DomainKeys Overview

Miles Libbey

Anti-spam Product Manager, Yahoo! Mail

Nov 9, 2004

Why use cryptography for sender authentication?

- IP address is insufficient for email identity today

- IP addresses currently don’t work well with Email Service Providers (ESP)
  - Receiver applies ESP’s reputation instead of client’s reputation
  - Many ESPs use 1 IP address for all their clients – reputation of 1 client can ruin reputation for others

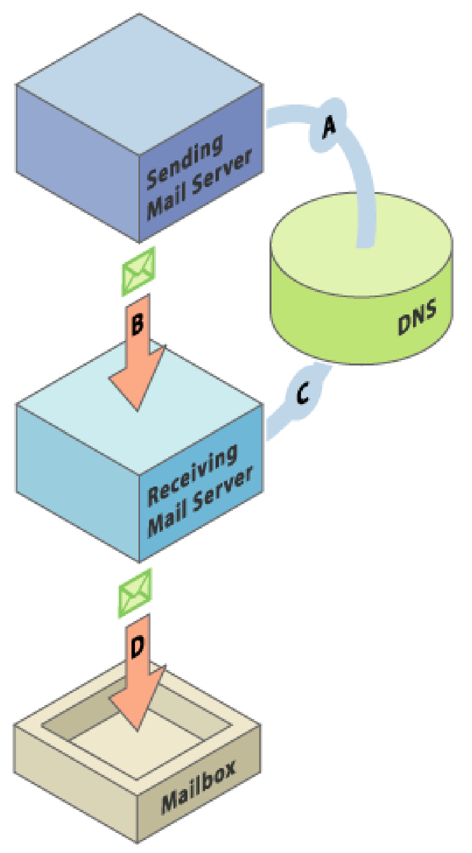
- IP addresses don’t survive forwarding (Goodguy ➔ Forwarder ➔ Recipient)
  - Forwarding system spam reputation probably mixed – in most cases blindly forwarding on spam
  - We need to apply Goodguy reputation – users want that mail in their inbox
  - How does recipient system know if they can trust forwarding system to validate header or message integrity
- Invisible to the user – they don’t know or care about IP addresses

DomainKeys technology summary: Setup

- Domain owner self generates private/public key pair
- Domain owner publishes public key in new, standardized DNS txt record
  - Private/Public keys determined solely by domain owner
  - As secure as DNS
  - Domain owner can revoke at will
  - Can have multiple keys per domain
  - Domain owner can ‘safely’ give their ESP a private key
    - Multiple keys allow multiple identities
    - Can constrain key to use by particular username
    - Can revoke after contract is done

DomainKeys technology summary: Sign and Verify

- Outbound email signed with private-key
  - Headers, body
  - Signature stored in header, adding ~150bytes to msg size
- Receiving system
  - Finds domain in body’s From: address
  - Retrieves public-key from domain’s DNS record
  - Verifies content was signed by corresponding private key, thus proving the From: domain



Designed for flexibility with minimal adoption hurdles

- Reuse existing hardware and software to minimize deployment cost
- Enables other technologies (BATV etc) to use keys
- DNS caching has significant performance benefits

Use Case: ESP on behalf of Company

- Company could give ESP a private key to use for signing
  - Publish public portion in DNS
  - Can constrain username options for key
  - Revoke at anytime

- Company could delegate sub-domain DNS
  - ESP responsible for DNS and MTA mgmt
  - Revoke delegation at anytime

Use Case: Mailing List

- Mailing list that doesn't change content
  - Signature not broken.
  - Can choose reputation it wants applied to its email

- Mailing list that changes content (e.g. Yahoo! Groups)
  - Adds an advertisement, unsubscribe instructions to email, breaking signature
  - Add Sender: header, and resign email
  - ISP likely wants to apply list reputation to email

Use Case: Forwarder

- Original author signs mail, and is verified using DomainKeys

Use case: Send this page to a friend

- News source can claim authorship of news story
  - From: news_articles@nytimes
  - Sender: news_articles@nytimes
  - Set Reply-to: as sending user’s address

Licensing

- Two defensive patents files surrounding DomainKeys
- Patent license designed to allow freedom to operate, while protecting industry
  - Royalty free
  - Sub-licensable
  - Perpetual unless sue Yahoo! or other implementer over DomainKeys
  - No registration required

Perceived Issues

- CPU Cost:
  - Sendmail study shows 8-16% mail server software CPU increase
- Replay: Spammer can forge own identity
  - A reputation problem; not authentication issue
- Message Integrity: Content changes are not authorized
  - Message can be re-signed, authorizing changes

Status

- Draft revision submitted to IETF mid August
- Yahoo! Mail in final stages of deployment process for signing. SBC, BT, Rogers to follow shortly.
- Yahoo! Mail, SBC, British Telecom, Rogers, to begin verification deployment shortly
- Receiving industry adoption: Gmail, Sify, Skylist have begun signing; AOL, Earthlink interested in testing
- Royalty free, open source reference implementation available on SourceForge
- Sendmail, Qmail, Exchange versions, as well as port25, OmniIT, Etype.net, and ActivSoftware support.

More information and specification:
http://antispam.yahoo.com/domainkeys

Tools for deployment
http://domainkeys.sourceforge.net