Beyond Sender ID and SPF — Cryptographic Solutions

Eric Allman
CTO

Cryptography-Based Authentication

- Conceptually simple: digitally sign the header and body using well-understood techniques
- Survives forwarding with no problems, but…
- Sensitive to message modification during transit
- Distribute public key using DNS
  - Avoids need for large Public Key Infrastructure
- Implementation tricky:
  - Some message modification during transit
  - Getting crypto correct and secure can be hard
  - Need for back-compatibility

Background of DomainKeys Identified Mail (DKIM)

- Started as merge of DomainKeys (Yahoo!) and Identified Internet Mail (Cisco)
- Announced recently (June), but work goes back to October (serious work started in January)
- Unprecedented industry cooperation
  - Participants include Alt-N, AOL, Brandenburg InternetWorking, Cisco, EarthLink, IBM, Microsoft, PGP Corporation, Sendmail, Strongmail, Tumbleweed, VeriSign, Yahoo!

DKIM Goals

- Low-cost (avoid large PKI, new Internet services)
- No trusted third parties
- No client User Agent upgrades required
- Transparent to end users
- Validate message itself (not just path)
- Allow sender delegation (e.g., outsourcing)
- Extensible to per-user signing

Technical Overview

- Signs body and selected parts of header
- Signature transmitted in DKIM-Signature header
  - DKIM-Signature is self-signed
  - Signature includes the signing identity (not inherently tied to From:, Sender:, or even header)
- Public key stored in DNS (new RR type, fall back to TXT) in **`_domainkey`** subdomain
- Namespace divided using selectors, allowing multiple keys for aging, delegation, etc.
- Sender Signing Policy lookup for unsigned or improperly 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=nowsp;
  t=1117574938; x=1118006938;
  h=from:to:subject:date;
  b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSb
    av+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

- DNS query will be made to:

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

Status of DKIM Specification

- At least three documents
  - Base, Sender Signing Policy, New DNS RR types
- Base document fairly stable, submitted to IETF
  - draft-allman-dkim-base-00.txt
- Sender Signing Policy in good shape but more to do; draft submitted to IETF
- New DNS RR types not yet started
- Three interoperating prototypes already running
  - At least two to be open sourced
- Standardization to proceed through IETF

What You Can Do to Prepare

- Audit your mail systems (incoming and outgoing)
- Find out who is (legitimately) sending mail as you
  - Satellite offices
  - Road warriors
  - Outsourcers
- Determine where incoming mail is being received
- Both of these can have lots of surprises
- You'll need to know these regardless of what scheme you use (Path-based or Signature-based)

Implementation Requirements

- Software upgrades at sender and recipient sites
  - Can (probably should) be at gateway
- Key generation and distribution (in DNS)
- Road Warriors may require conversion to VPN or SMTP Authentication
  - "Call home" and authenticate to send mail
  - Good support in most modern email clients
- CPU overhead appears to be about 5–10% based on early testing (but mail servers not CPU bound)

IP & Signing Overview

	Sender ID Framework		DKIM / DK
	Mail From	**PRA**	
How is validation performed?	RFC2821 MAIL FROM address, "bounce" or "envelope from" address	RFC2822 From address	Designated "signer" address/ RFC2822 From address
Strengths	Reduces bounce messages where the victim receives errors for mail they didn't sent	Validates the identity most users see and reduces the threat to phishing.	Provides end-to-end validation over multiple hops, (i.e forwarding).
MTA Updates	Receiving update required.		Sender and Receiving MTA update required
Weaknesses	Only validates the last hop		Can be "broken" by imperceptible changes
Records Publishing / Signing	Easy. Publish and maintain in DNS.		Create keys and publish in DNS.
Mailing lists	**Easy**		Hard
Forwarding	Hard	Requires an header added	**Easy**
Performance	Negotiable. ISPs may cache records for performance		5-10% processing CPU

Timing

- DKIM is similar to DomainKeys
  - DomainKeys keys can be used by DKIM
- DomainKeys already deployed by many large players (Yahoo, Gmail); DKIM upgrade expected to be easy, and can run in parallel with DomainKeys
- Prediction: DKIM deployment will start in 2006 (some leading edge adopters this year)
- Time to plan for DKIM is NOW