Anti-spam Technologies

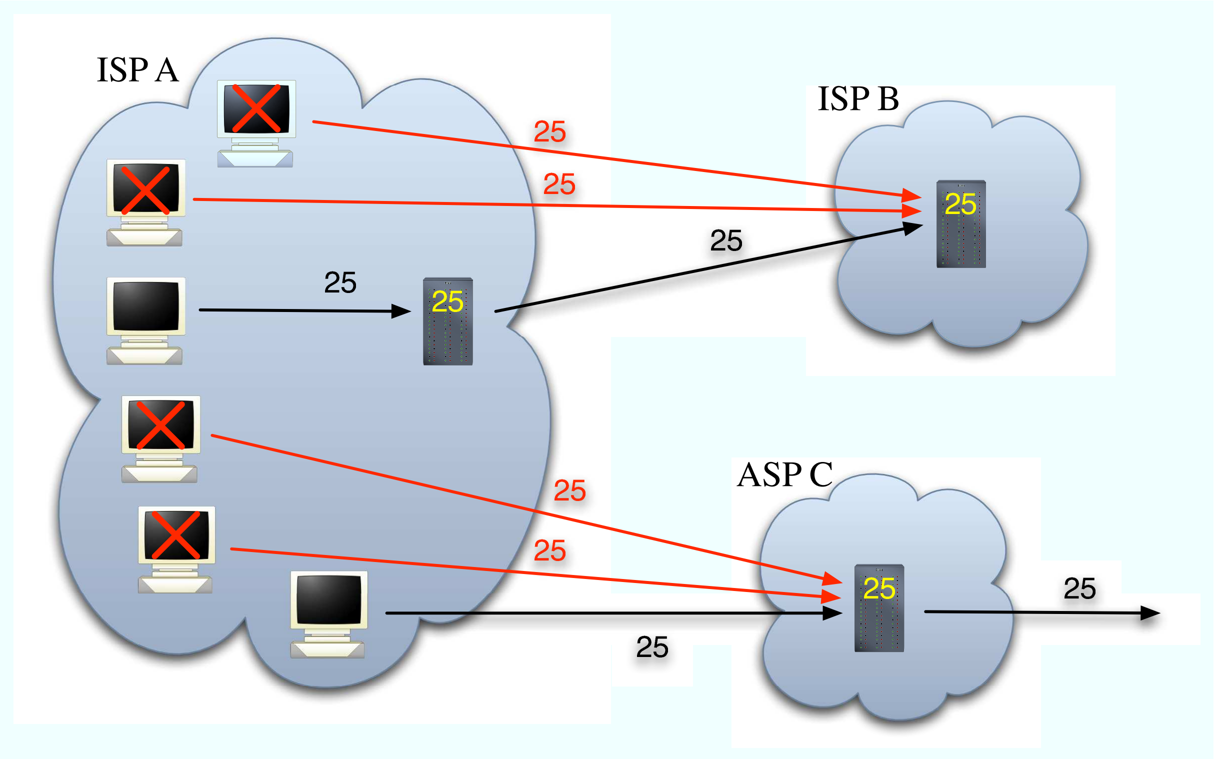
Kazu Yamamoto
Internet Initiative Japan Inc.
kazu@iij.ad.jp

Table of contents

- Problems on spams
- Solution scenario
- Submission port
- Domain authentication
- Problems on doman authentication
- Deploying SPF
- Summary

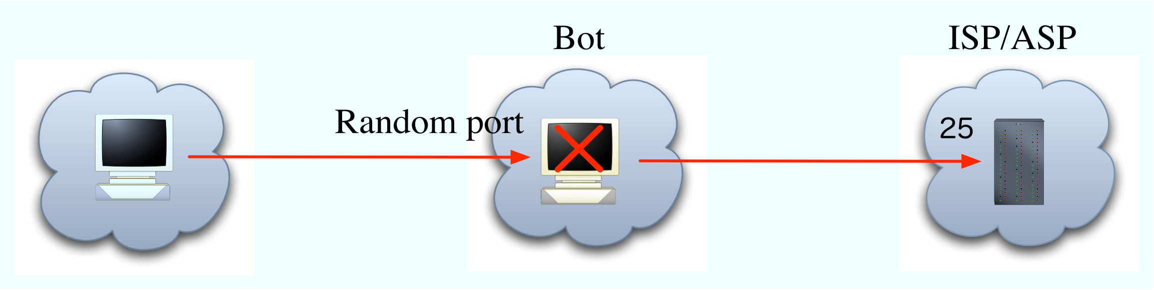
Problems on spams

Problems on spams



- Massive spams from botnet
- E-mail address can be faked
  - Cannot trace spammers
  - Phishing

How a BOT works?

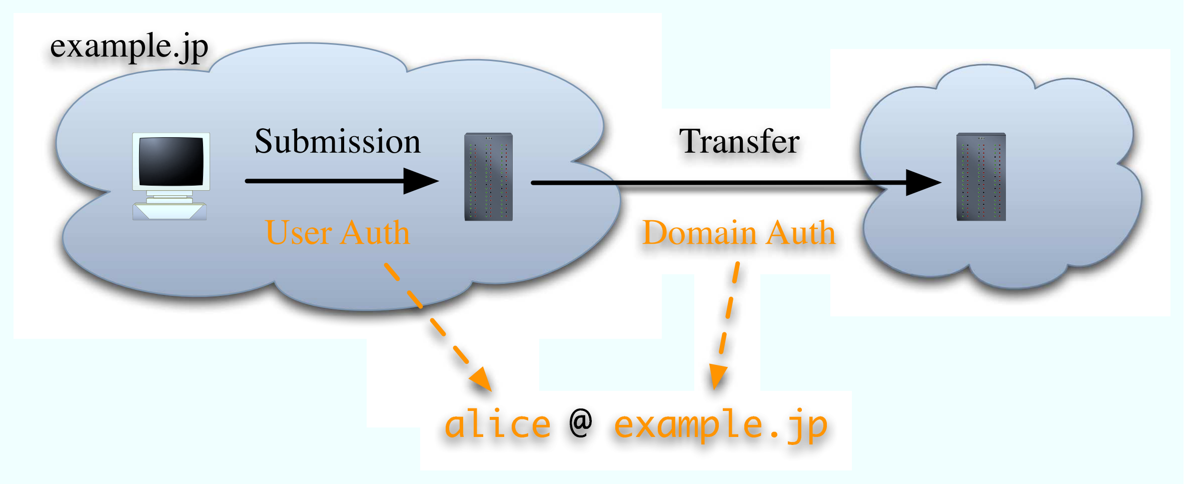


- BOT (a short term of "robot")
  - PCs get infected with viruses and viruses download BOT
    - If you connect vanilla Windows to the net with a global IP address, viruses transmit around 4 minutes
    - About 80 variations everyday
  - BOTs gain access to a controller PC and configure itself
  - Many sophisticated features
- SMTP relay
  - Relay a random port to port 25
  - For rent?
- It’s now business
  - BOTs try to hide themselves, do not destroy file system...

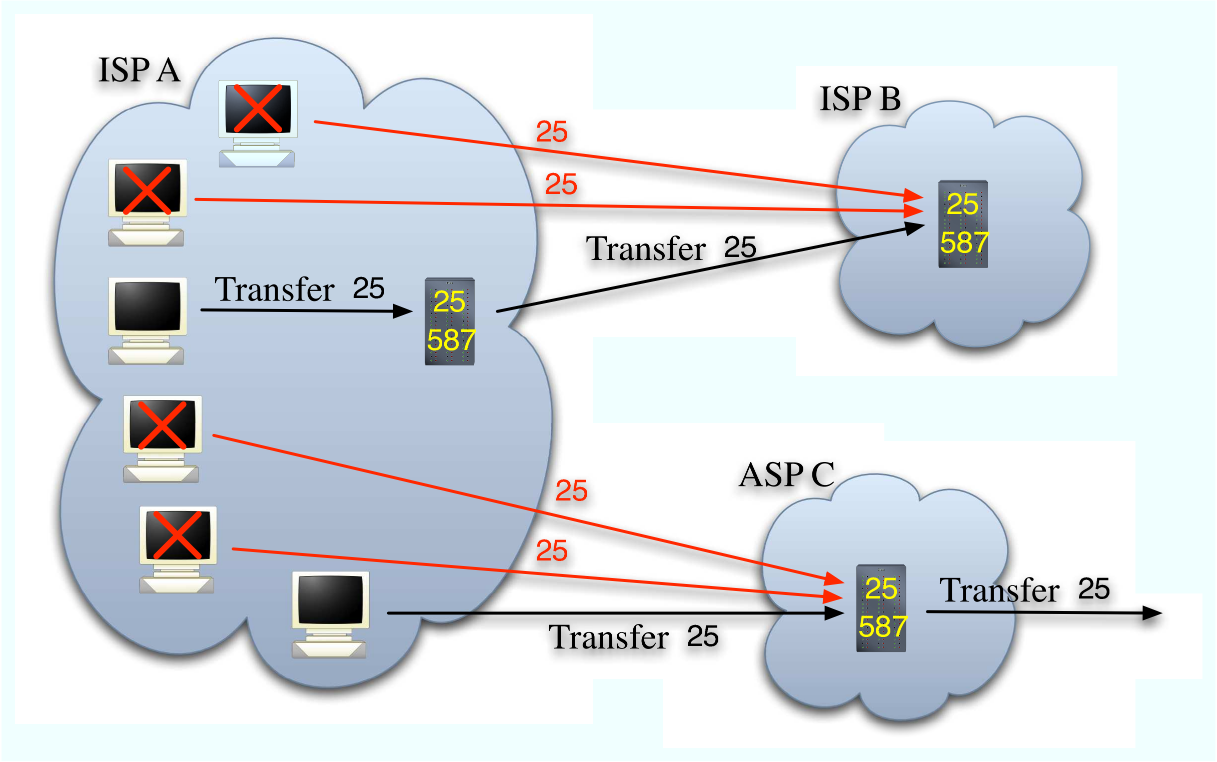
Solution scenario

Solutions

- Outbound port 25 blocking (OP25B)
  - Blocking spams from botnets
  - Separating to submission and transfer
- Two authentication methods
  - User authentication (SMTP AUTH)
  - Domain authentication (SPF + DKIM)
  - Preventing faking e-mail address

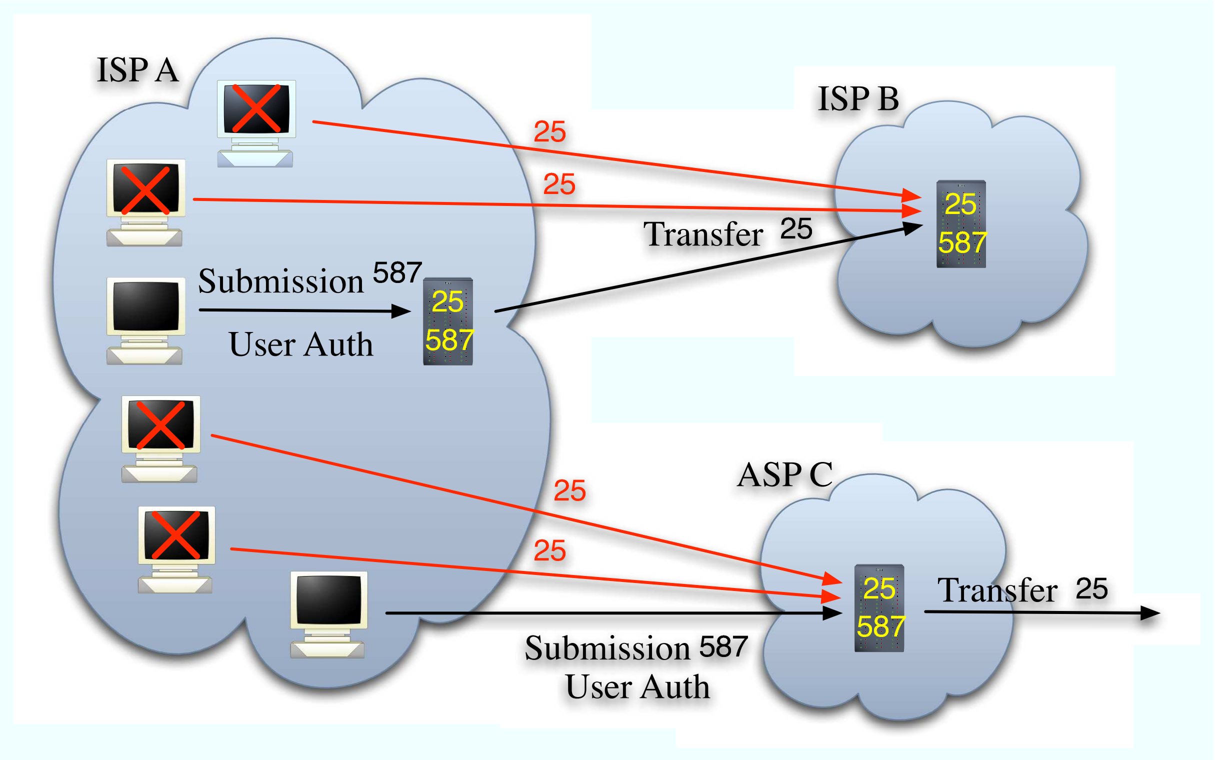


Preparing submission port



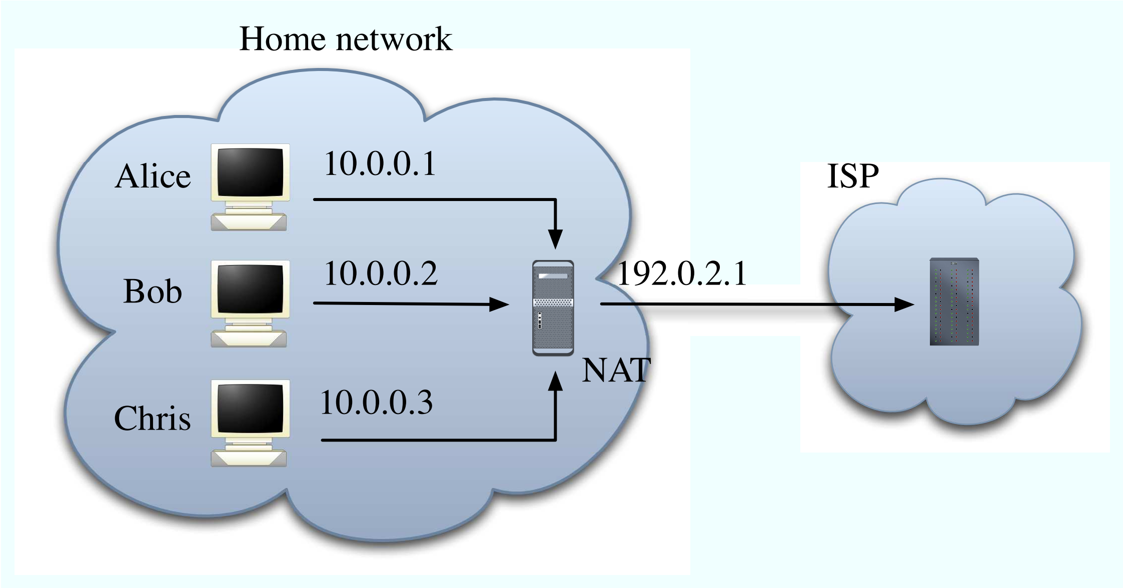
- Transfer = comm b/w servers (port 25)
- Submission
  = comm b/w mailreader and server (port 587)
  - The protocol is SMTP

Transition to submission port



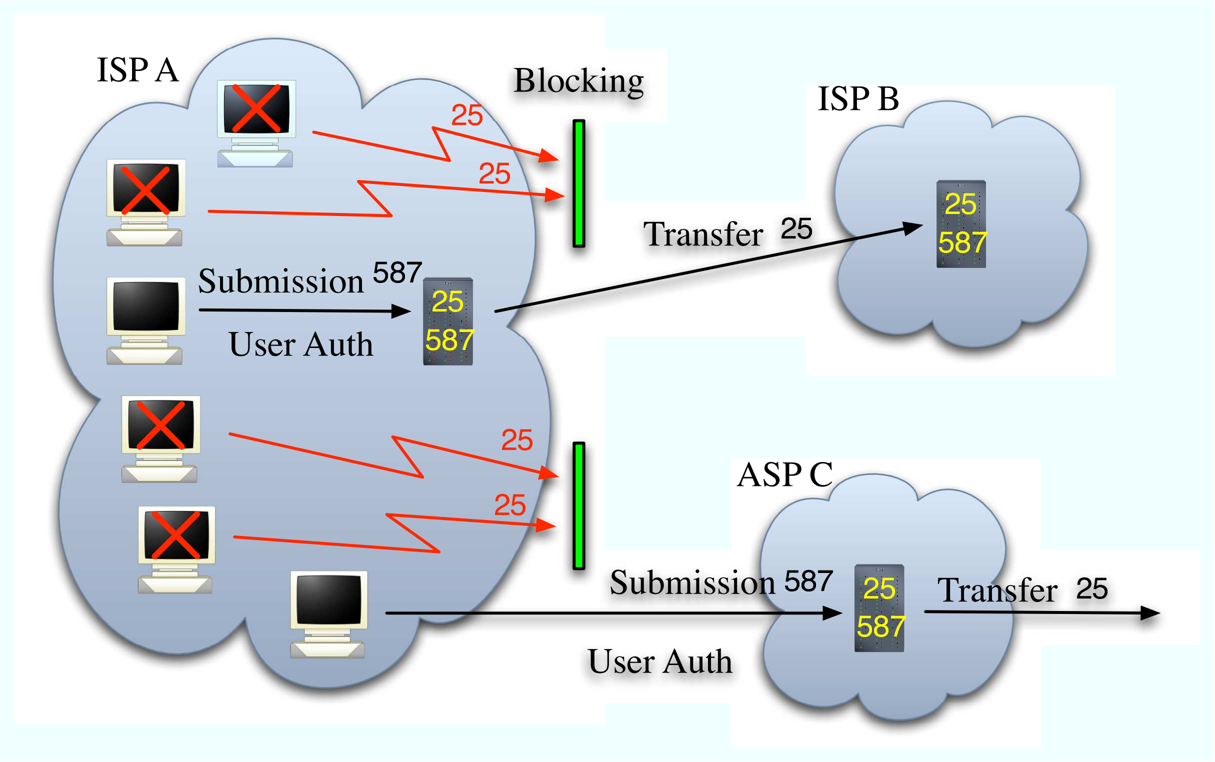
- Requiring SMTP AUTH for submission (port 587)
  - POP before SMTP is not good enough

POP before SMTP



- POP before SMTP authenticates IP addresses only
- It does NOT authenticate users
- It’s not alternative for SMTP AUTH

Outbound port 25 blocking

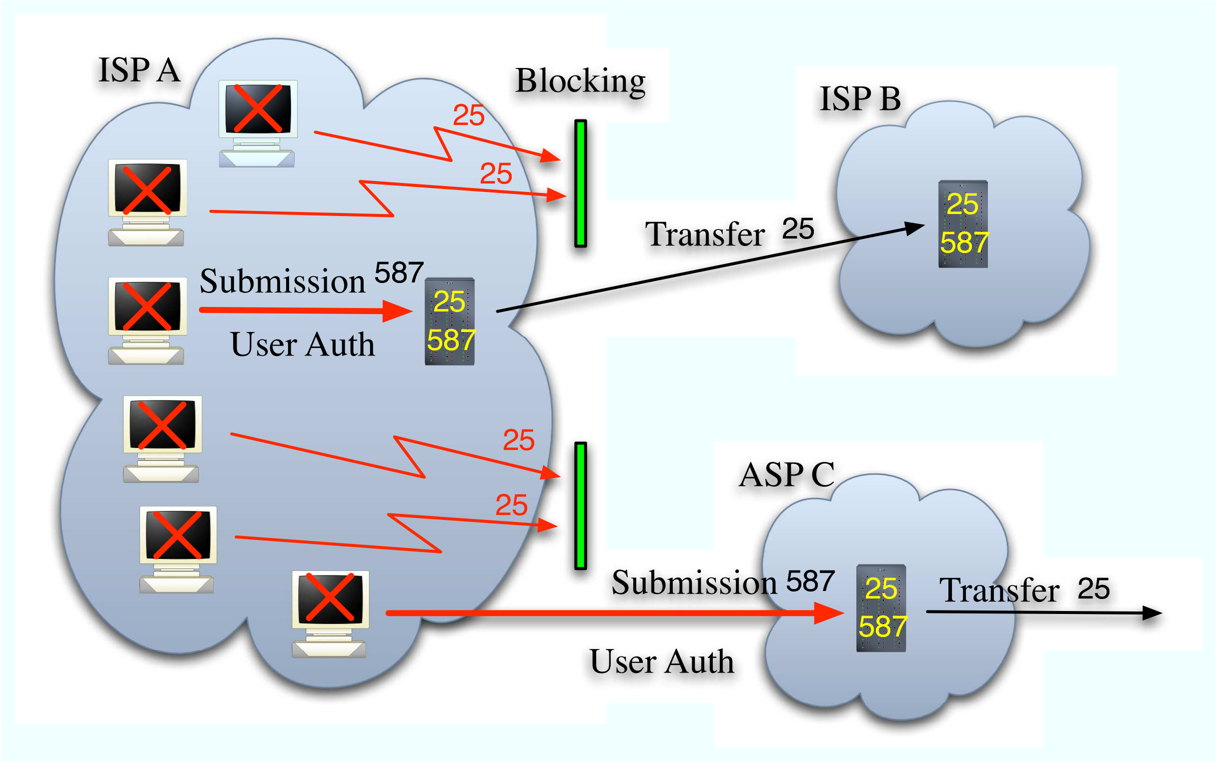


- ISPs in Japan start using OP25B only to hosts whose IP addresses are dynamic
- Those who want to operate mail servers in their home network should switch to fixed IP addresses

Deployment status of OP25B

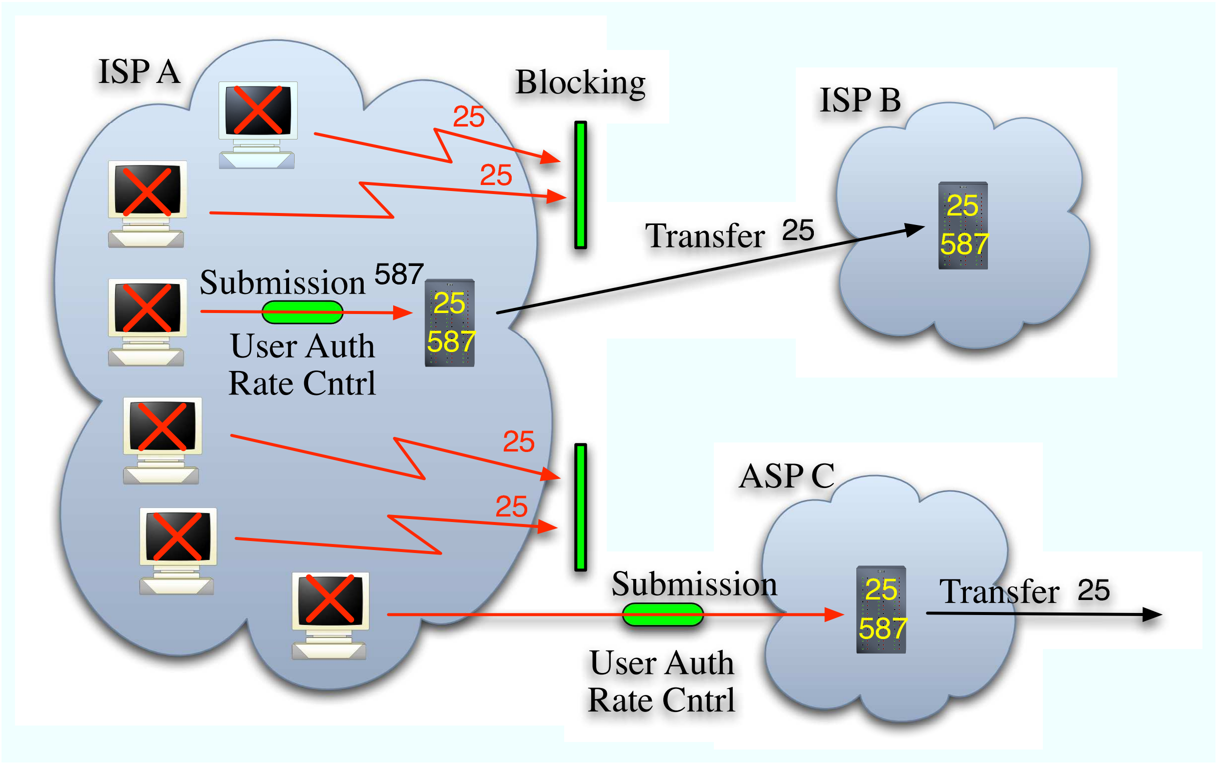
- Companies
  - Already deployed with firewall
- ISPs in America
  - AT&T, Bell CA, Bell South, Comcast,
  - Earthlink, MSN, Verizon,...
    - http://www.postcastserver.com/help/Port_25_Blocking.aspx
- ISPs in Japan
  - Described in the next session

New attacks



- BOTs will steal passwords
- Spammers will send spams with correct e-mail address

Rate control

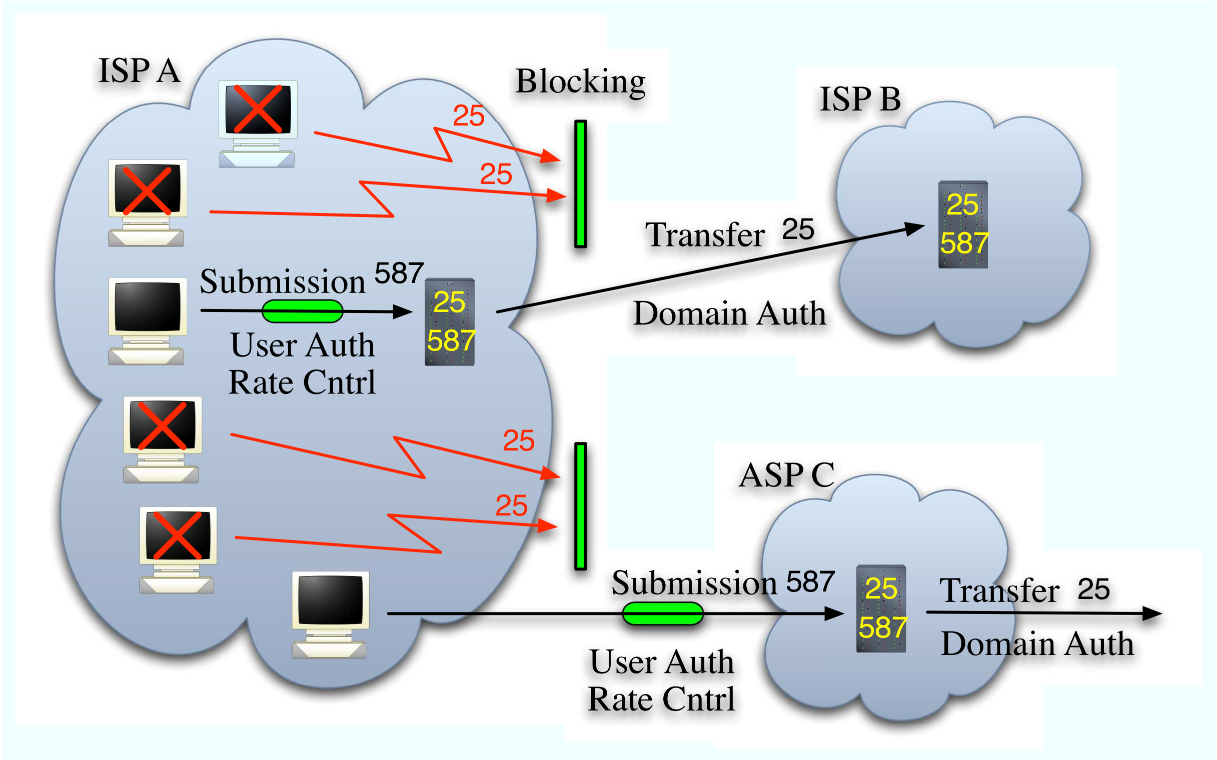


- Rate control is necessary for submission
  - Preventing massive spams in a short time

Rate control (2)

- Both directions
  - Inbound and outbound (submission)
- Limitations
  - Mail size
  - # of SMTP connections at the same time
  - # of SMTP connections from the same IP address
  - Frequency of SMTP connections from the same IP address
  - If a client causes user unknown, taking a longer time to accept the next connection from the client

Domain authentication



- Requiring domain authentication for transfer

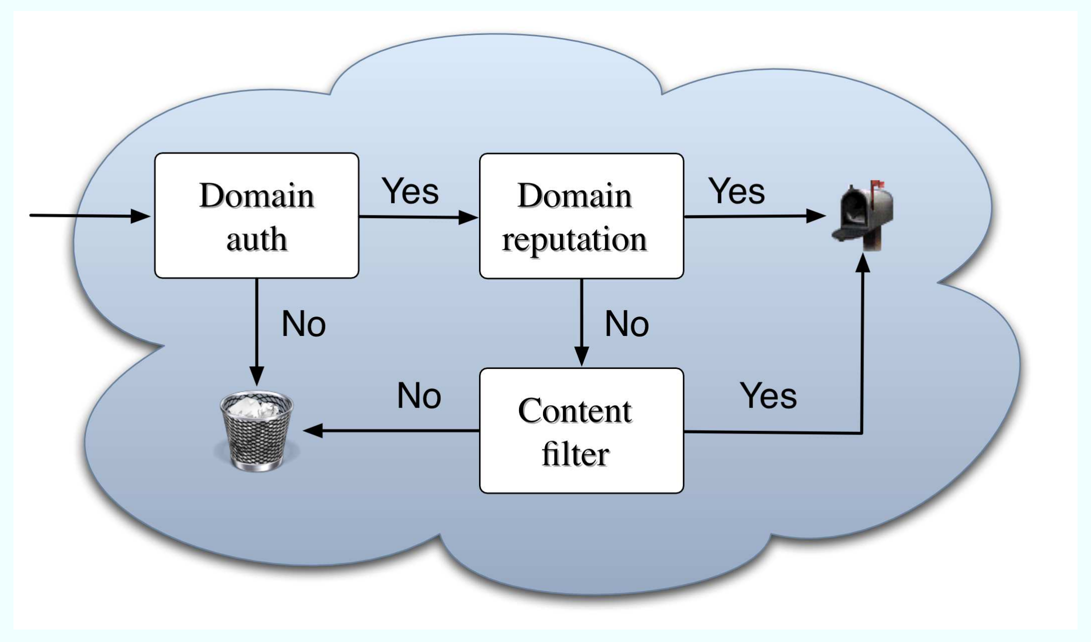
Domain reputation

- After e-mail messages are traceable
  - Spammers obtain their *daily* domain
  - They configure domain authentication
  - They send spams without address faking
- Reputation for domain is necessary
  - An example: cloudmark.com

```
% dig iij.ad.jp.rating.cloudmark.com txt
iij.ad.jp.rating.cloudmark.com.  1M IN TXT  "Status: Good"
iij.ad.jp.rating.cloudmark.com.  1M IN TXT  "Rating: 100"
```

Future image of ISP/ASP

- An example

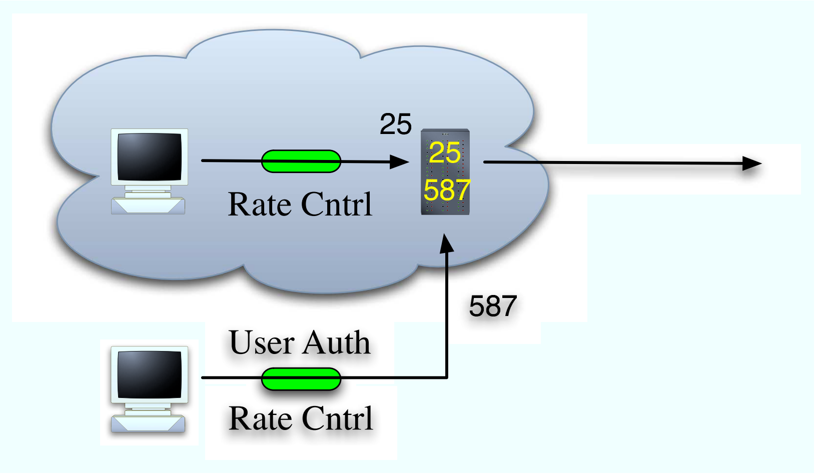


Submission port

Submission port

- Users have to configure their mailreaders
  - Webmails are not affected
- Ideal story
  - Providing submission port (587) and SMTP AUTH only
  - Preventing use of SMTP port (25) for submission purpose
- Status of mailreaders
  - Almost all mailreaders can use SMTP AUTH and change the port
  - Problem is mails from machinery
    - Report mails from programs
    - Mails from home appliance

Submission port (2)

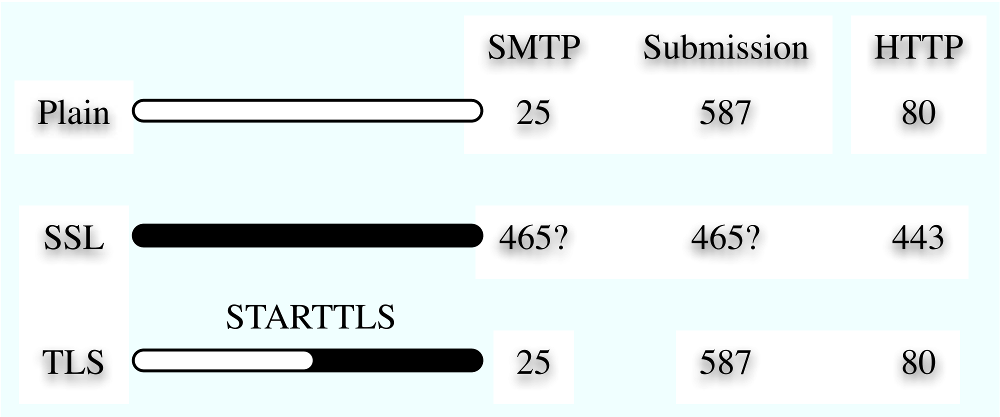


- Practical story
  - Allowing to use SMTP port (25) from the same domain
  - Allowing to use submission port (587) + SMTP AUTH only from the different domain
- Note
  - You may open submission port (587) without SMTP AUTH
  - Due to improper default of Sendmail

SMTP over SSL

- SMTP over SSL could be alternative
  - Many ISPes in Japan use port 465 for SMTP over SSL
  - Connections to port 465 get over OP25B
- Problems on SMTP over SSL
  - Port 465 used to be assigned to SMTP over SSL
  - Port 465 is now assigned to a protocol of Cisco
  - IETF will not assign a port to SMTP over SSL anymore
    - IETF promotes TLS, not SSL
    - Ports are assigned to POP over SSL and IMAP over SSL
    - It’s inconsistent but a reality

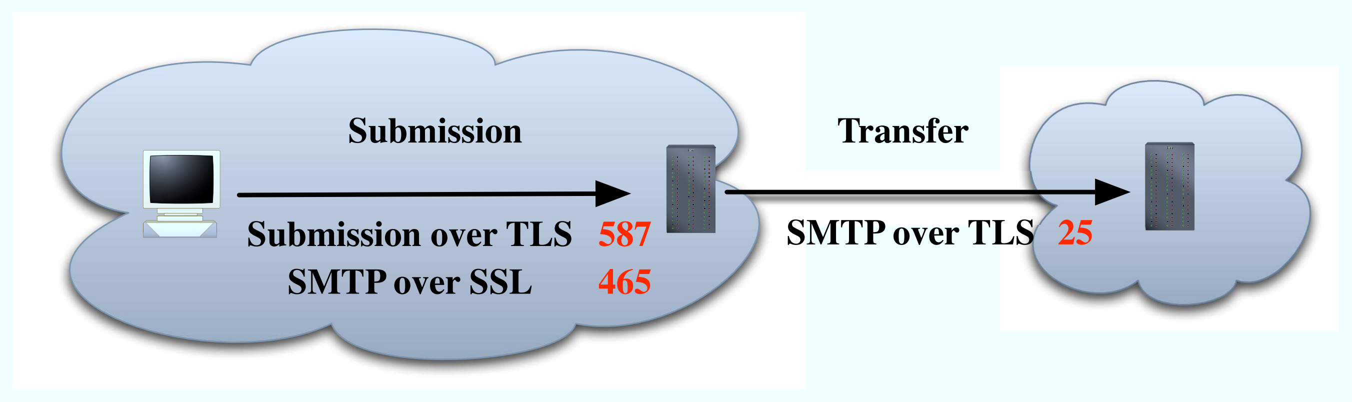
SSL and TLS



		SMTP	Submission	HTTP
Plain		25	587	80
SSL		465?	465?	443
TLS	STARTTLS	25	587	80

- SSL
  - No modification to SMTP
  - Another port is necessary
- TLS
  - Modification is necessary for SMTP
  - The same port

SMTP/submission over SSL/TLS



- Recommendations
  - Submission over TLS (port 587)
    - Best choice for submission
  - SMTP over SSL (port 465)
    - If you are using port 465 already, you don’t have to stop using it
  - SMTP over TLS (port 25)
    - If encryption is necessary for transfer

Outlook Express

- Port for submission
  - Default to 25
  - Can be set to 587
- SMTP AUTH
  - Raw passwords (SASL PLAIN/LOGIN) are supported
  - One time passwords (SASL CRAM-MD5) are NOT supported
- TLS over SSL
  - TLS is used if port is 25
  - Otherwise SSL is used
- You cannot protect your password
  - One time passwords are not supported
  - Submission over TLS (587) is not supported
  - SMTP over SSL (465) is supported
    but it's not IETF standard

Outlook Express (2)

- We have asked to improve OE several times, but MS does NOT

```
if (SSL) {
    if (port == 25) /* "|| port == 587" */
        TLS;
    else
        SSL; /* 465 is this case */
} else
    Plain SMTP;
```

- OE's receiving side is also vulnerable
  - One time password for POP (APOP) is NOT supported
- Why are you using OE?
  - Why don't you use Thunderbird, for instance?

Solutions to mailreaders

- Auto-configuration of Thunderbird
  - XML based "extension"
  - POP/IMAP/SMTP servers can be specified
  - Submission port, SMTP AUTH, TLS can also be configurable
  - ISP/ASPes can provide an XML package on their servers
  - Users download it
  - What users should do is just type name and account name
- Fallback from submission port to SMTP port
  - Submission port can be default with this technique
  - http://www.mew.org/~kazu/proj/submission/index.html.en

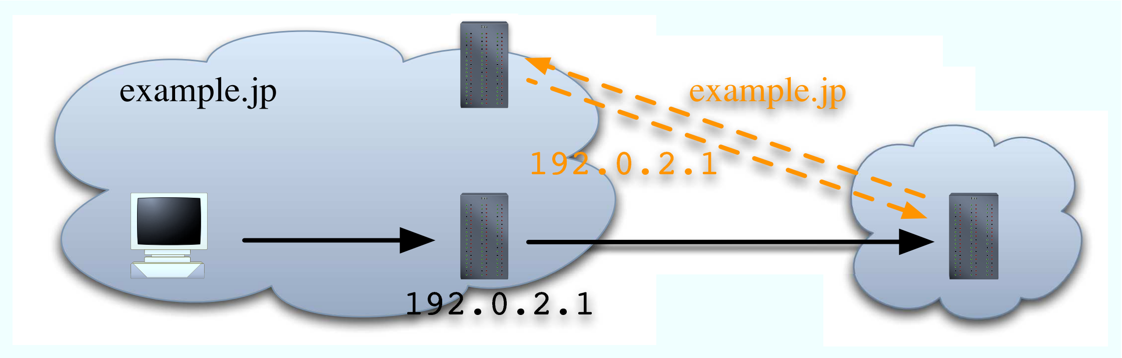
Domain authentication

Candidates of domain auth

- IP address base
  - SPF (Sender Policy Framework)
    - SMTP MAIL FROM (envelop information)
- Digital signature base
  - DKIM (DomainKeys Identified Mail)
    - Header (From:) + body
- They can co-exist
  - First, IP address base
  - Then, digital signature base
- DKIM is an anti-phishing technology
  - Protecting header

SPF mechanism

- Declaring sending servers (SPF RR, TXT RR)
  - example.jp IN TXT "v=spf1 +ip4:192.0.2.1 -all"
  - The IP address of the sending server is 192.0.2.1



- SPF verification in the receiver side

  1) Obtain the sender’s IP address from SMTP connection
  2) Extract domain name from SMTP MAIL FROM
  3) Look up DNS with the domain name and obtain IP addresses of sending servers
  4) Compare 1. and 3.

Declaring SPF RR

- Qualifier
  - "+" → pass
    - Accept receipt
- Qualifiers for "all"
  - "?" → neutral
    - Equivalent to *no* SPF RR
  - "~" → softfail
    - A level between neutral and fail
  - "-" → fail
    - Reject receipt
- Examples
  - example.jp IN TXT "v=spf1 +ip4:192.0.2.1 -all"
  - example.jp IN TXT "v=spf1 +a +mx ~all"
    - Indirect reference
  - example.jp IN TXT "v=spf1 -all"
    - Web only

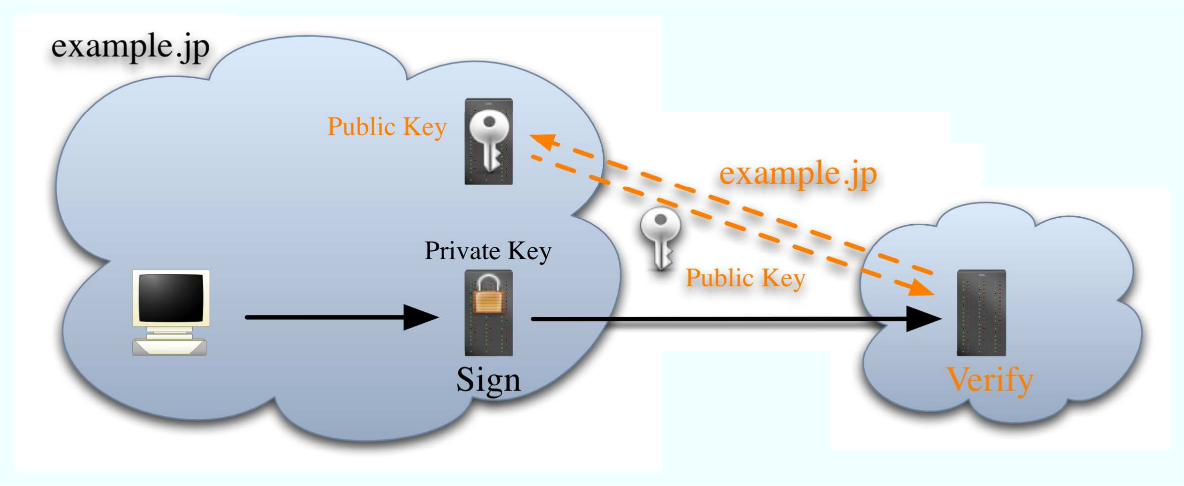
Signatures of DKIM

- Proposed by Yahoo! and Cisco
  - Two protocols have been merged
    - Yahoo! DomainKeys
    - Cisco Identified Internet Mail (IIM)
- Both header and body are signed
  - Signature is inserted to the header

```
DKIM-Signature: a=rsa-sha1; c=simple; d=example.jp; s=test;
  t=1137157317; x=1137762117; i=alice@example.jp; q=dns;
  h=DomainKey-Signature:Received:DKIM-Signature:
  DomainKey-Signature:Received:Message-ID:Date:From:Organization:
  User-Agent:MIME-Version:To:Subject:References:In-Reply-To:
  Content-Type:Content-Transfer-Encoding:Reply-To;
  b=ktdmQPIrkLGajBALhScj7I+Mx+h6uPBRxrcWm4pcW6bc8OwJTFdl9
  4LddNDq+iDGfT3m3Awe6j+Um2LIxpc0ET1dny0ut42H98I40C5QnjTo9
  8AahlUYkKeKXQZhTwU2PraJMBXFm8=
```

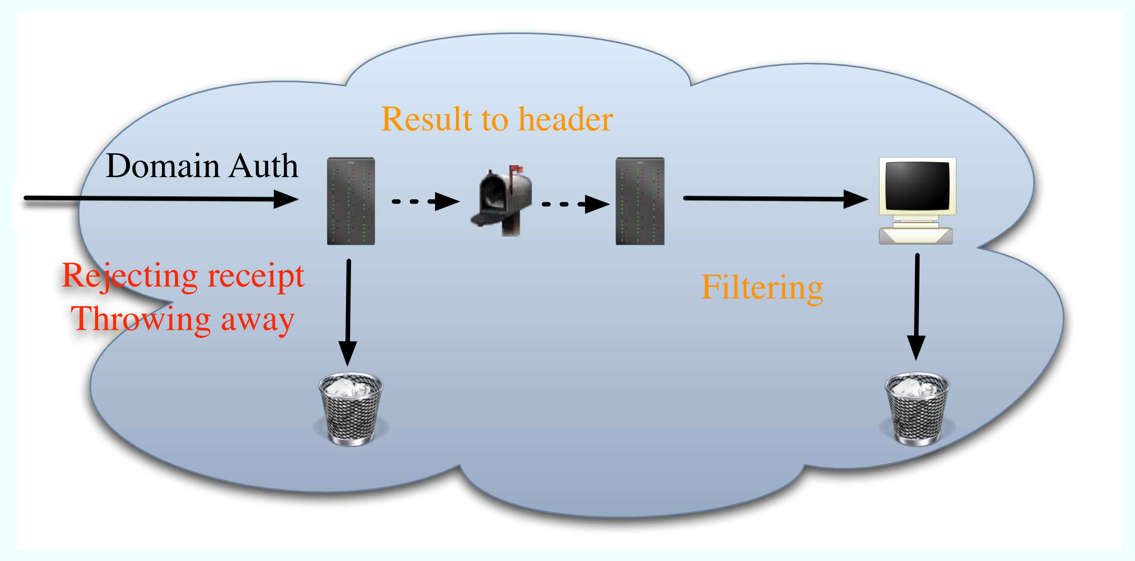
- Relies on DNS
  - Distributing public keys with DNS
  - No certificate authority (CA) is necessary

DKIM mechanism



- Sender side
  - Sign a mail with the private key
- Receiver side
  - Extract domain name from the signature
  - Look up DNS with the domain name and obtain the public key
  - Verify the signature

Transition to domain auth

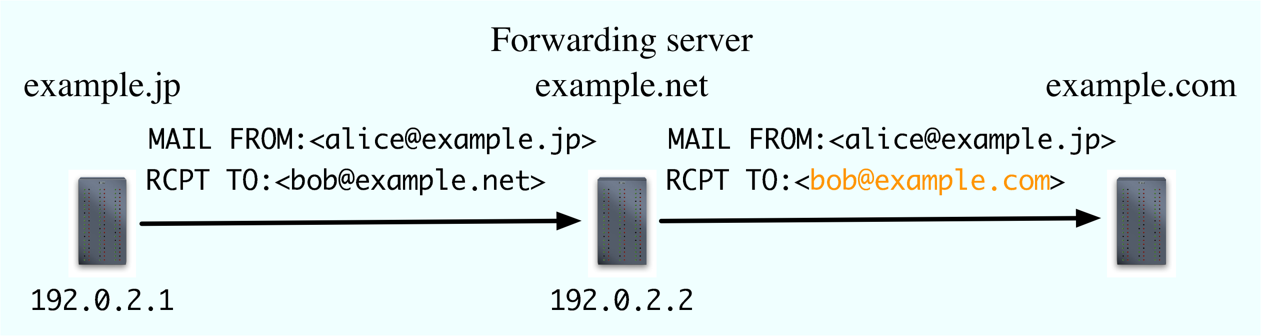


- First stage
  - Results are labeled to a header by receiving server

    Authentication-Results: mx.example.com
    from=alice@example.jp; spf=fail
  - Mailreaders filter with the label
- Second stage
  - Receiving server rejects receipt if verification fails

Problems on domain authentication

Forwarding and domain auth



Forwarding server

example.jp

example.net

example.com

MAIL FROM:<alice@example.jp>
RCPT TO:<bob@example.net>

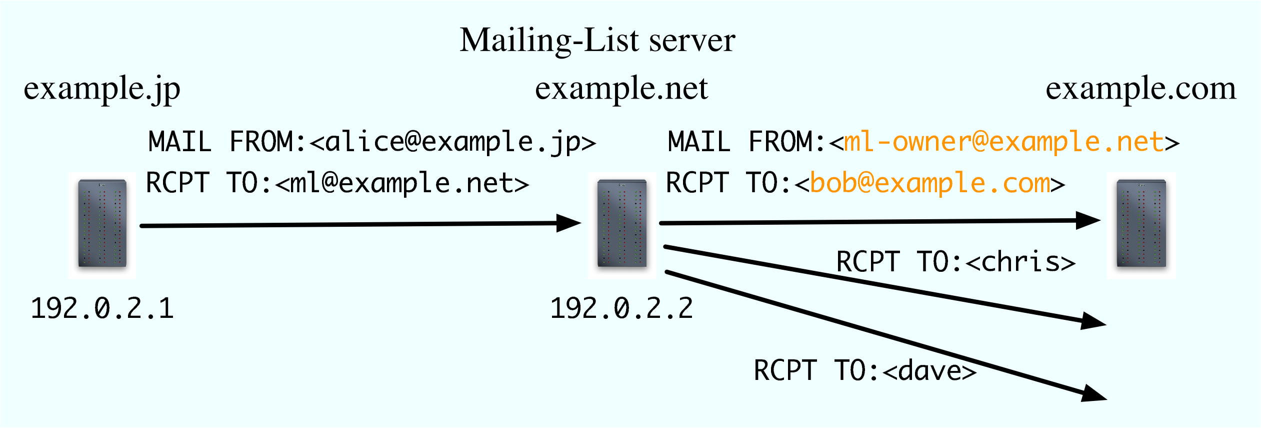
MAIL FROM:<alice@example.jp>
RCPT TO:<bob@example.com>

192.0.2.1

192.0.2.2

- SPF
  - Authentication fails
  - IP address changes but domain name does not change
  - Overriding MAIL FROM fixes this
    but routing loops occur
  - Proposals to prevent routing loops
    - http://www.iajapan.org/anti_spam/portal/en/s02_SPF.html
- DKIM
  - No problem because DKIM is independent of IP address

Mailing-list and domain auth



Mailing-List server

example.jp

example.net

example.com

```
MAIL FROM:<alice@example.jp>
RCPT TO:<ml@example.net>
```

```
MAIL FROM:<ml-owner@example.net>
RCPT TO:<bob@example.com>
RCPT TO:<chris>
RCPT TO:<dave>
```

192.0.2.1

192.0.2.2

- SPF
  - No problem because domain name also changes
- DKIM
  - Authentication may fail since ML server changes Subject: and body

SPF and DKIM

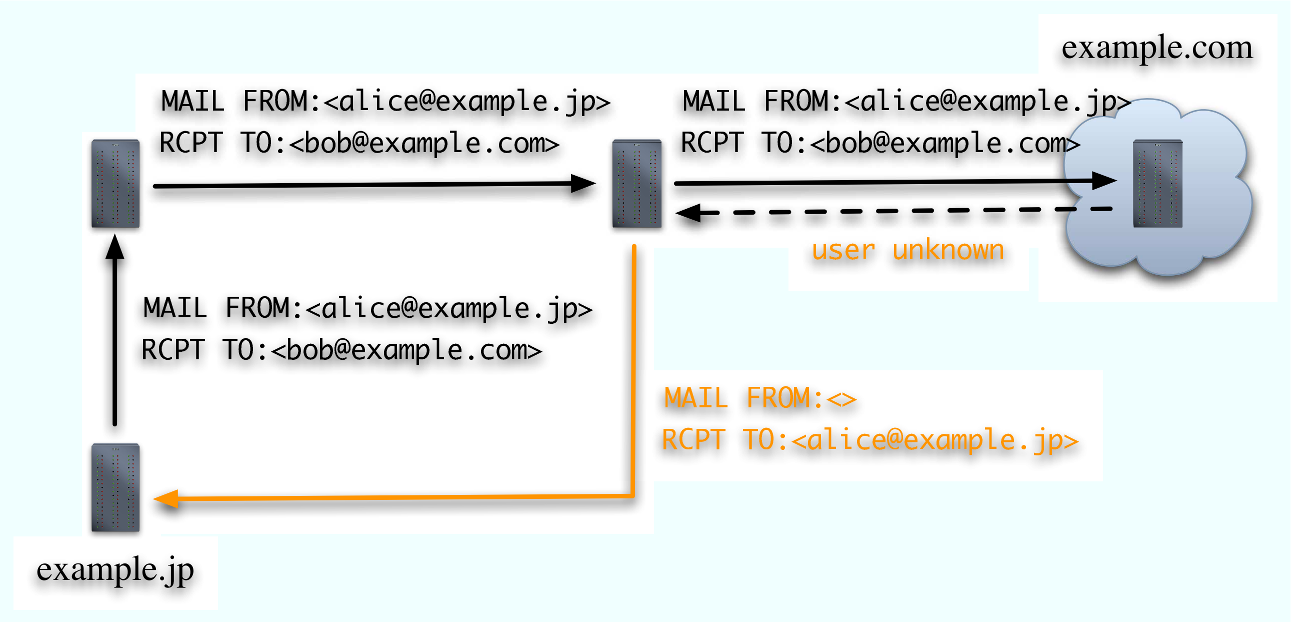
- SPF
  - Weak against forwarding
  - Strong against mailing-list
- DKIM
  - Strong against forwarding
  - Weak against mailing-list
- So, use both
  - SPF and DKIM can co-exist
  - If SPF check or DKIM check succeeds, accept receipt
  - If both checks fail, reject receipt

Deploying SPF

Problems on deploying SPF

- Early phase of deployment
  - Few merit of introduction
  - Operators are afraid that if they make mistakes, mails would be rejected by other sites
- Now in negative cycle
  - Sites cannot introduce until widely deployed
  - So, not widely deployed
- For positive cycle
  - We need motivation to introduce SPF
- Let’s make use of SPF to reduce unnecessary error mails!

Error mails on typical sites



example.com

```
MAIL FROM:<alice@example.jp>
RCPT TO:<bob@example.com>
```

```
MAIL FROM:<alice@example.jp>
RCPT TO:<bob@example.com>
```

user unknown

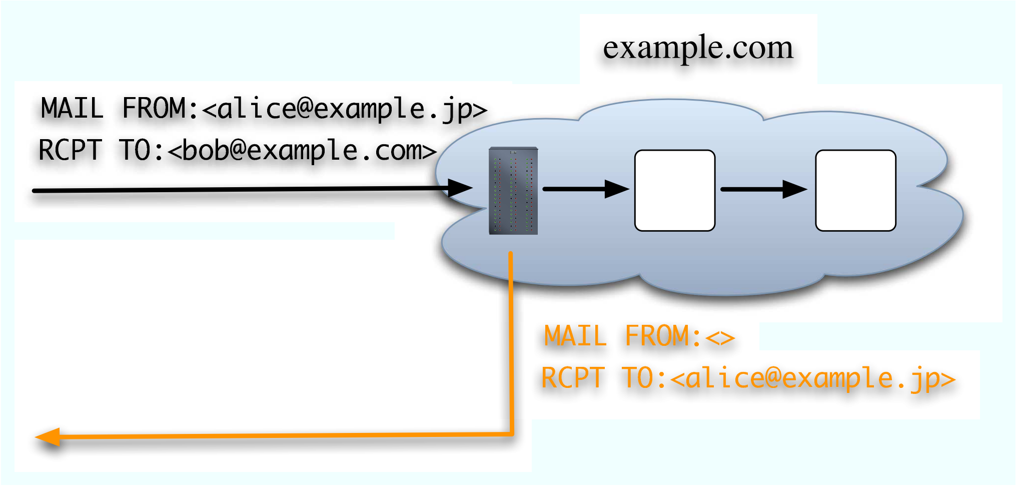
```
MAIL FROM:<alice@example.jp>
RCPT TO:<bob@example.com>
```

```
MAIL FROM:<>
RCPT TO:<alice@example.jp>
```

example.jp

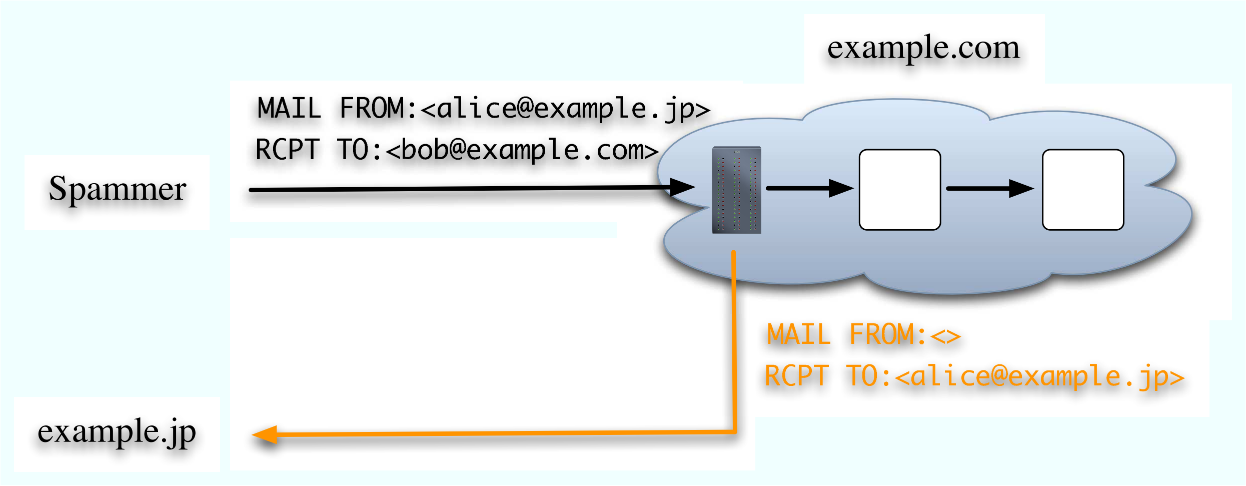
- The previous server generates an error mail
  - when it receives "user unknown"
  - when it receives "spool is full"

Error mails on ISPes


example.com
MAIL FROM:<alice@example.jp>
RCPT TO:<bob@example.com>
MAIL FROM:<>
RCPT TO:<alice@example.jp>

- ISP’s receiving server
  - accepts all mails even if a user is unknown to prevent harvesting attack
  - returns error mails by itself

Unnecessary error mails



```
MAIL FROM:<alice@example.jp>
RCPT TO:<bob@example.com>
```

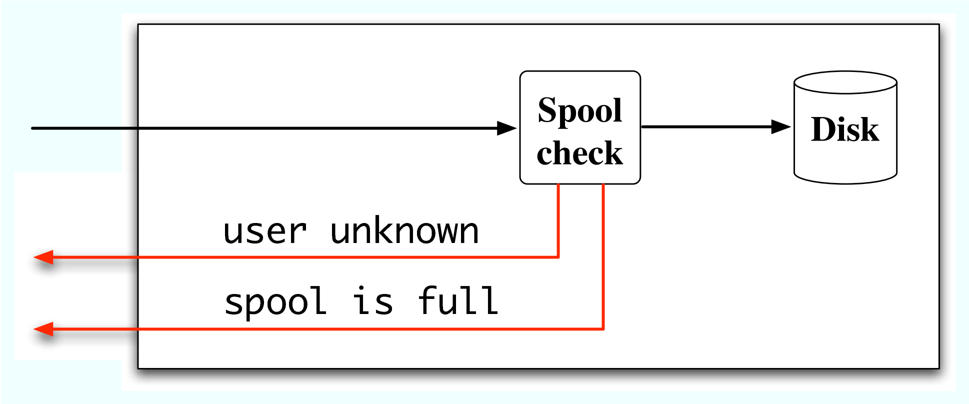
```
MAIL FROM:<>
RCPT TO:<alice@example.jp>
```

- Unnecessary error mails are caused by address faking
  - Almost all error mails are NOT necessary

Proposal for SPF deployment

- Reducing unnecessary error mails with SPF
- Redefine "~" (softfail)
  - MUST receive mails AND
  - Need NOT to generate error mails if user unknown
- Sender side declares "~all"
  - If it declares "?all", nothing improves
- Receiver side does not generate error mails if
  - SPF verification results in "fail" or "softfail" AND
  - user unknown

Reducing error mails with SPF

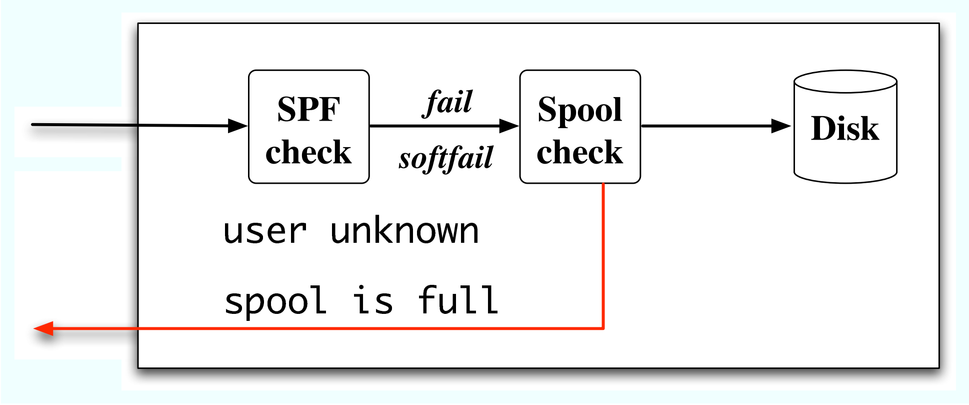


Spool check

Disk

user unknown

spool is full



SPF check

fail

softfail

Spool check

Disk

user unknown

spool is full

Reducing error mails with SPF (2)

- Positive cycle
  - If you declare "~all" in SPF RR,
    the number of receiving error mails will be reduced
- A patch for Sendmail
  - http://member.wide.ad.jp/wg/antispam/sm-dsn-supr/

Summary

Action items

- Submission and OP25B
  - Prepare submission port and SMTP AUTH
  - Consider to introduce OP25B
- SPF
  - Declare SPF RR with "~all" on sender side
  - Labeling result of SPF verification on receiver side
  - If SPF verification results in "fail" or "softfail" and user is unknown, do NOT generate an error mail
- DKIM
  - Consider to introduce DKIM
  - Labeling result of DKIM verification on receiver side

Documents

- Submission
  - RFC 4409
- SPF
  - RFC 4408
  - http://www.openspf.org/
- DKIM
  - Internet-draft
  - http://www.ietf.org/html.charters/dkim-charter.html
- The WIDE project
  - http://member.wide.ad.jp/wg/antispam/