So You've Got Authentication Now. Yippee.

Eric Allman
Sendmail, Inc.
MIT Spam Conference
March 2006

Obligatory Outline

SENDMAIL

- What Sender Domain Authentication Is
- What Sender Domain Authentication Isn't
- Brief DKIM Status Report
- How Do You Make Authentication Useful?
- How Do You Get it Adopted?

What Sender Domain Authentication Is

SENDMAIL®

- *(Phrasing is very political)*
- Primarily, a way for a signer to be able to assert that they really did process the mail, at least as far as signing it
  - In some sense a signer is telling the world that it is willing to be judged on the basis of the messages it signs
  - Partially: non-repudiation
- Secondarily, a way for domains used in From: header fields to communicate their Signing Practices

What Sender Domain Authentication Isn't

SENDMAIL

Perfect

- False auth failures will probably exist for some time until the structure of the net adapts
- In near time, will be primarily allow good senders to prove that a message came from them

An anti-spam mechanism, at least by itself

- Authentication does not mean goodness — spammers can authenticate too

A complete anti-phishing mechanism

- False failures make this problematic short term
- Also consider, the "similar-domain" problem (e.g., ebay-billing.com), the "full name" problem (e.g., eric@sendmail.com <phisher@phishers.r.us>

DKIM (DomainKeys Identified Mail)

SENDMAIL

- One of many authentication proposals
- Based on cryptographic signatures
  - But not intended to overlap PGP or S/MIME
- Currently in IETF WG
- Threats document nearing completion
- Base document is looking fairly positive for publication this year
- Signing Practices (much debate on name) will take longer and be controversial
  - Overlaps with reputation
- Overview document just starting
  - To have non-normative language
- DNS RR type just starting

Making Authentication Useful

SENDMAIL®

- Just some examples:
- Create reliable whitelisting
- Display authentication results to user
- Add reputation/accreditation and stir
- Use it as input to a larger system
- *All of these have some current implementations but are also ripe research areas*

Reliable Whitelisting

SENDMAIL

- We do whitelisting today, but based on IP address (hard to manage) or unauthenticated addresses (easy to abuse)
- Probably tied in with user's address book or similar mechanism so that it is reasonably transparent
- May be able to auto-whitelist addresses that you send to (i.e., allow a response to come back)
- Could be enterprise whitelisting for partners, customers, etc.
- Undoubtedly many other clever algorithms

Display Authentication Results to User

SENDMAIL

- Fairly obvious, but….
- Has to be simple to understand
- Probably should not display authentication failures for now
- Should display the authenticated domain clearly
- Should check to see if that domain is one the user knows about, has good rep, etc.
  - Don't put green smiley-face next to phishing site
- Combine with reputation reporting, etc.

Add Reputation/Accreditation and Stir

SENDMAIL®

- Probably the next big development area
- Still many research/development areas here
  - Domains with mixed reputations (e.g., ISPs)
  - Distribution of reputation/accreditation information
  - Reputation recovery
  - Meta-reputation (reputation of reputation and accreditation servers)
  - Feedback loops
  - Who pays? (Sender, Recipient, nobody, other)

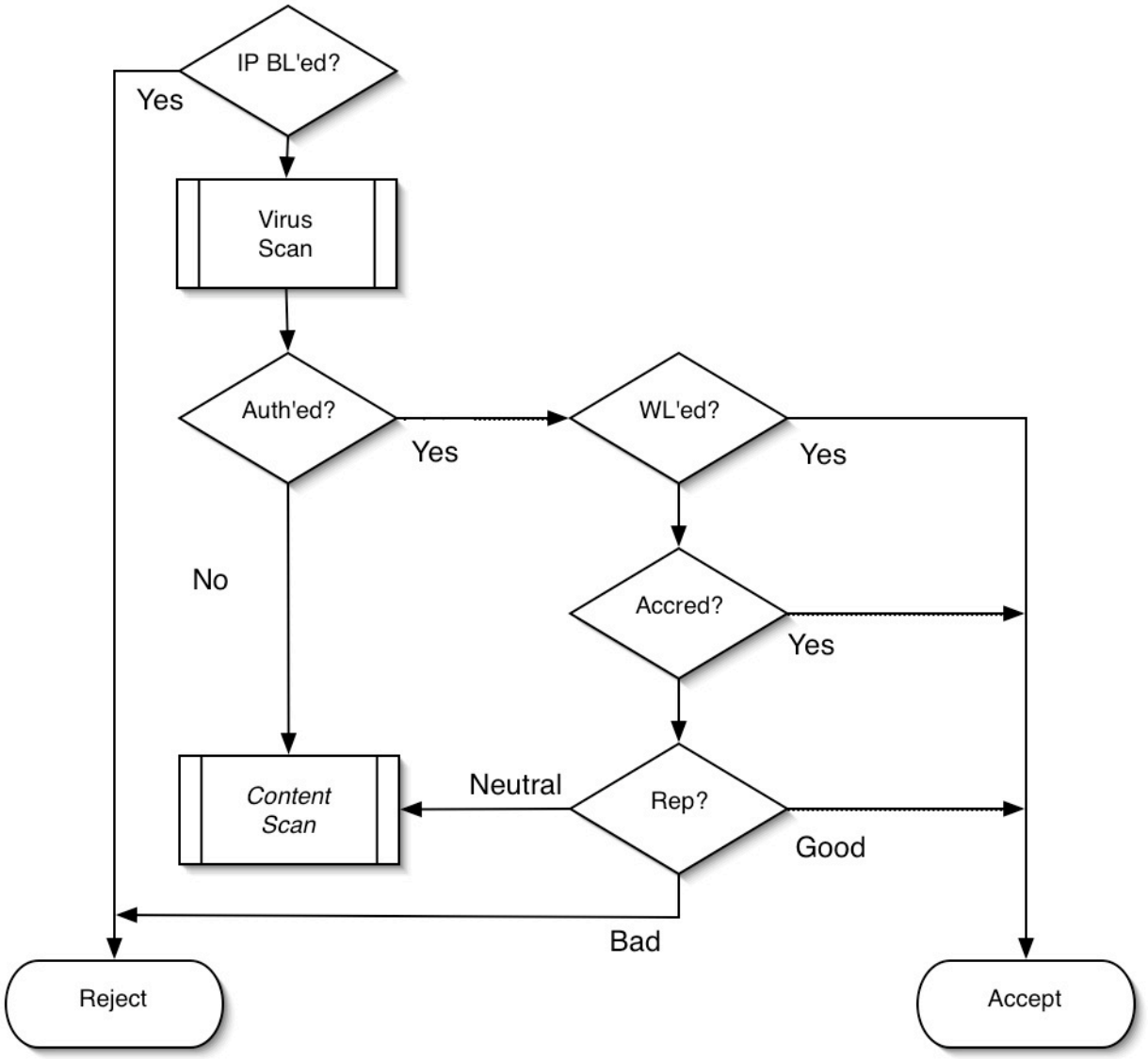
Use Authentication as Input to a Larger System

SENDMAIL®

- For example, spamassassin might use authenticated domains differently than unauthenticated domains
- Consider whitelists, blacklists, content scanning, challenge/response, etc.
- If most of my mail comes from known-good, authenticated senders, I don't need to content scan and can lower my FP rate
- Example (next page)

Potential Acceptance Flowchart (Simplified)

SENDMAIL®



Authentication Adoption

SENDMAIL

- A bit of chicken and egg problem
- Several large senders already adopting DomainKeys
  - Yahoo!, Gmail, Ebay, others
  - Creates demand for recipients to verify
  - Not a huge step from DK to DKIM
- Initially really only useful for filtering in good mail
  - This is valuable — can reduce false positive rate
- Challenge: Improving infrastructure to allow filter out
  - No munging in MTAs
  - All mailing list exploders updated
  - 8-bit MIME ubiquitous
  - Definitely a long-term horizon

Conclusions and Comments

SENDMAIL®

- Identity-based filtering can be a significant addition to the anti-spam toolkit
- Need authentication to achieve full potential of identity-based filtering
- Many areas ripe for research and development

Questions?