow (white) lists can reduce false positives
  - I’ll accept mail from my mother, my boss, or my bank without scanning

- Also, 90–99% of their spam comes from people or entities they do not know
  - Notable exception: on-line order acknowledgments

- Critical: must ensure sender is who they claim to be
  - ... not someone pretending to be my bank
  - Phishing usually involves identity theft
  - Authentication required

Authentication vs. Authorization

- People often confuse the two

- Authentication: proof that you are who you claim to be
  - Real life example: a passport

- Authorization: what you are allowed to do, generally based on:
  - Real life example: a visa in a passport
  - Prior knowledge by recipient of who you are
  - Trusted third party accreditation
  - Local- or network-wide reputation
  - “Entry methods” such as Challenge-Response or content scanning

Overview of DKIM

- Cryptography-based protocol, signs selected header fields and message body
  - Merge of DomainKeys (Yahoo!) and IIM (Cisco)
  - Merge created by an industry consortium
  - Significant industry support (see dkim.org for a list)

- Intended to allow good senders to prove that they did send a particular message, and to prevent forgers from masquerading as good senders (if those senders sign all outgoing mail)

- Not an anti-spam technology by itself

DKIM Goals

- Low-cost (avoid large PKI, new Internet services)
- No trusted third parties required (e.g., key servers)
- No client User Agent upgrades required
- Minimal changes for (naïve) end users
- Validate message itself (not just path)
- Allow sender delegation (e.g., outsourcing)
- Extensible (key service, hash, public key)
- Structure usable for per-user signing

DKIM Technology

- Signature transmitted in DKIM-Signature header field
  - DKIM-Signature is self-signed
  - Signature includes the signing identity (not inherently tied to envelope, `From:`, `Sender:`, or any other header)
- Initially, public key stored in DNS (new RR type, fall back to TXT) in `_domainkey` subdomain
  - Extensible to other key delivery mechanisms
- Namespace divided using *selectors*, allowing multiple keys for aging, delegation, etc.
  - Example: selectors for departments, date ranges, or third parties
- *Sender Signing Policy* lookup for unsigned, improperly signed, or third-party signed mail

DKIM-Signature header

- Example:

```
DKIM-Signature: a=rsa-sha1; q=dns;
  d=example.com;
  i=user@eng.example.com;
  s=jun2005.eng; c=relaxed/simple;
  t=1117574938; x=1118006938;
  h=from:to:subject:date;
  b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSb
    av+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

- DNS query will be made to:

```
jun2005.eng._domainkey.example.com
```

DKIM Status and Directions

- Currently submitted to Internet Engineering Task Force (IETF) as Internet-Drafts.
  - `draft-ietf-dkim-base-00.txt`
  - `draft-allman-dkim-ssp-01.txt`
  - `draft-fenton-dkim-threats-02.txt`
- Still some other drafts to be written
- IETF Working Group chartered, first meeting in March
- Several interoperating implementations, some open source
  - `http://sourceforge.net/projects/dkim-milter`

Eric Allman

Sendmail, Inc.