Achieving E2E Security

Phill Hallam-Baker

Comodo Inc.

http://prismproof.org/

15 Year Standards Stalemate

S/MIME

– Deployed in 5 billion clients

PGP

– Monopoly of mindshare

http://prismproof.org/

Solution

http://prismproof.org/

Success Criteria

- Everyone uses encryption by default

- Can’t be any more effort to use than email
  - Stop making humans do computer work
    - S/MIME certificate enrollment
  - Don’t need to be a human factors expert
    - Its removing stupidity, not being clever
    - Secure email is going to look the same as email

Dividing the Problem

Share this

Research here

3. **Trust Model**
4. **Transport**

http://prismproof.org/

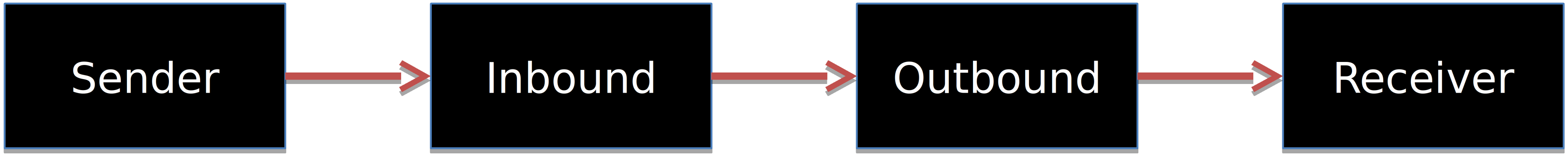
Alice sends email to Bob

- Types ‘Bo’
  - Autocompletes to “Bob” <bob@example.com>
- Checks it’s the right Bob
- Writes message
- Hits send

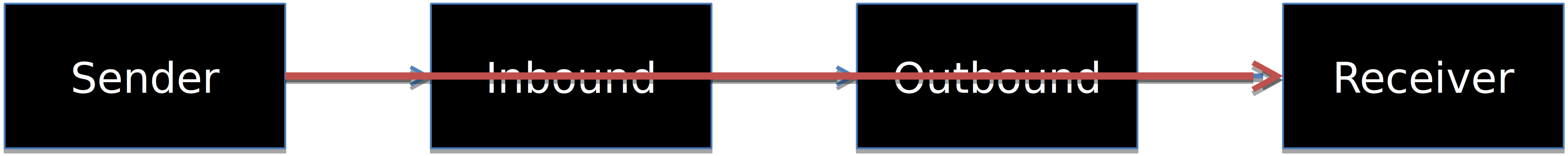
Why not encrypt?

- Sender Doesn’t know
  - The key to use
    - The key data
    - If it was the right key
    - If it is current
  - If Bob uses S/MIME or PGP
  - Cipher suites (most S/MIME limited to 3DES)
  - Wrapped message to protect headers
  - If Bob accepts or prefers encrypted mail

Security Models



Hop by hop



End to End

http://prismproof.org/

Asset Models

Asset	Hop by Hop	End to End
Content	TLS, S/MIME, PGP	S/MIME, PGP
Meta Data	TLS	[S/MIME]
Routing	TLS	
Traffic	Tor	

Content Protection

No apparent deficiencies

Meta Data Protection

Main

- Meta Data Protection
  - Wrap messages to hide headers[*]
  - STARTTLS Everywhere
  - STARTTLS Pinning

Desert

Exotic Transports

Onion routing

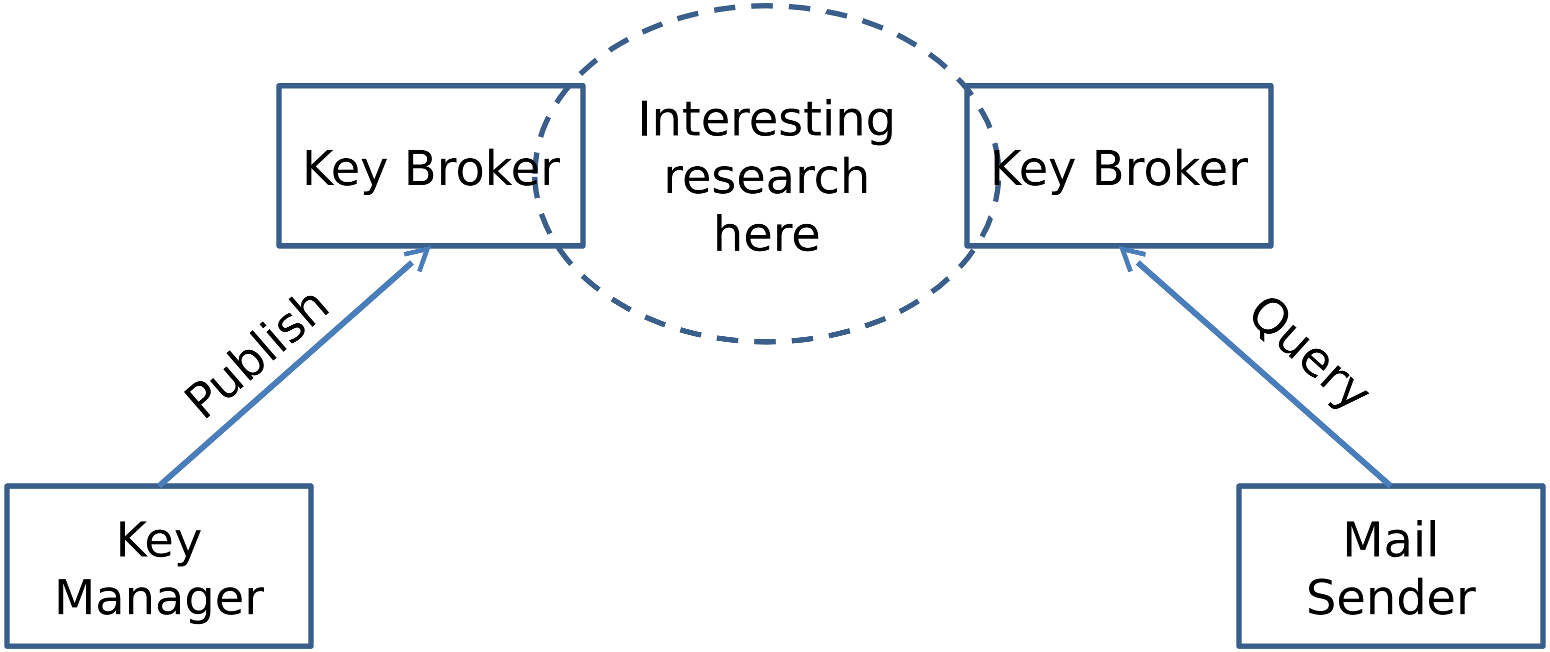
Flood fill

Key Management

- Solved but badly
  - Publication
  - Discovery

- Unsolved
  - Manage decryption keys with multiple devices
  - Key recovery for non-enterprise applications

Plumbing Requirements



http://prismproof.org/

Trust Model Requirement

- Hypotheses
  - “Trust model X is completely insecure”
  - “Trust model Y is better than Z”
  - How do we empirically determine which is true?
    - How hard is it for an attacker?

New Opportunities

Harber-Stornetta Patent Expiry

JSON

http://prismproof.org/