

Client SMTP Validation

- <http://www/jlc.net/CSV>

SMTP Original Design Goals

- ◆ Simple to use
- ◆ Millions of email addresses
- ◆ Any user can email any other user
- ◆ No prior arrangements needed
- ◆ No cost barrier

The Problem

- ◆ SMTP is too successful
 - ◆ Hundreds of millions of email addresses
 - ◆ Millions of users at a single domain
 - ◆ Overworked support staff at some domains
- ◆ Costs too low to discourage marginal uses
 - ◆ SPAM
- ◆ Users don't know what computer is doing
 - ◆ Viruses

The Problem CSV Tackles

- ◆ No trail of accountability
 - ◆ MTA can claim to represent any domain
 - ◆ That domain neither confirms nor denies it
 - ◆ MTA IP address not controlled by domain
 - ◆ The authority assigning it disclaims responsibility

CSV Design Goals

1. Produce a Trail of Accountability
 - ◆ Authenticate MTA by domain name
 - ◆ Document the authorization by the domain
2. Design Scalable Accreditation System
3. Standardize Process to Query Accreditation
4. Minimize Costs to Receiving SMTP Server

Trail of Accountability

- ◆ Authenticate MTA by domain name
 - ◆ Start with IP Address
 - ◆ Use HELO string
 - ◆ Authenticate by DNS Address query
 - ◆ IP match proves domain assigned the name
- ◆ Document the authorization by the domain
 - ◆ DNS SRV query returns authorization info

Design Scalable Accreditation

- ◆ Millions of domains
- ◆ Hundreds of accreditation services
- ◆ How do they keep up with each other?
 - ◆ Sender recommends several which directly rate it
 - ◆ Receiver queries any it trusts
 - ◆ Direct-rating services publish in standard format
 - ◆ Any rating service can query these records

Standard Accreditation Query

- ◆ Limited-purpose
 - ◆ Intended for “friendly” use
 - ◆ Services are “suggested” by domain being rated
 - ◆ Domains prefer services that rate them favorably
 - ◆ Rating services must consider their own reputation
 - ◆ Must down-rate domains that allow abuse
- ◆ Competing services must access ratings
 - ◆ Overall rating fully public
 - ◆ Limited access to additional information:
 - ◆ Length of time rated
 - ◆ Estimated email volume
 - ◆ etc.

Minimize Receiver Costs

- ◆ For each SMTP session, two DNS queries
 - ◆ type=SRV, returns authorization (and authentication)
 - ◆ Responsiveness controlled by sender
 - ◆ type=TXT, Returns Accreditation
 - ◆ Responsiveness controlled by accreditation service
 - ◆ Bandwidth and time costs can be strictly limited
 - ◆ Similar to costs of starting a TCP connection

Current Situation

- ◆ Receiving servers query multiple blacklists
- ◆ Whitelists use unauthenticated From addresses
- ◆ Post-processing (e.g. Bayesian) needed
- ◆ Still too much SPAM gets through
- ◆ SPAM reporting seems pointless

Situation with CSV

- ◆ Receiving servers query one service
- ◆ Whitelists of senders not needed
- ◆ No post-processing needed
- ◆ Strict limits possible on amount of SPAM
- ◆ SPAM reports produce quick results
 - ◆ Copy the accreditation service with each report

CSV Processing by Receiver

- ◆ Extract HELO domain-name
- ◆ Start two DNS queries
- ◆ Check SRV DNS response
 - ◆ “Authorized” bit
 - ◆ IP Address found in list
- ◆ Branch on accreditation response
 - ◆ Fully trustworthy – bypass further checking
 - ◆ Not trustworthy – reject before accepting DATA
 - ◆ In-the-middle – record response in header

DNS Publishing by Sender

- ◆ Authorization Record
 - ◆ “SRV 1 2 0 <domain-name>”
- ◆ Accreditation Records
 - ◆ “PTR <prefix><name><service>”

Direct Accreditation Services

- ◆ Publish DNS Record
 - ◆ e.g. “TXT marid,1,A”
- ◆ Free-with-boxtop for low-volume domains
 - ◆ Domain-Name registrars
 - ◆ Professional Societies
 - ◆ Alumni Associations
- ◆ Fee-based for bulk emailers
 - ◆ Expect <\$100 per million emails sent
 - ◆ Plus about \$10 per complaint

Indirect / Proxy Accreditation

- ◆ Query DNS for PTR records
- ◆ For each PTR
 - ◆ Lookup reputation of direct-accreditation service
 - ◆ Query DNS for SRV records
 - ◆ Accumulate with appropriate weightings
 - ◆ Adjust for other information sources
 - ◆ Return a single evaluation
- ◆ May be no-money-changing-hands shared service
- ◆ May be for-fee or for-trade service

Things CSV Won't Do

- ◆ No attempt to authenticate sender address
 - ◆ Abusive forgery should be limited by sending MTA domain's policies
- ◆ No checking of headers visible to end user
 - ◆ Future work item for the MARID working group

The MARID Working Group

- ◆ Created by the Internet Engineering Task Force
- ◆ MTA Authorization Records In DNS
- ◆ Two proposals currently being developed
 - ◆ CSV – considers HELO string
 - ◆ SPF – considers MAIL FROM
- ◆ Will be discussed at IETF August meeting
- ◆ Due to be submitted as Proposed Standard in late August

Recommendations

- ◆ Stay Tuned
 - ◆ Until specification is approved by Working Group, it's premature to advertise the DNS records
- ◆ When it becomes a standard:
 - ◆ Advertise the authorization DNS record
 - ◆ Start seeking ratings from direct-accreditation service (s), and advertising them in DNS
 - ◆ When convenient, enable CSV checking

Questions

- ◆ <http://www.jlc.net/MARID/CSV>
- ◆ Frequently Asked Questions
- ◆ Specification documents