Trust Path Discovery

draft-ono-trust-path-discovery-01.txt

Kumiko Ono

Henning Schulzrinne

Motivation

- Protection against unsolicited bulk messages
  - An option for sender filtering
    - Determine whether to accept communication's requests, e.g., emails, calls, instant messages from a "stranger"
    - Based on reputation of that stranger
- How to get the stranger's reputation
  - Query a third-party reputation system

  or
  - Query trusted friends and their friends

Protection Mechanisms for Unsolicited Bulk Messages

- Anti-spam/spit/spim
  - Content-based filtering
  - Sender-based filtering: (assume anti-spoofing)

  e.g.
    - Third-party accreditation for servers
    - Trust Path Discovery for servers and individuals
  - Others

  e.g.,
    - Make sending bulk messages burdensome
- Anti-spoofing
  - For SMTP sender

  e.g.,
    - Sender ID
    - DomainKeys
  - For SIP originator

  e.g.,
    - SIP identity
    - SAML with SIP?

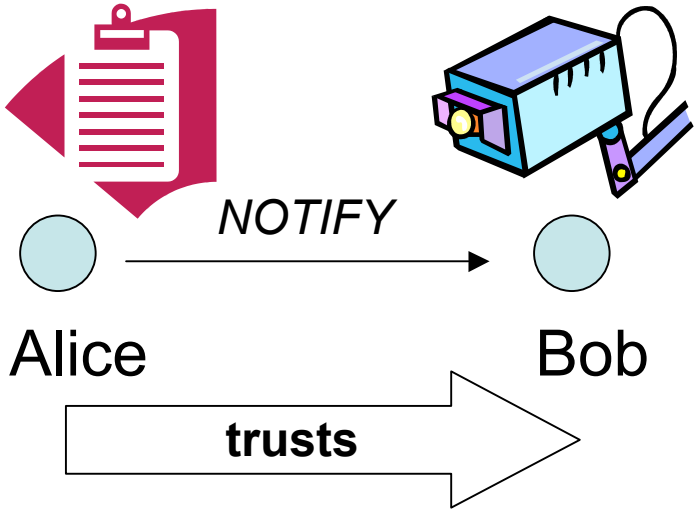
Our Approach

- Gathering trustworthy opinions on individuals and their domains from our friends or community
  - Opinions based on trust indicators which represent one's trust on receiving messages
  - Chains of trust relationships **= Trust paths**
    - Among individuals (users)
    - Among domains
    - Between a user and a domain

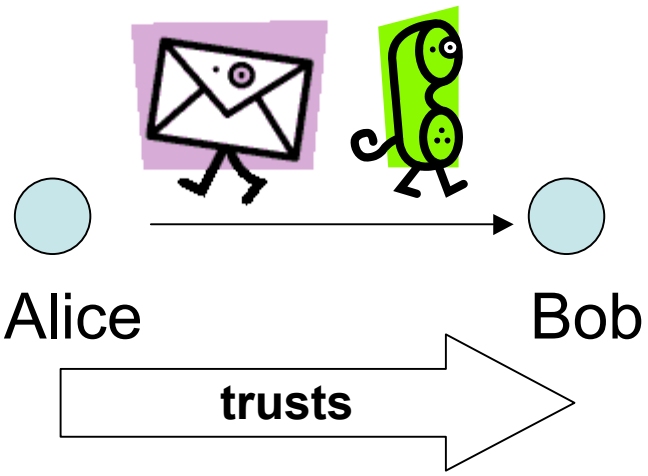
What are Trust Indicators?

- When Alice trusts Bob,

Bob is on Alice's watcher list (= subscribes to Alice)

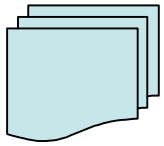


Log of sending email, call, or message



How to Gather “Trust paths”

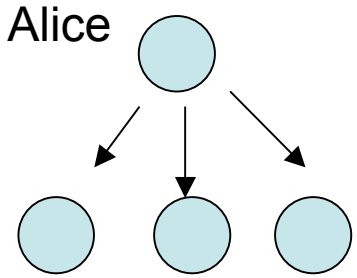
Trust indicators



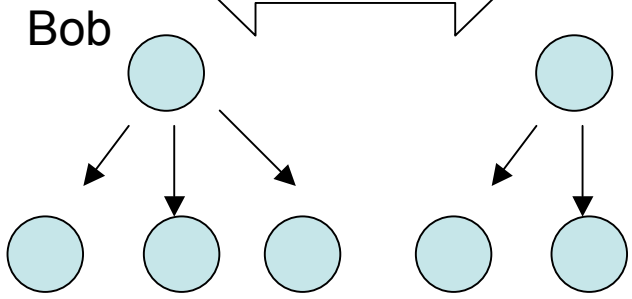
- Watcher list
- Log of sending mails
- Log of making calls

1. generate

Trust path (one-hop)

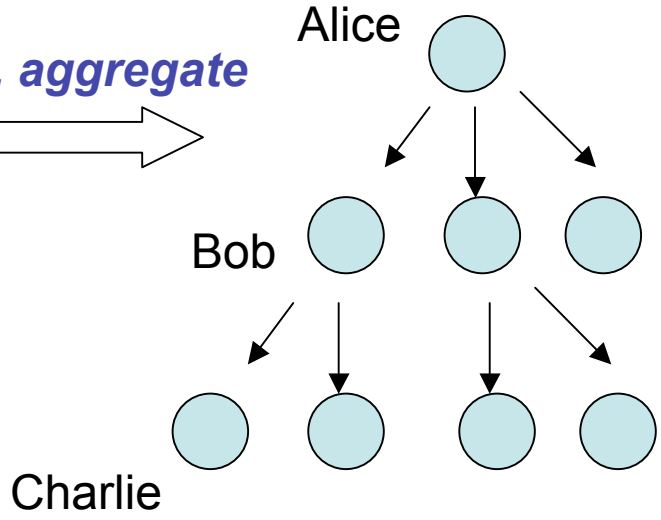


2. exchange



3. aggregate

Trust path (multi-hop)



How to Exchange "Trust paths"

- Push-based model: propagating trust paths in advance, e.g., at registration phase.
  - ϑ Responsive
  - Λ More need to disclose trust path. Privacy breach?
    - Trust-path can only contain public and semi-private information, because propagated trust path might be disclosed to third parties
- Query-based model: query trustworthiness when needed.
  - ϑ Less need to disclose trust paths
    - However, query itself is also privacy-sensitive
  - Λ Slower. Needs to query multiple servers/individuals
    - "Who trusts you?" "Who trusts Alice?"

Our proposal: Push-based model

Conclusion

- Current Status
  - Propagation mechanism
    - A new event package, “opinion”
    - SUBSCRIBE/NOTIFY/(PUBLISH)
  - Implementation in progress

Your feedback is welcome!

Related Work: Domain Name Accreditation

draft-ietf-marid-csv-dna-02.txt