



UNIVERSITY OF  
CALGARY

# **An Empirical Analysis of Email Delivery Security**

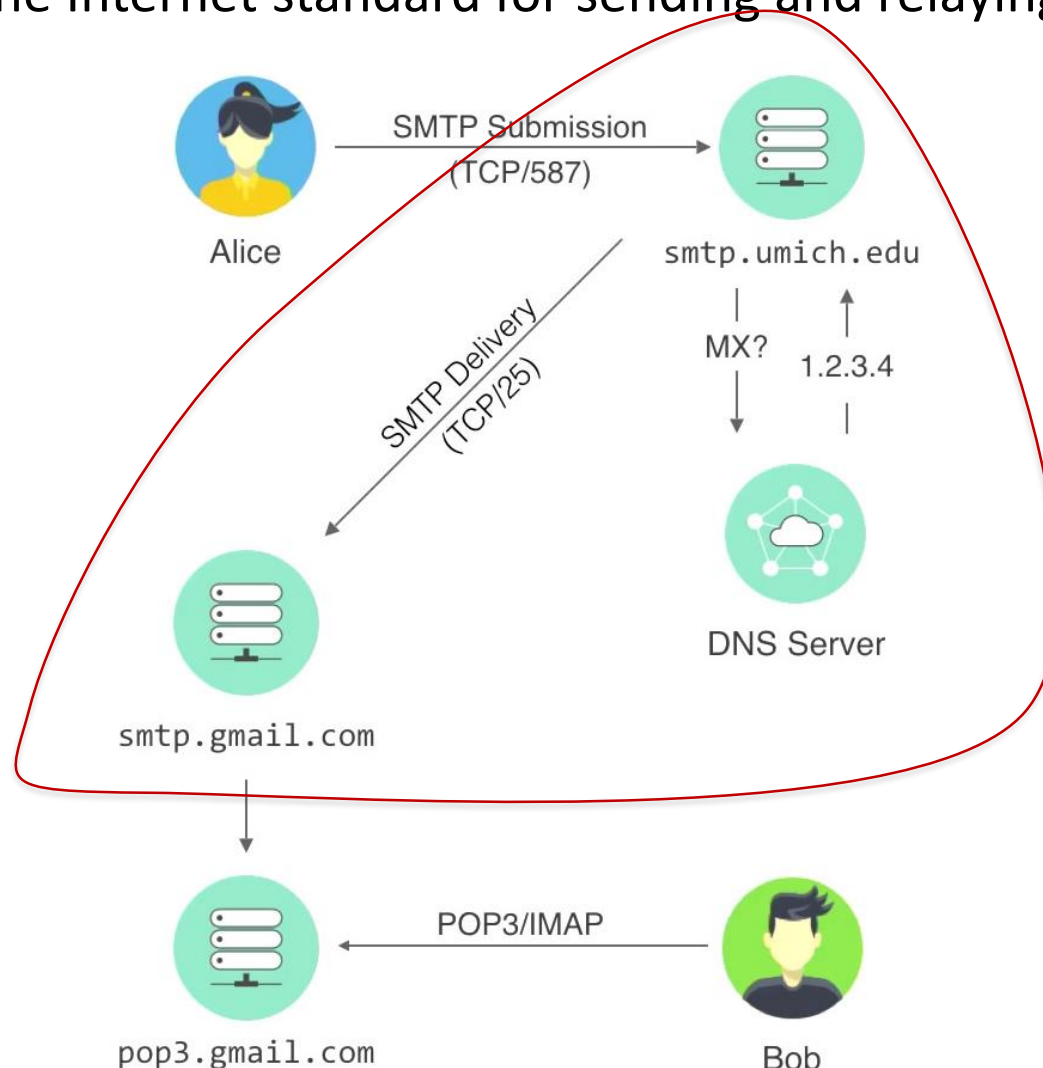
Zakir Durumeric et al.  
ACM IMC 2015

**How is your everyday email protected?**



# SMTP (Simple Mail Transfer Protocol)

- SMTP is the Internet standard for sending and relaying email.



- The original SMTP (RFC 821) had no built-in security at all.
- There have been several security extensions over the years:

Confidentiality (encrypt email in transit)

1

STARTTLS

Authenticate email on receipt

1

DKIM (Domain Keys Identified Mail)

2

SPF (Sender Policy Framework)

3

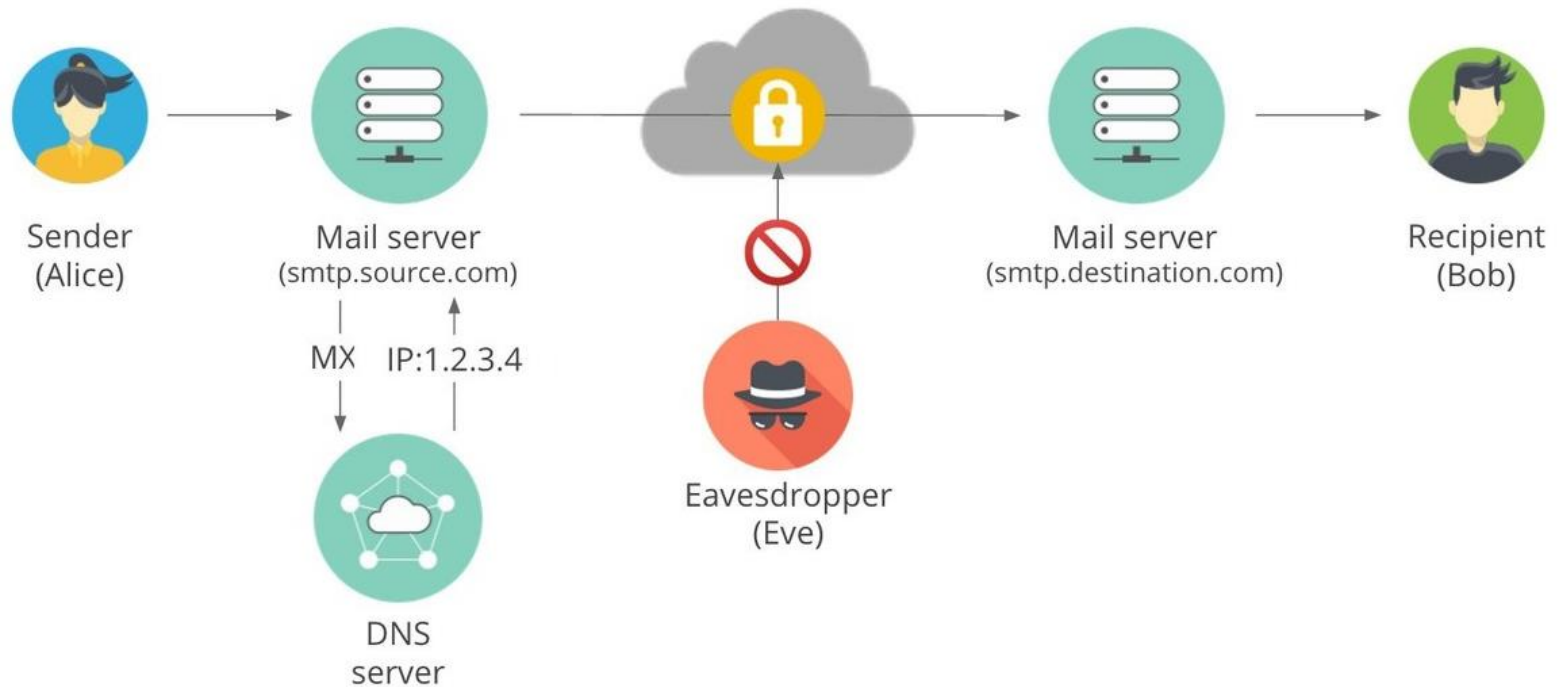
DMARC (Domain-based Message  
Authentication, Reporting + Conformance)



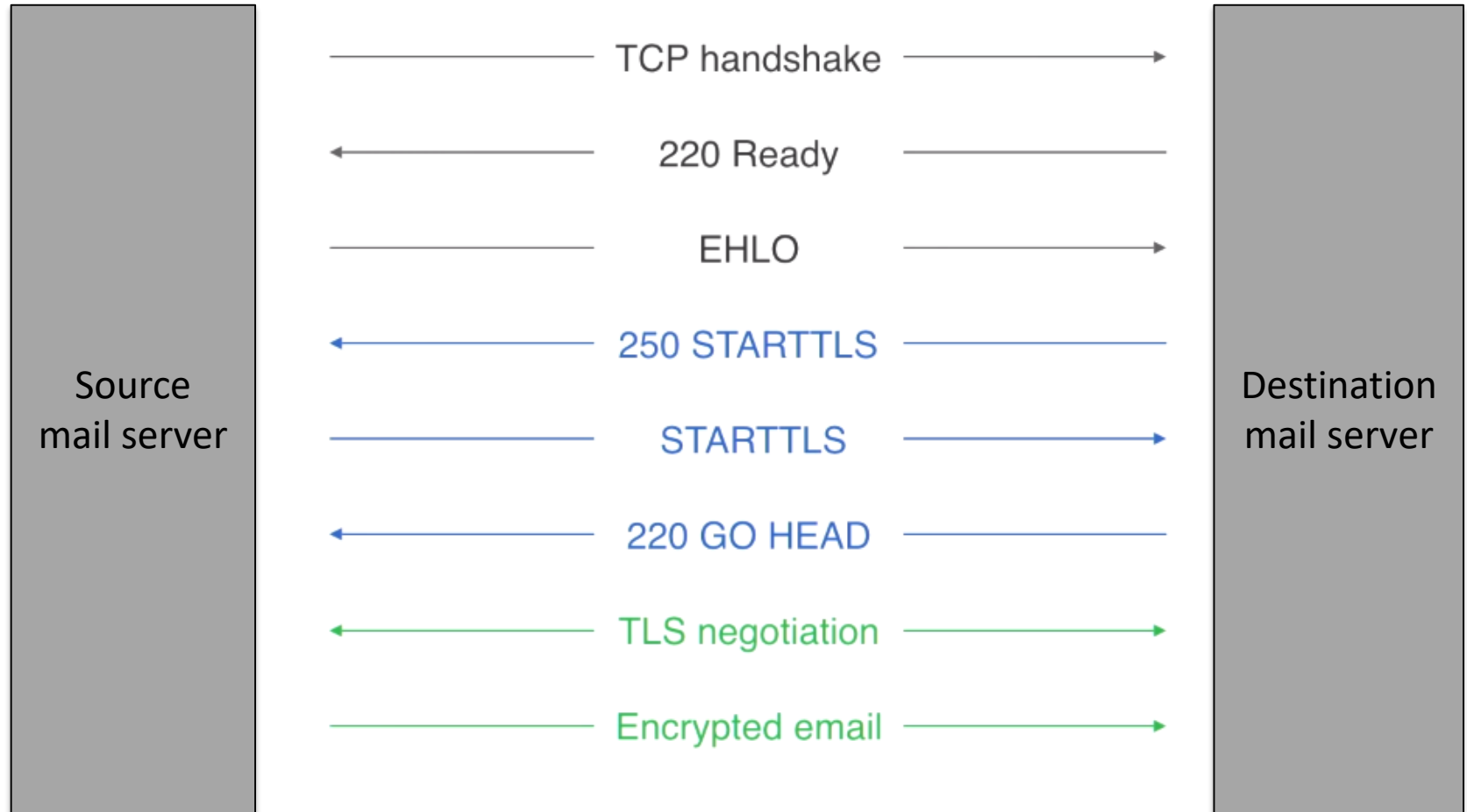
Deployment is voluntary and (usually) invisible to end users!

- 16 months of gmail inbound/outbound messages
  - Longitudinal view: January 2014 to April 2015
  - Used Google's "Transparency Report" for message stats
  - Also: analysis of ciphers negotiated with SMTP servers
  
- Mail servers from the top 1 million Alexa domains
  - Snapshot view: current state as of April 2015
  - Performed MX lookups in DNS for popular domains
  - For domains with mail servers (79%), a DNS query was used to identify security extensions supported (if any)
  - Attempted SMTP/STARTTLS handshake using Zmap

# STARTTLS: TLS for SMTP



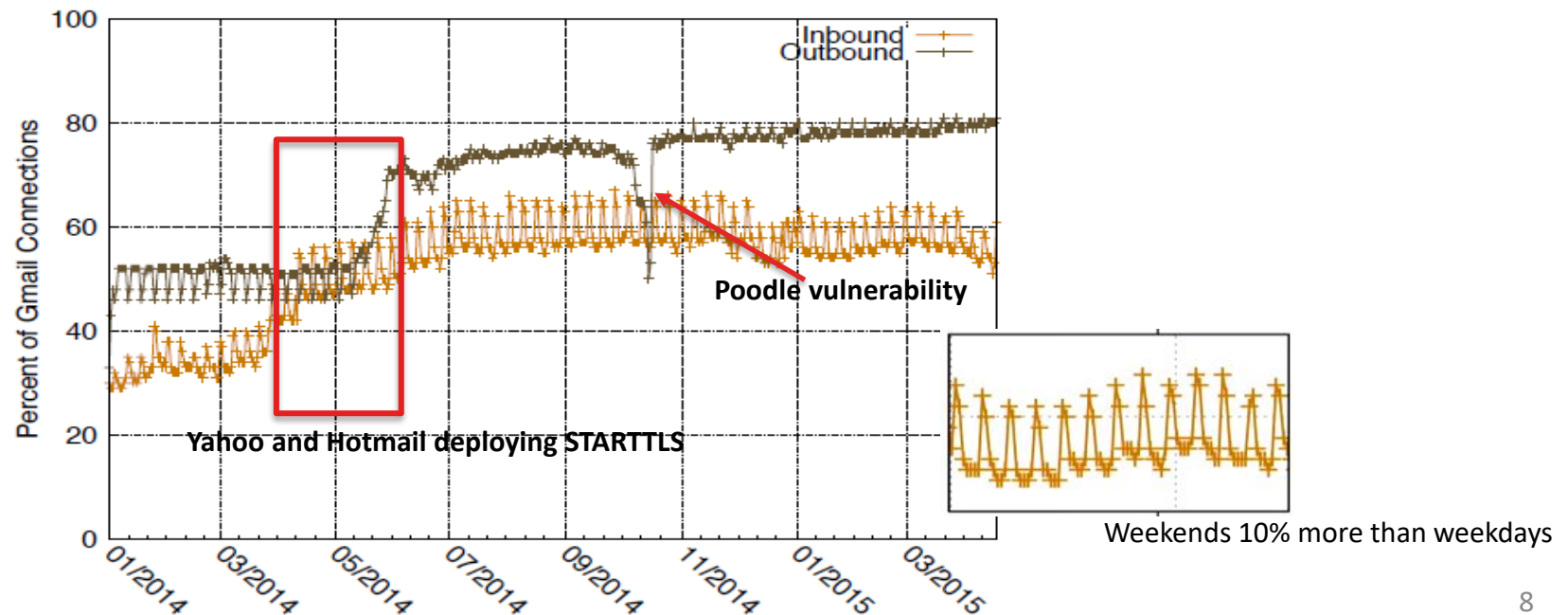
- Allows TLS session to be started during an SMTP connection
- Mail is transferred over an encrypted session
- Protection against passive eavesdroppers



# Empirical Measurements of STARTTLS

- Based on the volume of messages protected by STARTTLS
- As of April 26, 2015

|                          | STARTTLS Initiation | Increase from January 2014 |
|--------------------------|---------------------|----------------------------|
| <b>Outgoing messages</b> | 80%                 | 54%                        |
| <b>Incoming messages</b> | 60%                 | 82%                        |

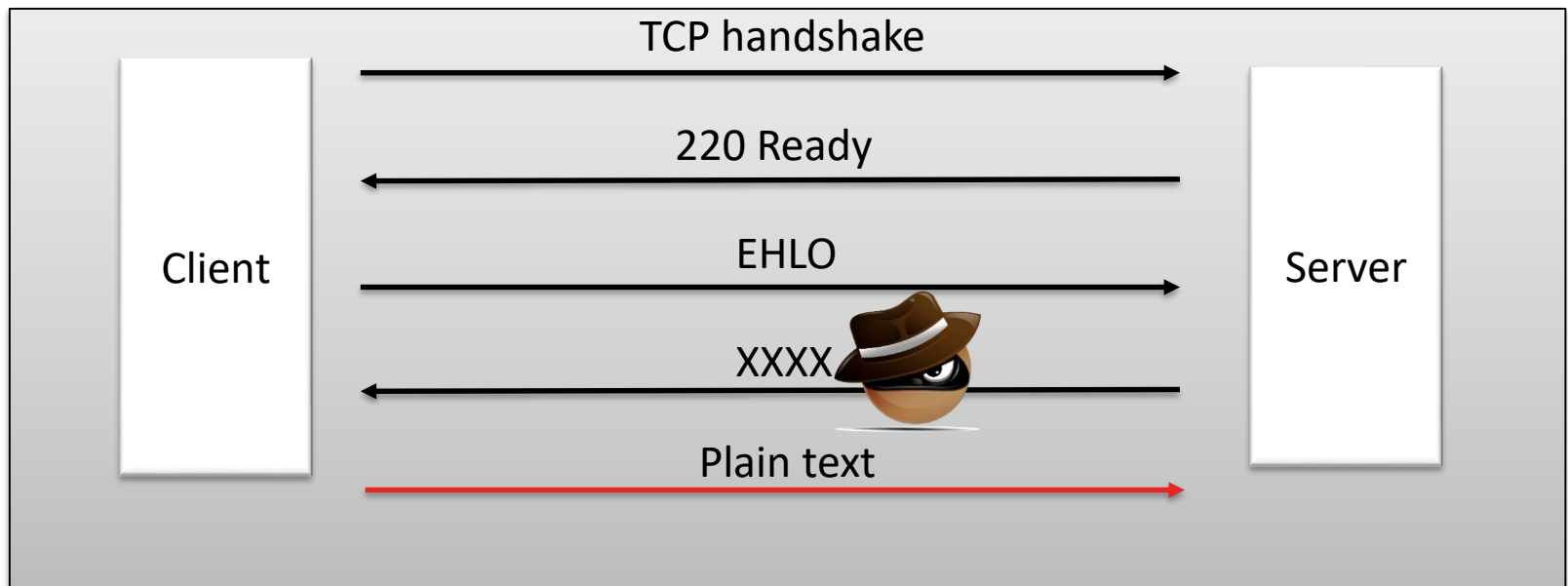


## Findings:

- 80% of outbound connections are protected by TLS
- About half of all incoming connections chose a strong cipher suite
- About 45% of clients use RC4 despite its known weaknesses

| Provider      | Incoming Key Exchange | Incoming Cipher | Certificate Name | Outgoing Key exchange | Outgoing Cipher |
|---------------|-----------------------|-----------------|------------------|-----------------------|-----------------|
| Gmail         | ECDHE                 | AES128-GCM      | match            | ECDHE                 | AES128-GCM      |
| Yahoo         | ECDHE                 | AES128-GCM      | match            | ECDHE                 | RC4-128         |
| Microsoft     | ECDHE                 | AES256-CBC      | match            | ECDHE                 | AES256          |
| Apple iCloud  | ECDHE                 | AES128-GCM      | match            | DHE                   | AES128-GCM      |
| Facebook mail | RSA                   | AES128-CBC      | mismatch         | ECDHE                 | AES128-CBC      |
| Comcast       | RSA                   | RC4-128         | match            | DHE                   | AES128-CBC      |
| AT&T          | ECDHE                 | AES128-GCM      | match            | ECDHE                 | RC4-128         |

- STARTTLS provides protection against passive eavesdroppers, but not against active attackers who can tamper with packets
- STARTTLS is designed to “**fail open**” rather than “**fail closed**” (i.e., defaults to plain text if TLS negotiation fails)
- An active attacker can manipulate the packets containing STARTTLS to prevent servers from establishing a secure channel!



# Geographical Analysis of Active Attacks

| Organization Type     |     |
|-----------------------|-----|
| Corporation           | 43% |
| ISP                   | 18% |
| Financial Institution | 14% |
| Academic Institution  | 8%  |
| Healthcare Provider   | 3%  |
| Unknown               | 3%  |
| Airport               | 2%  |
| Hosting Provider      | 2%  |
| NGO                   | 1%  |

| Country          |       |
|------------------|-------|
| Tunisia          | 96.1% |
| Iraq             | 25.6% |
| Papua New Guinea | 25.0% |
| Nepal            | 24.3% |
| Kenya            | 24.1% |
| Uganda           | 23.3% |
| Lesotho          | 20.3% |
| Sierra Leone     | 13.4% |
| New Caledonia    | 10.1% |
| Zambia           | 10.0% |

| Country                |      |
|------------------------|------|
| Reunion                | 9.3% |
| Belize                 | 7.7% |
| Uzbekistan             | 6.9% |
| Bosnia and Herzegovina | 6.5% |
| Togo                   | 5.5% |
| Barbados               | 5.3% |
| Swaziland              | 4.6% |
| Denmark                | 3.7% |
| Nigeria                | 3.6% |
| Serbia                 | 3.1% |

Cisco exploits this feature to detect spammers and prevent attacks.

**Downfall:** Every email from your country will be in plain text!

- When we receive a message, we want to see if it is sent from someone **authorized** in the source domain.
- Detecting spams

## SPF (Sender Policy Framework)

- Allows a domain to put a DNS TXT record that lists the IP addresses of their legitimate mail servers
- Example: <spf-mail.example.com> “v=sfp1 ip4:64.18.0.0/20 -all”



## DKIM (Domain Keys Identified Mail )

- The sender publishes its public key in a DNS record

```
20120113._domainkey.gmail.com. 300 IN TXT "k=rsa\; p=MIIBIjAN...AQAB"
```

- Sender attaches cryptographic signature in a message's header

DKIM-Signature:

v=1;

a=rsa-sha256;

c=relaxed/relaxed;

d=gmail.com;

s=20120113;

h=from:date:....subject:to;

bh=RjhXzraob5/q4159G000YE=;

b=YZmpde8KxvpfX...anUdYxVgc

Signing domain

Body hash

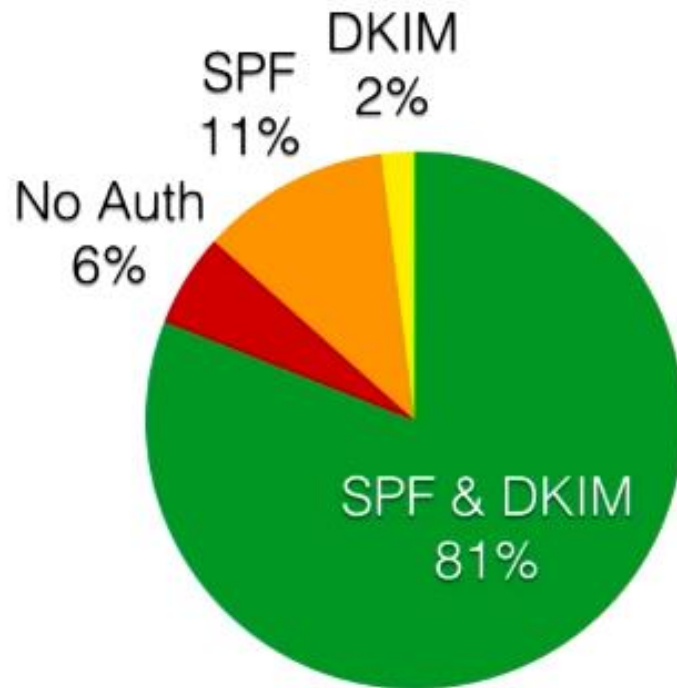
Digital signature of the content

- Recipient checks the signature, using the public key p

- DMARC: Domain-based Message Authentication, Reporting, and Conformance
- Builds upon DKIM and SPF

```
_dmarc.yahoo.com. 1800 IN TXT "v=DMARC1;  
p=reject;  
pct=100;  
rua=mailto:dmarc_y_rua@yahoo.com;"
```

- Recipient checks for the sender's policy



**Delivered Gmail Messages**

| Technology   | Top 1M |
|--------------|--------|
| SPF Enabled  | 47%    |
| DMARC Policy | 1%     |

| DMARC Policy | Top 1M |
|--------------|--------|
| Reject       | 20%    |
| Quarantine   | 8%     |
| None         | 72%    |

**Top Million Domains**

**April 2015**

- SMTP by itself is NOT secure
- Mail community has started to deploy new security extensions, but progress is slow for small organizations
- STARTTLS is not a long-term solution, since active attacks are prevalent and potentially very serious