Fighting spam with capability keys

Rob J Meijer

Overview

- Spam
- E-Mail addresses
- Mail Capability keys
- Delegation
- Accountability

Spam

- Unsolicitated bulk e-mail
- Mostly for marketing purposes
- Profitable for sender

Spam, the down side

- Over 100 billion spam messages every day.
- Doubles every 8 to 12 months
- Massive loss of productivity
- Loss of data
- Just plain annoying
- Is e-mail doomed?

E-Mail addresses

- Addresses like `alice@op.nu`
- Possession enables addressing peer
- Unrevocable
- forgeable

E-mail Capability keys

- Addresses like alice +3a66f0 @op.nu
- Non forgeable ?
  - key should be sufficiently long.
- Possession grants `capability` to address peer.
- Revocable

Delegation

- We can keep track of issued keys:
  - alice+3a66f0@op.nu : issued to Bob
  - alice+4d7fb1@op.nu : issued to Bob
- Introduction is delegation
  - Bob shares key alice+4d7fb1@op.nu with Carol.
  - Carol now has the capability to address Alice.
  - Bob should stop using this key
  - Bob should inform Alice using Cc.
- We can keep track of usage
  - alice+3a66f0@op.nu : issued to Bob
  - alice+4d7fb1@op.nu : issued to Bob
  - alice+4d7fb1@op.nu : Delegated Bob > Carol

An other spam message

```
From:  Sales <sales@cheapviagra.com>
To:  Allice <alice+4d7fb1@op.nu>
Subject:  Cheap Viagra
```

Accountability

- We can revoke the key, but who is accountable
- Spam appears to have come from `sales@cheapviagra.com`
- Alice knows key `alice+4d7fb1@op.nu` was issued to Bob
- Alice knows that the key was delegated to Carol
- Accountability is ambiguous, but scoped.

Removing Ambiguity

- Bob sends an introduction message:
  - To: alice+4d7fb1@op.nu
  - Cc: carol+904b1f@capibara.com
- Alice sends a new key to Carol
  - From: alice+dd73ff@op.nu
  - To: carol+904b1f@capibara.com
- Carol sends a new key to Alice
  - From: carol+c0fee4@capibara.com
  - To: alice+4d7fb1@op.nu
- Alice revokes her introduction key alice+4d7fb1@op.nu
- Carol revokes her introduction key

Removing Ambiguity (II)

- No Ambiguity
  - alice+3a66f0@op.nu : issued to Bob
  - alice+4d7fb1@op.nu : auto revoked
  - alice+dd73ff@op.nu : issued to Carol

Conclusion

- Adding password capabilities to e-mail addresses can countermeasure spam.
- Cc can be used to `share` accountability.
- With two step introductions and auto revocation, accountability becomes unambiguous.