Advanced Mail

lctseng / Liang-Chi Tseng

Introduction

- SPAM vs. non-SPAM
  - Mail sent by spammer vs. non-spammer
- Problem of SPAM mail
  - Over 99% of E-mails are SPAM! Useless for mankind!
- SPAM detection?
  - Client-based detection
    - These methods actually are the spammer detection techniques.
    - Usually are cost-effective, which can easily reach over 95% accuracy with only few computational resources.
  - Content-based detection
    - These methods are the real spam detection techniques.
    - Usually are costly with less than 90% accuracy
      - Lots of training and computation spent on it.
  - Who is the winner? Client-based? Content-based? (or Spammer?)
  - Endless war between the administrators and spammers.

Overview

- The following techniques are some (new) tools for an administrator to fight with spammers:
  - Greylisting
    - A client-based method that can stop mails coming from some spamming programs.
  - SPF (Sender Policy Framework)
    - A client-based method to detect whether a client is authorized or not.
  - DKIM (DomainKey Identified Mail)
    - A content-based method to verify the source of a mail (with only few computation cost.)
    - Check a mail is modified or not

Greylisting (1)

- http://www.greylisting.org/
- Greylisting is a client-based method that can stop mails coming from some spamming programs.
- Behavior of different clients while receiving SMTP response codes

Response Codes	2xx	4xx	5xx
Normal MTA	Success	Retry later	Give-up
Most Spamming Programs	Success	Ignore and send another	Give-up

  - While spammers prefer to send mails to other recipients rather than keeping log and retrying later, MTAs have the responsibility of retring a deferred mail.

Greylisting (2)

- Idea of greylisting:
  - Taking use of 4xx SMTP response code to stop steps of spamming programs.
- Steps:
  - Pair (recipient, client-ip)
  - Reply a 4xx code for the first coming of every (recipient, client-ip) pair.
  - Allow retrial of this mail after a period of time (usually 5~20 mins).
    - Suitable waiting time will make the spamming programs giving up this mail.

Greylisting (3)

- Tool: mail/postgrey (port or pacakge)
  - A policy service of postfix.
  - Daemon-based, like amavisd
- Configuration
  - In /etc/rc.conf

```
postgrey_enable="YES"
```

  - service postgrey start
  - Run on TCP port 10023
  - In main.cf

```
smtpd_recipient_restrictions = permit_mynetworks,
                               permit_sasl_authenticated,
                               reject_unauth_destination,
                       check_policy_service inet:127.0.0.1:10023
```

  - Reload Postfix

Greylisting (4)

- When a mail is reject by postgrey, you can find it in /var/log/maillog

```
450 4.2.0 <lctseng@nasa.lctseng.nctucs.net>:
Recipient address rejected: Greylisted,
see http://postgrey.schweikert.ch/help/nasa.lctseng.nctucs.net.html
```

- Whitelist Configuration
  - /usr/local/etc/postfix/postgrey_whitelist_clients
  - /usr/local/etc/postfix/postgrey_whitelist_recipients

Sender Policy Framework (SPF)

- A client-based method to detect whether a client is authorized or not.
- http://www.openspf.org
- RFC 4408
- SPF in FreeBSD
  - mail/libspf, mail/libspf2

Sender Policy Framework (SPF) – Is following mail questionable?

```
Delivered-To: lctseng@gmail.com
Received: by 10.129.125.135 with SMTP id y129csp250129ywc;
        Wed, 9 Mar 2016 22:29:43 -0800 (PST)
X-Received: by 10.50.59.212 with SMTP id b20mr1774964igr.30.1457…
        Wed, 09 Mar 2016 22:29:43 -0800 (PST)
Return-Path: <lctseng@cs.nctu.edu.tw>
Received: from demo1.nasa.lctseng.nctucs.net ([140.113.168.238])
        by mx.google.com with ESMTP id yq7si2678395igb.103.2016…
        for <lctseng@gmail.com>;
        Wed, 09 Mar 2016 22:29:43 -0800 (PST)
Received: from localhost (localhost [127.0.0.1])
        by demo1.nasa.lctseng.nctucs.net (Postfix) with SMTP id 49ECB27B
        for <lctseng@gmail.com>; Thu, 10 Mar 2016 14:27:21 +0800 (CST)
Message-Id: <20160310062726.49ECB27B@demo1.nasa.lctseng.nctucs.net>
Date: Thu, 10 Mar 2016 14:27:21 +0800 (CST)
To: lctseng@gmail.com
From: lctseng@cs.nctu.edu.tw
Subject: SPF Test

SPF TEST
```

Sender Policy Framework (SPF) – SMTP trace

```
220 demo1.nasa.lctseng.nctucs.net ESMTP Postfix
HELO localhost
250 demo1.nasa.lctseng.nctucs.net
mail from: lctseng@cs.nctu.edu.tw
250 2.1.0 Ok
rcpt to: lctseng@gmail.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
To: lctseng@gmail.com
From: Liang-Chi Tseng <lctseng@cs.nctu.edu.tw>
Subject: SPF Test
Message-ID: <56E10EC9.8050705@cs.nctu.edu.tw>
Date: Thu, 10 Mar 2016 14:16:00 +0800

SPF TEST
.
250 2.0.0 Ok: queued as 2962327B
```

Sender Policy Framework (SPF) – With SPF detection

```
Delivered-To: lctseng@gmail.com
Received: by 10.129.125.135 with SMTP id y129csp250129ywc;
        Wed, 9 Mar 2016 22:29:43 -0800 (PST)
X-Received: by 10.50.59.212 with SMTP id b20mr1774964igr.30.1457…
        Wed, 09 Mar 2016 22:29:43 -0800 (PST)
Return-Path: <lctseng@cs.nctu.edu.tw>
Received: from demo1.nasa.lctseng.nctucs.net ([140.113.168.238])
        by mx.google.com with ESMTP id yq7si2678395igb.103.2016…
        for <lctseng@gmail.com>;
        Wed, 09 Mar 2016 22:29:43 -0800 (PST)
Received-SPF: softfail (google.com: domain of transitioning
lctseng@cs.nctu.edu.tw does not designate 140.113.168.238 as permitted
sender) client-ip=140.113.168.238;
Authentication-Results: mx.google.com;
       spf=softfail (google.com: domain of transitioning
lctseng@cs.nctu.edu.tw does not designate 140.113.168.238 as permitted
sender) smtp.mailfrom=lctseng@cs.nctu.edu.tw
Received: from localhost (localhost [127.0.0.1])
        by demo1.nasa.lctseng.nctucs.net (Postfix) with SMTP id 49ECB27B
        for <lctseng@gmail.com>; Thu, 10 Mar 2016 14:27:21 +0800 (CST)
Message-Id: <20160310062726.49ECB27B@demo1.nasa.lctseng.nctucs.net>
To: lctseng@gmail.com
From: lctseng@cs.nctu.edu.tw
…
```

Sender Policy Framework (SPF) – Other SPF Results

- Permitted

```
Received-SPF: pass (google.com: domain of
lctseng@nasa.lctseng.nctucs.net designates 140.113.168.238 as permitted
sender) client-ip=140.113.168.238;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of lctseng@nasa.lctseng.nctucs.net
designates 140.113.168.238 as permitted sender)
smtp.mailfrom=lctseng@nasa.lctseng.nctucs.net
```

- No SPF record found (neutral)
  - But with DNS A record

```
Received-SPF: neutral (google.com: 140.113.168.238 is neither permitted
nor denied by best guess record for domain of
lctseng@nasa.lctseng.nctucs.net) client-ip=140.113.168.238;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: 140.113.168.238 is neither permitted nor
denied by best guess record for domain of
lctseng@nasa.lctseng.nctucs.net)
smtp.mailfrom=lctseng@nasa.lctseng.nctucs.net
```

Sender Policy Framework (SPF) – The idea

- For a domain administrator, he can claim which mail server will be used in his environment.
  - Ex. For cs.nctu.edu.tw, {csmailer,csmailgate,csmail}.cs.nctu.edu.tw are the authorized mail servers.
    - Mails out from these servers are authorized mails (under control of administrator.)
    - Other mails might be forged and have higher probability to be SPAMs.
- SPF technique specifies all possible outgoing mail clients in the TXT record of DNS service to claim the authorized mail servers.

```
IN     TXT   "v=spf1 a mx ~all"
```

- When destination MTA receives a mail, it will check the client ip:
  - For a mail out from authorized servers, it should be safe.
  - For a mail out from unauthorized servers, it might be forged.

SPF Record Syntax – Mechanisms (1/2)

```
v=spf1 a mx ~all
```

- all
  - Always matches
  - Usually at the end of the SPF record
- ip4 **(NOT ipv4)**
  - ip4: <ip4-address>
  - ip4: <ip4-network>/<prefix-length>
- ip6 **(NOT ipv6)**
  - ip6:<ip6-address>
  - ip6:<ip6-network>/<prefix-length>
- a
  - a
  - a/<prefix-length>
  - a:<domain>
  - a:<domain>/<prefix-length>

The content of this page and following are from http://www.openspf.org/SPF_Record_Syntax

SPF Record Syntax – Mechanisms (2/2)

```
v=spf1 a mx ~all
```

- mx
  - mx
  - mx/<prefix-length>
  - mx:<domain>
  - mx:<domain>/<prefix-length>
- ptr
  - ptr
  - ptr:<domain>
- exists
  - exists:<domain>
- include
  - include:<domain>
  - Also lookup record from <domain>
  - Warning: If the domain does not have a valid SPF record, the result is a **permanent error**. Some mail receivers will *reject* based on a **PermError**.

SPF Record Syntax – Qualifiers & Evaluation

```
v=spf1 a mx ~all
```

- Qualifiers
  - \+ Pass (default qualifier)
  - – Fail
  - ~ SoftFail
  - ? Neutral
- Evaluation
  - Mechanisms are evaluated in order: (first match rule)
    - If a mechanism results in a hit, its qualifier value is used.
    - If no mechanism or modifier matches, the default result is "Neutral“
  - Ex.
    - "v=spf1 +a +mx -all"
    - "v=spf1 a mx -all"

cs.nctu.edu.tw

"v=spf1 a mx
a:csmailer.cs.nctu.edu.tw
a:csmailgate.cs.nctu.edu.tw
a:csmail.cs.nctu.edu.tw ~all"

SPF Record Syntax – Evaluation Results

Result	Explanation	Intended action
Pass	The SPF record designates the host to be allowed to send	Accept
Fail	The SPF record has designated the host as NOT being allowed to send	Reject
SoftFail	The SPF record has designated the host as NOT being allowed to send but is in transition	Accept but mark
Neutral	The SPF record specifies explicitly that nothing can be said about validity	Accept
None	The domain does not have an SPF record or the SPF record does not evaluate to a result	Accept
PermError	A permanent error has occurred (eg. Badly formatted SPF record)	Unspecified
TempError	A transient error has occurred	Accept or reject

SPF Record Syntax – Modifier

- redirect
  - redirect=<doamin>
  - When mail server is outside from my domain
  - The SPF record for domain replace the current record. The macro-expanded domain is also substituted for the current-domain in those look-ups.
- exp
  - exp=<doamin>
  - Explaination
  - If an SMTP receiver rejects a message, it can include an explanation. An SPF publisher can specify the explanation string that senders see. This way, an ISP can direct nonconforming users to a web page that provides further instructions about how to configure SASL.
  - The domain is expanded; a TXT lookup is performed. The result of the TXT query is then macro-expanded and shown to the sender. Other macros can be used to provide an customized explanation.

Sender Policy Framework (SPF) – Example for Forged Headers

- On lctseng
- Envelop From: lctseng@nasa.lctseng.nctucs.net
- Mail Headers
  - From: lctseng@cs.nctu.edu.tw Forged!
  - To: lctseng@gmail.com
- Related SPF Records:

cs.nctu.edu.tw	**nasa.lctseng.nasa.nctucs.net**
"v=spf1 a mx a:csmailer.cs.nctu.edu.tw a:csmailgate.cs.nctu.edu.tw a:csmail.cs.nctu.edu.tw ~all"	"v=spf1 a mx ~all"

Sender Policy Framework (SPF) – Example for Forged Headers

```
220 demo1.nasa.lctseng.nctucs.net ESMTP Postfix
HELO localhost
250 demo1.nasa.lctseng.nctucs.net
mail from: lctseng@nasa.lctseng.nctucs.net
250 2.1.0 Ok
rcpt to: lctseng@gmail.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
To: lctseng@gmail.com
From: Liang-Chi Tseng <lctseng@cs.nctu.edu.tw>
Subject: SPF Test
Message-ID: <56E10EEE.8050705@nasa.lctseng.nctucs.net>
Date: Thu, 10 Mar 2016 14:36:00 +0800

SPF TEST
.
250 2.0.0 Ok: queued as 2962327B
```

Pass!
Only check “Envelope from”
Only check last MTA’s IP

```
Received-SPF: pass (google.com: domain of
lctseng@nasa.lctseng.nctucs.net designates 140.113.168.238 as permitted
sender) client-ip=140.113.168.238;
```

SPF Record Syntax – Enable SPF Check in Postfix

- Install "postfix-policyd-spf-python"
- In main.cf

```
smtpd_recipient_restrictions =
        …
        reject_unauth_destination,
        check_policy_service unix:private/policyd-spf
        …
policyd-spf_time_limit = 3600
```

- In master.cf

```
policyd-spf  unix  -       n       n       -       0       spawn
        user=nobody argv=/usr/local/bin/policyd-spf
```

- Reload Postfix
- Result: mail from Gmail

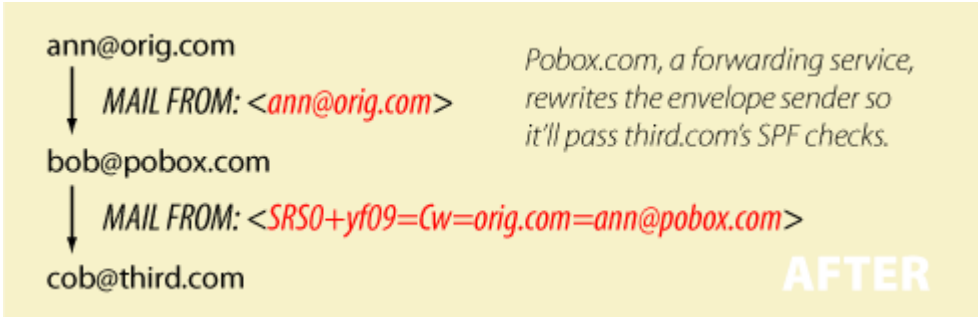
```
Received-SPF: pass (demo1.nasa.lctseng.nctucs.net:
 domain of gmail.com designates 209.85.161.182 as permitted sender)
client-ip=209.85.161.182; envelope-from=lctseng@gmail.com;
helo=mail-yw0-f182.google.com;
```

Sender Policy Framework (SPF) – SPF and Forwarding

- Does SPF break forwarding?
  - Yes, but only if the receiver checks SPF without understanding their mail receiving architecture.
  - Forwarders should apply Sender Rewriting Scheme (SRS) to rewrite the sender address after SPF checks.
    - If receivers are going to check SPF, they should whitelist forwarders that do not rewrite the sender address from SPF checks.

  [Ref] http://www.openspf.org/FAQ/Forwarding

- SRS: Sender Rewriting Scheme
  - http://www.openspf.org/SRS



Sender Policy Framework (SPF) – Forwarding Example

- On Gmail (lwhsu.tw's account)
  - Envelop From: lwhsu.tw@gmail.com
- Mail Headers
  - From: lwhsu@cs.nctu.edu.tw
  - To: lwhsu@lwhsu.org
- On knight.lwhsu.org (lwhsu.org's mx)
  - ~lwhsu/.forward:

    liwenhsu@gmail.com
- Flow:
  - lwhsu.tw@gmail.com → lwhsu@knight.lwhsu.org → liwenhsu@gmail.com

```
Delivered-To: liwenhsu@gmail.com
Received: by 10.229.81.4 with SMTP id v4cs221969qck;
        Sun, 10 May 2009 11:09:26 -0700 (PDT)
Received: by 10.216.2.84 with SMTP id 62mr2907141wee.217.1241978964147;
        Sun, 10 May 2009 11:09:24 -0700 (PDT)
Return-Path: <lwhsu.tw@gmail.com>
Received: from knight.lwhsu.ckefgisc.org (lwhsusvr.cs.nctu.edu.tw [140.113.24.67])
        by mx.google.com with ESMTP id 24si6143118eyx.13.2009.05.10.11.09.22;
        Sun, 10 May 2009 11:09:23 -0700 (PDT)
Received-SPF: neutral (google.com: 140.113.24.67 is neither permitted nor denied by domain
        of lwhsu.tw@gmail.com) client-ip=140.113.24.67;
Authentication-Results: mx.google.com; spf=neutral (google.com: 140.113.24.67 is neither
        permitted nor denied by domain of lwhsu.tw@gmail.com)
        smtp.mail=lwhsu.tw@gmail.com;
Received: by knight.lwhsu.ckefgisc.org (Postfix)
        id 47F571143E; Mon, 11 May 2009 02:09:21 +0800 (CST)
Delivered-To: lwhsu@lwhsu.org
Received: from an-out-0708.google.com (an-out-0708.google.com [209.85.132.243])
        by knight.lwhsu.ckefgisc.org (Postfix) with ESMTP id D832B11431
        for <lwhsu@lwhsu.org>; Mon, 11 May 2009 02:09:20 +0800 (CST)
Received: by an-out-0708.google.com with SMTP id d14so1324869and.41
        for <lwhsu@lwhsu.org>; Sun, 10 May 2009 11:09:19 -0700 (PDT)
Sender: lwhsu.tw@gmail.com
Received: by 10.100.248.4 with SMTP id v4mr14373811anh.121.1241978954295; Sun,
        10 May 2009 11:09:14 -0700 (PDT)
Date: Mon, 11 May 2009 02:09:13 +0800
Message-ID: <ef417ae30905101109j5c7b27bcy70a5bcf6d58092ab@mail.gmail.com>
Subject: test SPF
From: Li-Wen Hsu <lwhsu@cs.nctu.edu.tw>
To: lwhsu@lwhsu.org
```

Sender Policy Framework (SPF) - Enable Sender Rewrite Scheme (1)

- Tool: mail/postsrsd
- Configuration
  - In main.cf

```
sender_canonical_maps = tcp:127.0.0.1:10001
sender_canonical_classes = envelope_sender
recipient_canonical_maps = tcp:127.0.0.1:10002
recipient_canonical_classes = envelope_recipient
```

  - In /etc/rc.conf

```
postsrsd_enable="YES"
```

- Enable service
  - servie postsrsd start
  - postfix reload

Sender Policy Framework (SPF) - Enable Sender Rewrite Scheme (2)

- Example:
  - lctseng@cs.nctu.edu.tw → lctseng@nasa.lctseng.nctucs.net →lctseng@gmail.com
  - Without SRS

```
Received-SPF: softfail (google.com: domain of transitioning
lctseng@cs.nctu.edu.tw does not designate 140.113.168.238 as permitted
sender) client-ip=140.113.168.238;
```

  - With SRS

```
Received-SPF: pass (google.com: domain of
SRS0=o35H=PH=cs.nctu.edu.tw=lctseng@demo1.nasa.lctseng.nctucs.net
designates 140.113.168.238 as permitted sender) client-
ip=140.113.168.238;
```

Sender Policy Framework (SPF) – Some More Examples

```
$dig cs.nctu.edu.tw txt

;; ANSWER SECTION:
cs.nctu.edu.tw.        3600    IN      TXT     "v=spf1 a mx a:csmailer.cs.nctu.edu.tw
a:csmailgate.cs.nctu.edu.tw a:csmail.cs.nctu.edu.tw a:csmail1.cs.nctu.edu.tw
a:csmail2.cs.nctu.edu.tw a:www.cs.nctu.edu.tw a:csws1.cs.nctu.edu.tw
a:csws2.cs.nctu.edu.tw ~all"
```

List all authorized senders of cs.nctu.edu.tw

```
;; ANSWER SECTION:
csmx1.cs.nctu.edu.tw.   3600    IN      TXT     "v=spf1 a -all"
;; ANSWER SECTION:
csmx2.cs.nctu.edu.tw.   3600    IN      TXT     "v=spf1 a -all"
;; ANSWER SECTION:
csmx3.cs.nctu.edu.tw.   3600    IN      TXT     "v=spf1 a -all"
```

HELO addresses for CS MX servers

When a mail server sends a bounce message (returned mail), it uses a null MAIL FROM: <>, and a HELO address that's supposed to be its own name. SPF will still operate, but in "degraded mode" by using the HELO domain name instead. Because this wizard can't tell which name your mail server uses in its HELO command, it lists all possible names, so there may be multiple lines shown below. If you know which hostname your mail server uses in its HELO command, you should pick out the appropriate entries and ignore the rest.

Sender Policy Framework (SPF) – Backward Compatibility (1/2)

- When there is no SPF record, guess by A record.

```
Delivered-To: lwhsu.tw@gmail.com
Received: by 10.90.56.12 with SMTP id e12cs719147aga;
        Tue, 12 May 2009 00:49:39 -0700 (PDT)
Received: by 10.224.2.85 with SMTP id 21mr5508548qai.262.1242114578996;
        Tue, 12 May 2009 00:49:38 -0700 (PDT)
Return-Path: <lwhsu@freebsd.cs.nctu.edu.tw>
Received: from FreeBSD.cs.nctu.edu.tw (FreeBSD.cs.nctu.edu.tw [140.113.17.209])
        by mx.google.com with ESMTP id 7si4128629qwf.35.2009.05.12.00.49.38;
        Tue, 12 May 2009 00:49:38 -0700 (PDT)
Received-SPF: pass (google.com: best guess record for domain of
        lwhsu@freebsd.cs.nctu.edu.tw designates 140.113.17.209 as permitted sender)
        client-ip=140.113.17.209;
Authentication-Results: mx.google.com; spf=pass (google.com: best guess record for
        domain of lwhsu@freebsd.cs.nctu.edu.tw designates 140.113.17.209 as permitted
        sender) smtp.mail=lwhsu@freebsd.cs.nctu.edu.tw
Received: by FreeBSD.cs.nctu.edu.tw (Postfix, from userid 1058)
        id 6D98E61DBC; Tue, 12 May 2009 15:49:37 +0800 (CST)
Date: Tue, 12 May 2009 15:49:37 +0800
From: Li-Wen Hsu <lwhsu@FreeBSD.org>
To: lwhsu.tw@gmail.com
Subject: test tw.freebsd.org SPF
```

Sender Policy Framework (SPF) – Backward Compatibility (2/2)

- Comparative result – when SPF record available:

```
Delivered-To: lwhsu.tw@gmail.com
Received: by 10.90.56.12 with SMTP id e12cs719801aga;
        Tue, 12 May 2009 00:56:27 -0700 (PDT)
Received: by 10.224.74.84 with SMTP id t20mr5499756qaj.328.1242114987266;
        Tue, 12 May 2009 00:56:27 -0700 (PDT)
Return-Path: <lwhsu@freebsd.cs.nctu.edu.tw>
Received: from FreeBSD.cs.nctu.edu.tw (FreeBSD.cs.nctu.edu.tw [140.113.17.209])
        by mx.google.com with ESMTP id 5si4111810qwh.54.2009.05.12.00.56.26;
        Tue, 12 May 2009 00:56:27 -0700 (PDT)
Received-SPF: pass (google.com: domain of lwhsu@freebsd.cs.nctu.edu.tw
        designates 140.113.17.209 as permitted sender) client-ip=140.113.17.209;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of
        lwhsu@freebsd.cs.nctu.edu.tw designates 140.113.17.209 as permitted sender)
        smtp.mail=lwhsu@freebsd.cs.nctu.edu.tw
Received: by FreeBSD.cs.nctu.edu.tw (Postfix, from userid 1058)
        id 78CD461DB0; Tue, 12 May 2009 15:56:25 +0800 (CST)
Date: Tue, 12 May 2009 15:56:25 +0800
From: Li-Wen Hsu <lwhsu@FreeBSD.org>
To: lwhsu.tw@gmail.com
Subject: test tw.freebsd.org SPF (2)
```

Sender Policy Framework (SPF) – Example of include mechanism

- Gmail send mails for pixnet.net
  - But they still have dedicated mail servers (with IP 60.199.247.0/24)

```
knight:~ -lwhsu- dig pixnet.net txt

;; ANSWER SECTION:
pixnet.net.             86400   IN      TXT     "v=spf1
include:aspmx.googlemail.com ip4:60.199.247.0/24 ~all"
```

DomainKeys and DKIM

- A content-based method to verify the source of a mail (with only few computation cost.)
  - Allows an organization to claim responsibility for transmitting a message, in a way that can be validated by a recipient.
- Consortium spec
  - Derived from Yahoo DomainKeys and Cisco Identified Internet Mail
  - RFCs
    - RFC 4870 Domain-Based Email Authentication Using Public Keys Advertised in the DNS (DomainKeys)
    - RFC 4871 DomainKeys Identified Mail (DKIM) Signatures
- http://www.dkim.org/
  - http://www.dkim.org/info/DKIM-teaser.ppt

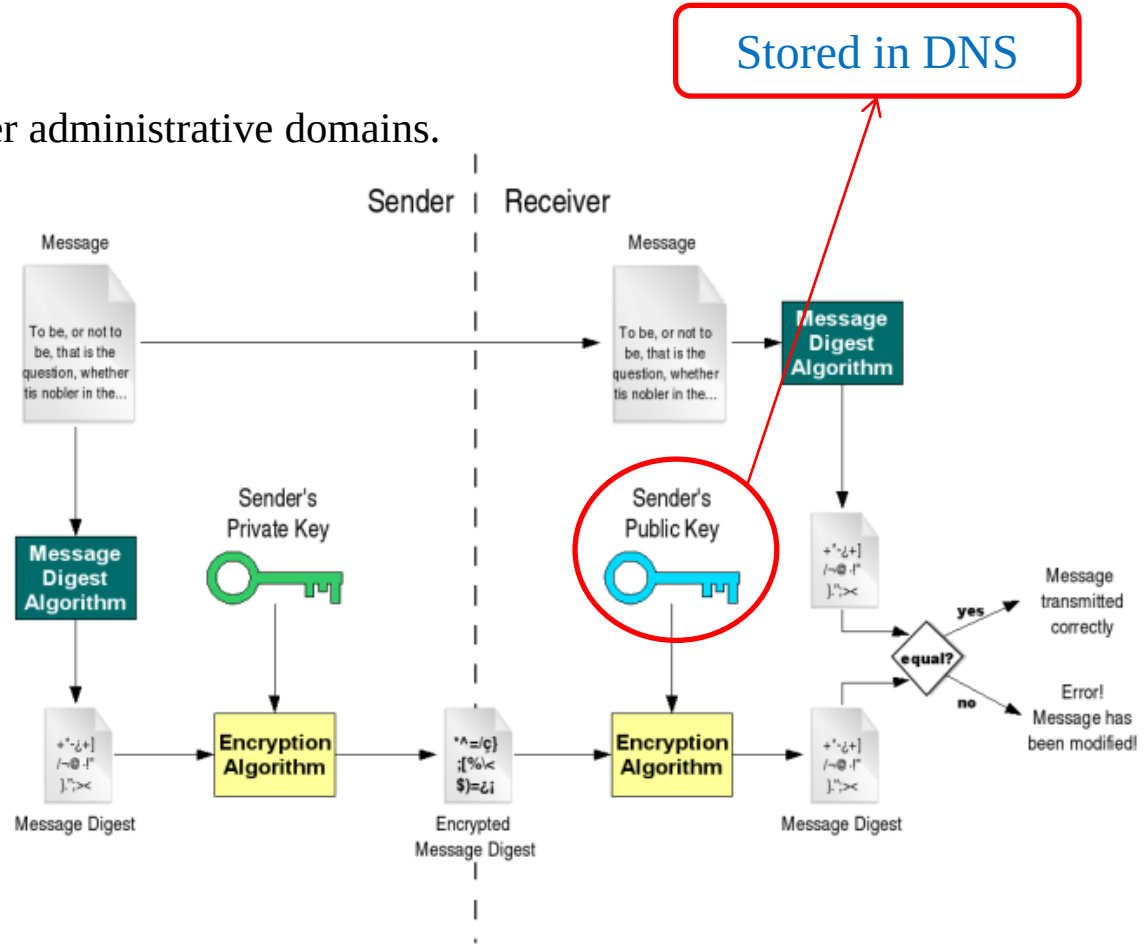
DKIM: Goals

- Validate message content, itself
  - Not related to path
- Transparent to end users
  - No client User Agent upgrades *required*
  - But extensible to per-user signing
- Allow sender delegation
  - Outsourcing
- Low development, deployment, use costs
  - Avoid large PKI, new Internet services
  - No trusted third parties (except DNS)

DKIM: Idea

- Msg header authentication
  - DNS identifiers
  - Public keys in DNS
- End-to-end
  - Between origin/receiver administrative domains.
  - Not path-based

※ Digital signatures



DKIM: Technical High-points

- Signs body and selected parts of header
- Signature transmitted in DKIM-Signature header
- Public key stored in DNS
  - In _domainkey subdomain
  - New RR type, fall back to TXT
- Namespace divided using selectors
  - Allows multiple keys for aging, delegation, etc.
- Sender Signing Policy lookup for unsigned or improperly signed mail

http://www.dkim.org/info/DKIM-teaser.ppt

DKIM-Signature header (1/4)

- `v=` Version
- `a=` Hash/signing algorithm
- `q=` Algorithm for getting public key
- `d=` Signing domain
- `i=` Signing identity
- `s=` Selector
- `c=` Canonicalization algorithm (simple or relaxed)
- `t=` Signing time (seconds since 1/1/1970)
- `x=` Expiration time
- `h=` List of headers included in signature; dkim-signature is implied
- `b=` The signature itself
- `bh=` Body hash

DKIM-Signature header (2/4)

- Example:

```
DKIM-Signature: a=rsa-sha1; q=dns;
  d=example.com;
  i=user@eng.example.com;
  s=jun2005.eng; c=relaxed/simple;
  t=1117574938; x=1118006938;
  h=from:to:subject:date;
  b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSb
    av+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

- DNS query will be made to:

```
jun2005.eng._domainkey.example.com
```

DKIM-Signature header (3/4)

- Example: Signature of Yahoo Mail

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=yahoo.com.tw; s=s1024; t=1242033944;
        bh=t3GnH+pN34KpMhlX59Eezm+9eCI68fU2hgid1Kscdrk=;
        h=Message-ID:X-YMail-OSG:Received:X-Mailer:Date:From:Subject:
        To:MIME-Version:Content-Type: Content-Transfer-Encoding;
        b=emLg4QonGbqb3PhZIEoYfiQVDYMwcBBB6SAEW+RziBEhjxKS2O
        UWmq5EpD1cxX+uz9MzJ4+fK4QRJZOtd0Y10c6Ce2J+V+C/RHnrjZ
        3PF8kAhjqvT1GTTdohxivLGrMftg1xFGO//M7ML/fcI4UJL+XP1xhJMB
        aHlHMGhE1sdGQ=
DomainKey-Signature: a=rsa-sha1; q=dns; c=nofws; s=s1024;
        d=yahoo.com.tw; h=Message-ID:X-YMail-OSG:Received:X-Mailer:
        Date:From:Subject:To:MIME-Version:Content-Type:Content-
        Transfer-Encoding;
        b=DlAhpuGID5ozcL77Ozm5doCQsxHSWaYHULW2hWAb3heXwewHga
        mqO+McEcSIplcB1JXTIBka7BR6HvbSPWX/XiMrVAjvb6zeRWiXSBWdt
        xIMpQhjJiBdzC8Y1BPCsdv2UwMgxOmR6i51BTIl+GDWFIKSgm5ky/
        zU+ZsdwIhlss=;
```

DKIM-Signature header (4/4)

- Example: Signature of Google Mail

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com;
        s=gamma; h=domainkey-signature:mime-version:date:message-id:
        subject:from:to:content-type;
        bh=o8h0LUwAIau52hau5ntEJaPU6qQn7rkIboJwbgnuNgc=;
        b=DxuMYeFtjXIt5eltj2MlzIXuOLA1y6f94+imgSKexX7EvhGMGUe82+4v
        78Vrpm5xmkNKp2xHsjvESpyWEAyt22ZKEV4OHClyqWPuabpwas0UD
        tV9KEwf9K663sCvrtoi9IpUQDPjP+aqC+po7tuLRiWfHYMETt5NpQfoWD
        pmoXw=
DomainKey-Signature: a=rsa-sha1; c=nofws; d=gmail.com; s=gamma;
        h=mime-version:date:message-id:subject:from:to:content-type;
        b=T2N/3v39iaiL3tWBKoZadVYr5BsotqTIKe7QL3oEy1e+2OiUCIbLGepx
        I7YXJ0Wt3MLx3ZcnkdNlGhrCWqXw7aV4gWw7GCsey2qZnakBTQ/BiH3
        TyrD3vdaDB8KJU0jC3Q4uE+Y2jQalXC60wsJtCByCpdXq0VVorgpLCJg4
        TnM=
```

DKIM – Set up your own DKIM (1)

- DKIM checking is already in your Postfix
- Now we want to add our own DKIM keys and records
- Tool: opendkim
  - mail/opendkim
  - Add pseudo user

```
pw useradd -n opendkim -d /var/db/opendkim -g mail -m
   -s "/usr/sbin/nologin" -w no
```

  - Enable daemon, in /etc/rc.conf

```
milteropendkim_enable="YES"
milteropendkim_uid="opendkim"
```

  - In main.cf

```
smtpd_milters = inet:127.0.0.1:8891
non_smtpd_milters = $smtpd_milters
milter_default_action = accept
```

DKIM – Set up your own DKIM (2) - OpenDKIM

❑ Configuration

- There is a sample file provided:
  - /usr/local/share/doc/opendkim/opendkim.conf.simple
- We provide a sample configuration here:
  - /usr/local/etc/opendkim.conf

```
LogWhy                  yes
Syslog                  yes
SyslogSuccess           yes

Canonicalization        relaxed/simple

Domain                  nasa.lctseng.nctucs.net
Selector                default
KeyFile                 /var/db/opendkim/default.private

Socket                  inet:8891@localhost

ReportAddress           postmaster@nasa.lctseng.nctucs.net
SendReports             yes
```

DKIM – Set up your own DKIM (3) - OpenDKIM

- Create keys and files

```
opendkim-genkey -D /var/db/opendkim -d
nasa.lctseng.nctucs.net -s default
```

- Under /var/db/opendkim
  - Private key: default.private
  - DNS record: default.txt
- Set up your DNS record using default.txt

```
default._domainkey      IN      TXT     ( "v=DKIM1; k=rsa; "

"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCiq1eJb+4Z3dXmCx6Ux+Qn
4oxj0CySkrPU3qm1fqi8FZaOsu64yfNr6ovr0gP4knzLltg527cQ2nxxAODEZXP
CaG4ujX9rKO1p/d7EMCqyqakJKyrJOSwWmI6ZIpEGj2ilviypEbe55/9xmoky/A
YTbJr6wVugKWDvywX7b9+APQIDAQAB" )  ; ----- DKIM key default for
nasa.lctseng.nctucs.net
```

- Start service & reload Postfix
  - service milter-opendkim start

DKIM – Set up your own DKIM (4) - Example

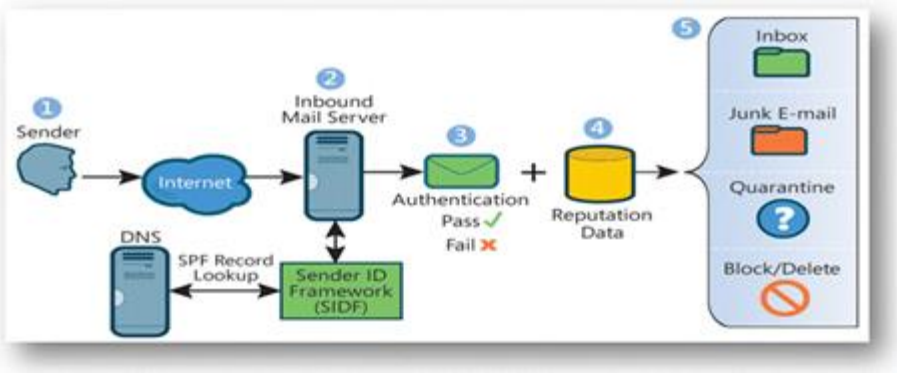
```
Received: from demo1.nasa.lctseng.nctucs.net ([140.113.168.238])
        by mx.google.com with ESMTP id
k14si3508069iok.92.2016.03.10.00.46.05
        for <lctseng@gmail.com>;
        Thu, 10 Mar 2016 00:46:06 -0800 (PST)
Received-SPF: pass (google.com: domain of lctseng@nasa.lctseng.nctucs.net
designates 140.113.168.238 as permitted sender) client-ip=140.113.168.238;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of lctseng@nasa.lctseng.nctucs.net
designates 140.113.168.238 as permitted sender)
smtp.mailfrom=lctseng@nasa.lctseng.nctucs.net;
       dkim=pass header.i=@nasa.lctseng.nctucs.net;
       dkim=pass header.i=@nasa.lctseng.nctucs.net
Received: from demo1.nasa.lctseng.nctucs.net (localhost [127.0.0.1])
        by localhost (Postfix) with ESMTP id AF1AF28C;
        Thu, 10 Mar 2016 16:44:40 +0800 (CST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple;
        d=nasa.lctseng.nctucs.net; s=default; t=1457599480;
        bh=q5cyARPl5zX/knmvCnEy11G7/r6gcljJ44qrvv5DErY=;
        h=To:From:Subject:Date;
        b=A9hItAg0uAU3Fj2UsQeNcdl8YisfX5O/qnp4KM210bMEw3u4acdRvx79ByOJ2fPiz
         //0VhBDRKn80NjpnJVNeAU7t9ChEi2RABbI7Kj1VDfs2b/OmJqdbs9G2jaCoellzvj
         hPUn8YvP4zPA8VFz+Hxph6czMEAozoM6YJP3s6mQ=
```

Appendix

Anything else? Of course!

Sender ID

- RFC4406, 4405, 4407, 4408
- Caller ID for E-mail + Sender Policy Framework (SPF 2.0)
- http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx



Sender ID – paypal.com example

```
knight:~ -lwhsu- dig paypal.com txt

;; ANSWER SECTION:
paypal.com.             3600    IN      TXT     "v=spf1 mx include:spf-
1.paypal.com include:p._spf.paypal.com include:p2._spf.paypal.com
include:s._spf.ebay.com include:m._spf.ebay.com include:c._spf.ebay.com
include:thirdparty.paypal.com ~all"
paypal.com.             3600    IN      TXT     "spf2.0/pra mx
include:s._sid.ebay.com include:m._sid.ebay.com include:p._sid.ebay.com
include:c._sid.ebay.com include:spf-2._sid.paypal.com
include:thirdparty._sid.paypal.com ~all"
```

Other MTA?

- qmail
- exim
- Sendmail X
  - http://www.sendmail.org/sm-X/
- MeTA1
  - http://www.meta1.org/