"A One Page Document About SPF, DKIM and DMARC and Email Domain Reputation" (DRAFT v0.1)

I. The Problem

As originally designed, any user can emit mail messages for any domain (as a trivial example, in most email clients (such as Thunderbird), users can self-specify their name and email address in their email client's preference panel). This vulnerability to untrustworthy ("spoofed") domains is routinely exploited by spammers and phishers to impersonate legitimate sending domains, particularly domains for things like banks, credit card companies, etc.

II. SPF ("Sender Permitted From")

SPF attempts to tackle the spoofing problem by allowing a domain to say, "Only the following systems are authorized to send mail from my domain..." For example, Comcast Corporation says (via a TXT record it publishes in the domain name system (DNS)) that corporate comcast.com email should only come from two IPs:

```
% host -t txt comcast.com
comcast.com descriptive text "v=spf1 ip4:69.241.43.119 ip4:76.96.32.253 ~all"
```

Of course, while Comcast can offer this guidance to Internet mail recipients, in order for that guidance to actually reduce the level of spoofed email, *receiving* sites need to check SPF records as part of their email filtering. Most popular mail transfer agents (such as Sendmail, Postfix, Exim, etc.) allow you to easily automatically do this.

That said, there are many subtle points to consider if you're thinking about deploying SPF to sign or filter mail; if interested in potentially doing so, we strongly urge you to consult http://www.openspf.org/ for more information.

III. DKIM ("Domain Keys Identified Email")

DKIM employs a different approach. DKIM allows a domain's mail servers to cryptographically sign a message, thereby showing that it is "accepting responsibility for that email while it is in transit." Like SPF, DKIM leverages the domain name system to share the required information, in this case, the cryptographic keys that are needed to validate the signature seen on a message. For example, if a message is DKIM signed with the header:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com;
 s=20120113; h=mime-version:date:message-id:subject:from:to:content-type;
 bh=fRlAwqIAlJ/o2drCurT/w7UKzZbFXXlelZusopC2rWg=;
 b=ar7awxbRv3L1YkcwrN+Goa61EPcbgkFPF7KF4XaKje45tORhDlCm/Kj41D4+3d0RpU [etc]
```

There will be a corresponding key in a TXT record that's at **20120113**._domainkey.**gmail.com** -- for example:

```
$ host -t txt 20120113._domainkey.gmail.com
;; Truncated, retrying in TCP mode.
20120113._domainkey.gmail.com descriptive text "k=rsa\;p=MIIBIjANBgkqhkiG9w0BAQEFAA [etc]
```

While this may appear complex, the mechanics of the cryptographic signing and verification are normally easily handled "in the background" by popular mail transfer agents, just as for SPF. See http://www.dkim.org/ for more.

IV. DMARC ("Domain Based Message Authentication, Reporting and Conformance")

DMARC is designed to fix some of the lingering issues that SPF and DKIM didn't fully address. For example, DMARC makes it possible for a domain owner to tell recipients that all mail from their domain MUST be DKIM signed, or it should be rejected. DMARC also provides a feedback mechanism allowing domain owners to ask for daily reports from mail recipients describing (in summary form) how the mail for their domain looked to them -- were there spoofed emails from SPF-disallowed addresses? Were there messages with bad DKIM signatures? See http://www.dmarc.org/ for more information about DMARC and what it can potentially do for your domain.