Federal Trade Commission Email Authentication Summit

Douglas Otis

Senior Engineer

Research and Development

MAPS

November 8, 2004

maps

Agenda

- Why email authentication
- The need for security
- Who deserves the reputation
- Repairing SMTP with CSV
- Reducing abuse while avoiding risk

maps

Email Security Functions: Holding Someone Accountable

Term	*Function*
Identification	Who does this purport to be?
Authentication	Is it really them?
Authorization	What are they allowed to do?
Accreditation	Are they recognized?

maps

Key for Email Authentication

- It’s about security
- Reputation provides protection
- Security risks are greater with email
- CSV repairs SMTP and retains paradigms

maps

Mailbox-domain Reputation?

- What entity receives the reputation?
- Litigation required to ascertain negligence?
- Mailbox-domain reputation with exceptions?
- Which mailbox-domain has been assured?

maps

Reputation Model

- Name based reputation is needed
- Insurance industry structure analogy
- Ensuring reputation evaluates sources
- Identifying those able to respond

maps

CSV-CSA SRV Record

- _client._smtp.HELO-Domain
- TTL Class SRV (normal use)
- Priority : Version (1)
- Weight : 1 = Not Authorized, 2 = Authorized
- Target : Name w/addresses (Additional Data)

maps

Repairing SMTP

- DNS dropping of addresses permitted
- Client SMTP Validation (CSV)
- Establishing new expectations
- Asserting mail policies

maps

Mailbox-domain Path Registration

- **PTR Root-Name-List of HELO-domains (1 lookup)**
  my-mail-provider.com
  customer-support-outsourcing.com
  advertise-with-us.com

- **TXT Scripted Address-List of SMTP clients (1-100+ lookups)**
  spf2.0/mfrom,pra
  ip4:172.28.68.0/28
  include:customer-support-outsourcing.com
  a:customer123.advertise-with-us.com/28
  exists:%{ir}.%{d} … fubar:1234 ?all

maps

Avoiding Risk

- Poisoning exploits
- Hundreds of DNS lookups per message
- UDP overwhelms TCP
- UDP without exponential back-off
- Designed scale of DNS query/response

maps

Conclusion

- Worry about security
- Security must guide reputation assignment
- Repair HELO-domain authentication
- Avoid adding new security risks
- CSV retains the current email paradigms
- http://www.csvmail.org/

maps