Email Reputation

Thomas Pomroy
Information and Educational Technology
tepomroy@ucdavis.edu

UCDAVIS

What are we talking about here ?

Technology to help evaluate the authenticity of email

Components:

- DNS – mapping of domain names to IP addresses
- SPF – IP address based
- DKIM – Encryption Key based
- DMARC – Policy and reporting

SPF – Sender Policy Framework

What is SPF?

An anti-forgery technology for email

How does it work?

Organizations publish a list of computers which are authorized to send email “as” your domain configurable on a per-domain name basis

Why do third party vendors ask to have their servers added to our SPF record?

Inclusion in the SPF record for a domain (ucdavis.edu) in some cases helps third-party emails avoid being filtered as spam or fraudulent.

Why don’t we include <your favorite email marketing vendor>?

SPF – Sender Policy Framework

ucdavis.edu's SPF record:

v=spf1 ip4:209.92.124.51/32 ip4:209.92.124.151/32 ip4:198.17.84.4/32 ip4:198.17.84.15/32 ip4:128.120.0.0/16 ip4:169.237.0.0/16 ip4:152.79.0.0/16 **include**:spf.protection.outlook.com **include**:_spf.google.com ~all

The SPF record UC Davis people want:

v=spf1 ip4:128.120.0.0/16 ip4:169.237.0.0/16 ip4:152.79.0.0/16 ip4:209.92.124.51/32 ip4:209.92.124.151/32 ip4:198.17.84.4/32 ip4:198.17.84.15/32 **include**:spf.protection.outlook.com **include**:_spf.google.com **include**:amazonses.com **include**:infusionmail.com **include**:aspmx.pardot.com **include**:sendgrid.net include:ccsend.com **include**:e2ma.net **include**:servers.mcsv.net **include**:salesforce.com ~all

SPF – Sender Policy Framework

The problem:

When receiving email servers read SPF records they are limited to ten DNS lookups.

Each “include” statement is one or more DNS lookups.

ucdavis.edu’s SPF record: 7 DNS lookups

The SPF record UC Davis people want: 27 DNS lookups

SPF – Sender Policy Framework

The solution: replace “include” statements with IP addresses: **(3 lookups)**

ucdavis.edu v=spf1 ip4:13.111.0.0/22 ip4:13.111.53.0/24 ip4:13.111.54.0/24 ip4:23.103.128.0/19 ip4:23.103.191.0/24 ip4:23.103.198.0/23 ip4:23.103.200.0/21 ip4:23.103.208.0/21 ip4:40.92.0.0/14 ip4:40.107.0.0/16 ip4:50.31.32.0/19 ip4:54.153.58.128 ip4:54.240.0.0/18 ip4:64.4.22.64/26 ip4:64.233.160.0/19 ip4:65.55.88.0/24 ip4:65.55.169.0/24 ip4:66.102.0.0/20 ip4:66.179.68.0/26 ip4:66.179.102.0/25 ip4:66.179.147.160/27 ip4:66.249.80.0/20 ip4:70.166.189.64/29 include:spf1.ucdavis.edu ~all

spf1.ucdavis.edu v=spf1 ip4:70.166.203.176/28 ip4:72.14.192.0/18 ip4:74.125.0.0/16 ip4:94.245.120.64/26 ip4:104.47.0.0/17 ip4:108.177.8.0/21 ip4:108.177.96.0/19 ip4:128.120.0.0/16 ip4:128.136.37.0/24 ip4:134.170.140.0/24 ip4:136.147.135.0/24 ip4:136.147.176.0/24 ip4:136.147.182.0/24 ip4:139.60.0.0/22 ip4:148.105.8.0/21 ip4:152.79.0.0/16 ip4:157.55.234.0/24 ip4:157.56.110.0/23 ip4:157.56.112.0/24 ip4:167.89.0.0/17 ip4:168.245.0.0/17 ip4:169.237.0.0/16 ip4:172.217.0.0/19 include:spf2.ucdavis.edu ~all

spf2.ucdavis.edu v=spf1 ip4:172.217.32.0/20 ip4:172.217.128.0/19 ip4:172.217.160.0/20 ip4:172.217.192.0/19 ip4:173.194.0.0/16 ip4:192.254.112.0/20 ip4:198.2.128.0/18 ip4:198.17.84.4 ip4:198.17.84.15 ip4:198.21.0.0/21 ip4:198.37.144.0/20 ip4:198.245.81.0/24 ip4:199.122.123.188/30 ip4:199.122.123.192 ip4:199.127.232.0/22 ip4:199.255.192.0/22 ip4:205.201.128.0/20 ip4:207.46.51.64/26 ip4:207.46.100.0/24 ip4:207.46.163.0/24 ip4:208.75.120.0/22 ip4:208.76.24.0/22 include:spf3.ucdavis.edu ~all

spf3. ucdavis.edu v=spf1 ip4:208.117.48.0/20 ip4:209.85.128.0/17 ip4:209.92.124.51 ip4:209.92.124.151 ip4:213.199.154.0/24 ip4:213.199.180.128/26 ip4:216.32.180.0/23 ip4:216.58.192.0/19 ip4:216.239.32.0/19 ip6:2001:4860:4000::/36 ip6:2001:489a:2202::/48 ip6:2404:6800:4000::/36 ip6:2607:f8b0:4000::/36 ip6:2800:3f0:4000::/36 ip6:2a00:1450:4000::/36 ip6:2a01:111:f400::/48 ip6:2c0f:fb50:4000::/36 ~all

DKIM - Domain Keys Identified Mail

DKIM uses encryption keys to create and attach a signature to each email which can be verified be the recipient email server.

How is it set up?

A sending service creates a private encryption key and gives the client (in this case, us) a public key which we publish in DNS. Multiple keys can be configured for multiple services.

Why sign emails with DKIM?

DMARC - Domain-based Message Authentication, Reporting and Conformance

DMARC is used to evaluate the overall authenticity of an email using SPF and DKIM results

Passing either SPF or DKIM evaluation results in a “pass”

DMARC is configured with a “policy” to either:

- Take no action regardless
- Quarantine messages which fail both checks (suspected spam)
- Reject messages which fail both checks (drop the message)

Moving your organization to DMARC policy = Quarantine strengthens the reputation of your domain’s brand

How can I use this information?

IET will soon be moving to a new method of publishing our SPF record, allowing for many more third-party email sending services to be included

IET will be publishing DKIM keys for third-party email sending services as requested

A governance group of who will decide which vendors are accepted for use at UC Davis will decide what goes into the SPF record and has published DKIM keys. (forthcoming)

You can do all this in a custom subdomain right now if you can’t wait

Questions

Thomas Pomroy
Information and Educational Technology
tepomroy@ucdavis.edu

UCDAVIS