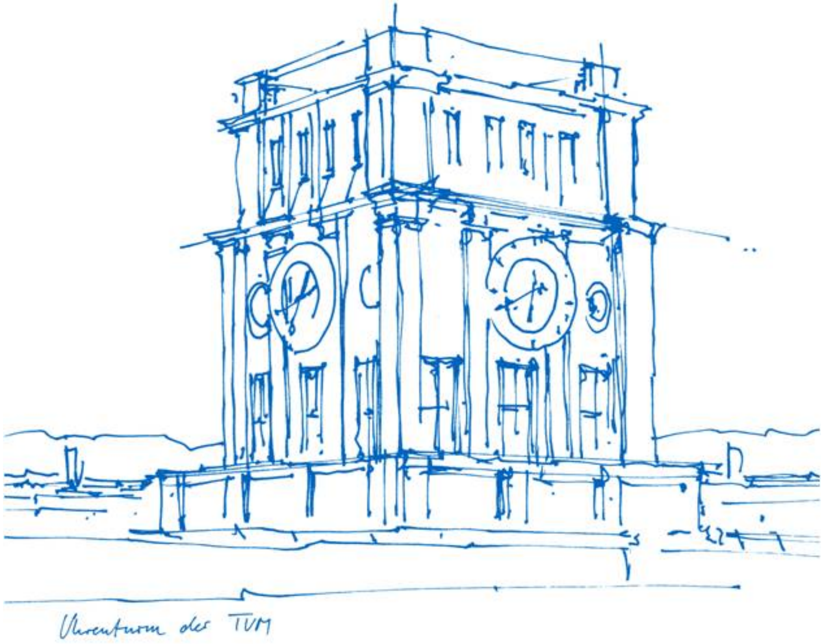
Neither Snow Nor Rain Nor MITM ...
An Empirical Analysis of Email Delivery Security

by Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten
Elie Bursytein, Nicolas Lidzborski, Kurt Thomas,
Vijay Eranti, Michael Bailey, J. Alex Champaign

Muhammad Triwindu Prasetya

Technische Universität München

München, 22 June 2017



Agenda

1. Abstract
2. Introduction
3. Background
4. Methodology
    1. Implementation
    2. Dataset
5. Results
6. Conclusion

Abstract

- SMTP (Simple Mail Transfer Protocol)
  - Note: does not have a feature for authenticating the sender or encrypt mail in transit
- The team present:
  - The report on global adoption rate of SMTP security extension, including:
    - STARTTLS
    - SPF (Sender Policy Framework)
    - DKIM (DomainKeys Identified Mail)
    - DMARC (Domain – based Message Authentication Reporting & Conformance)
  - The data from 2 perspectives:
    - SMTP configuration for Alexa Top Million domains (from April 2015)
    - SMTP connection to and from Gmail (January 2014 – April 2015)
  - The evidence of such attacks in the wild highlighting, 7 countries where:
    - More than 20% inbound Gmail message arrives in clean text due to network attackers

Introduction

E-mail carries some of users most sensitive communication, such as:

- Private correspondence
- Financial detail
- Password recovery confirmation (lead to other critical resources)

What users expected?

- Private
- Unforgeable

However, SMTP does not authenticate sender or encrypt mail in transit. Instead, servers support security extension features voluntary.

And also the team, measure the global adoption of SMTP security extension and resulting impact on end users.

Continued...

The team used the data from both perspectives to estimate:

- The volume of messages
- Total of mail servers that support encryption and authentication
- Identify mail server configuration pitfalls that weaken security guarantees
- Expose threats introduced by lax security policy (enable wide – scale surveillance and message forgery)

Gmail Perspective

- Incoming message by TLS have increased 82%
  - Peaking at 60% of all inbound mail in April 2015
- Outgoing grew 54% with 80% of messages are protected
  - Improvement largely increased by small number of popular web mail provider, such as:
    - Yahoo
    - Outlook

Alexa Top Million Perspective

- Only 82% SMTP Server associated with Alexa support TLS
  - Mere 35% are properly configured to allow server authentication
  - 2 or 3 SMTP software platform fail to protect the message by default

Adoption SMTP Security Extension

- Gmail
  - Able to validate 94% inbound message (combination DKIM and SPF)
- Alexa Top Million
  - Among the mail servers, only 47% deploy SPF policies and 1% provide DMARC policy
  - Implication: make the recipients unsure the unsigned message is invalid or expected

Example of an attack:

- The team identify 41,405 SMTP server in 4,714 ASes and 193 countries can‘t protect passive eavesdropper due to corruption on STARTTLS on network
- Analyzing that mail sent to Gmail from these hosts
  - Found that in 7 countries, >20% of all messages prevented from being encrypted
  - 96% of messages are downgraded to cleartext are sent from Tunisia

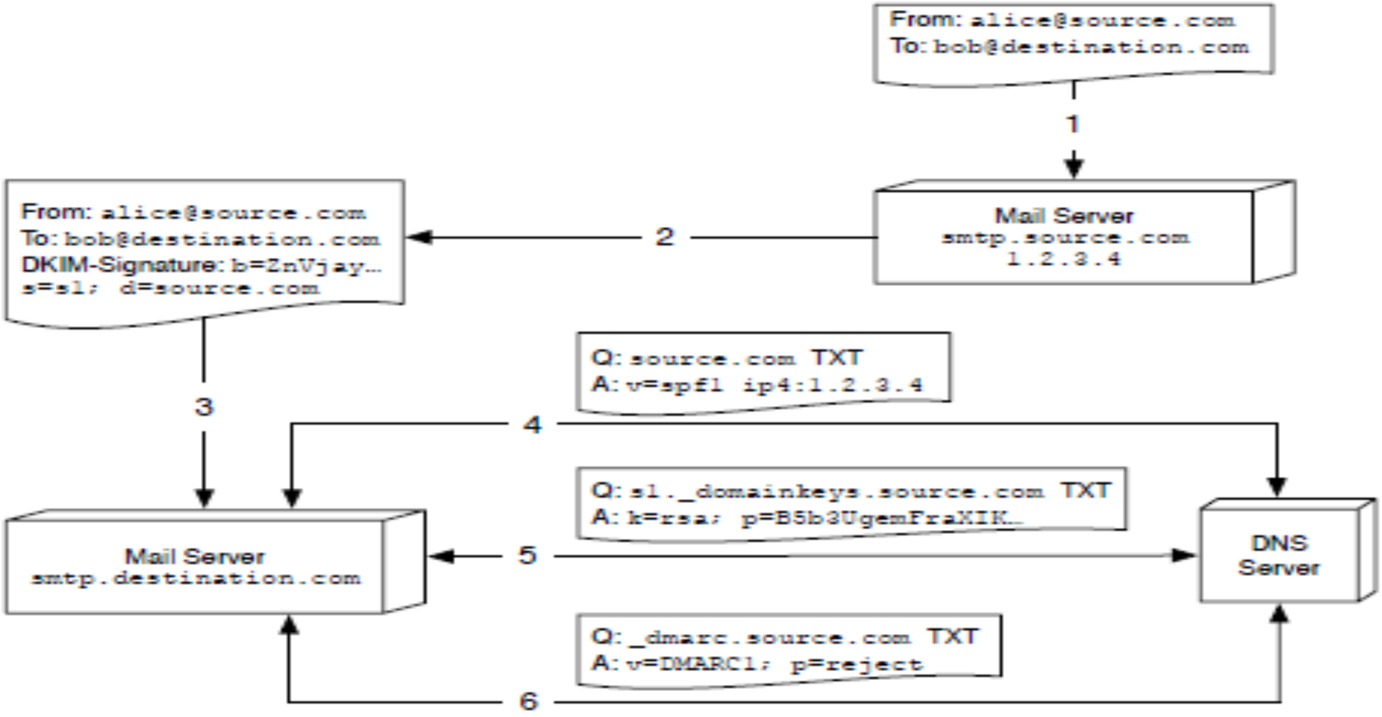
Background

SMTP does not support confidentiality of message in transit and authenticating message after recipients received the message.

- Protecting messages in transit
  - One way: use STARTTLS
    - STARTTLS aims to protect hops between server
    - Primarily protect from passive eavesdroppers
    - Not use for authentication mail server, rather providing encryption
    - If STARTTLS no supported, mail server relay the message in cleartext

Continued...

- Authenticating Mail



From: alice@source.com
To: bob@destination.com

Mail Server
smtp.source.com
1.2.3.4

From: alice@source.com
To: bob@destination.com
DKIM-Signature: b=ZnVjay…
s=s1; d=source.com

Q: source.com TXT
A: v=spf1 ip4:1.2.3.4

Q: s1._domainkeys.source.com TXT
A: k=rsa; p=B5b3UgemFraXIK…

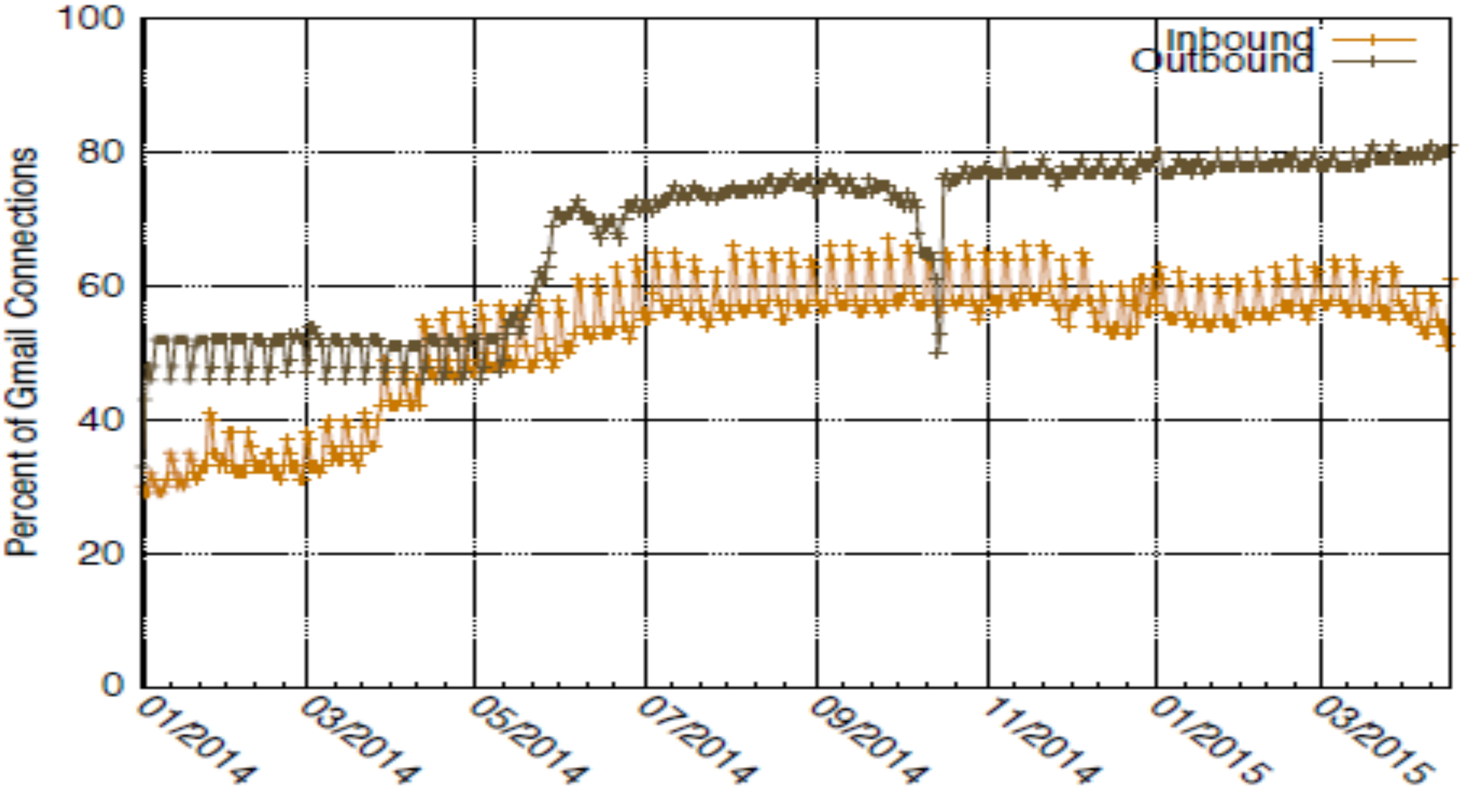
Q: _dmarc.source.com TXT
A: v=DMARC1; p=reject

Mail Server
smtp.destination.com

DNS
Server

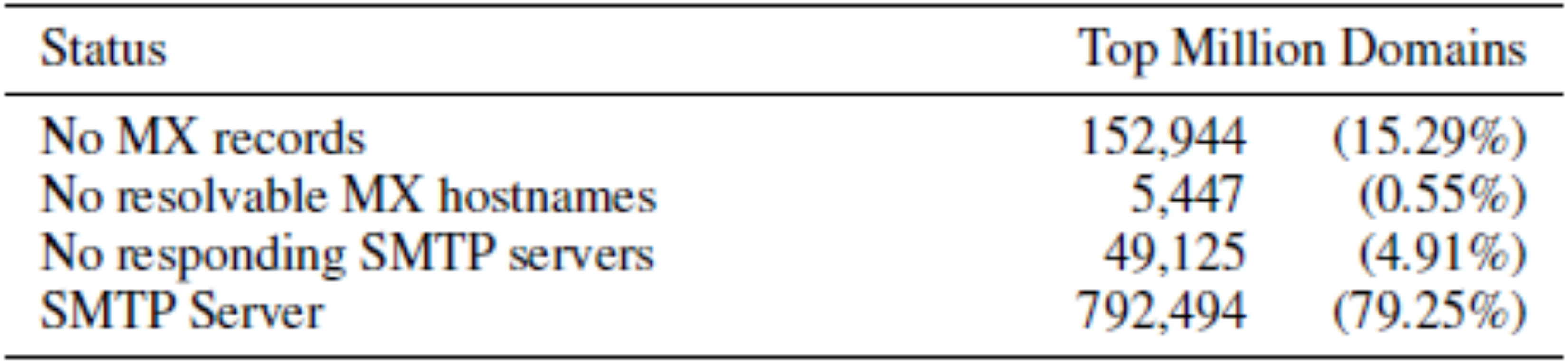
Dataset

Gmail Inbound and Outbound Messages



Continued...

Alexa Top Million Mail Severs

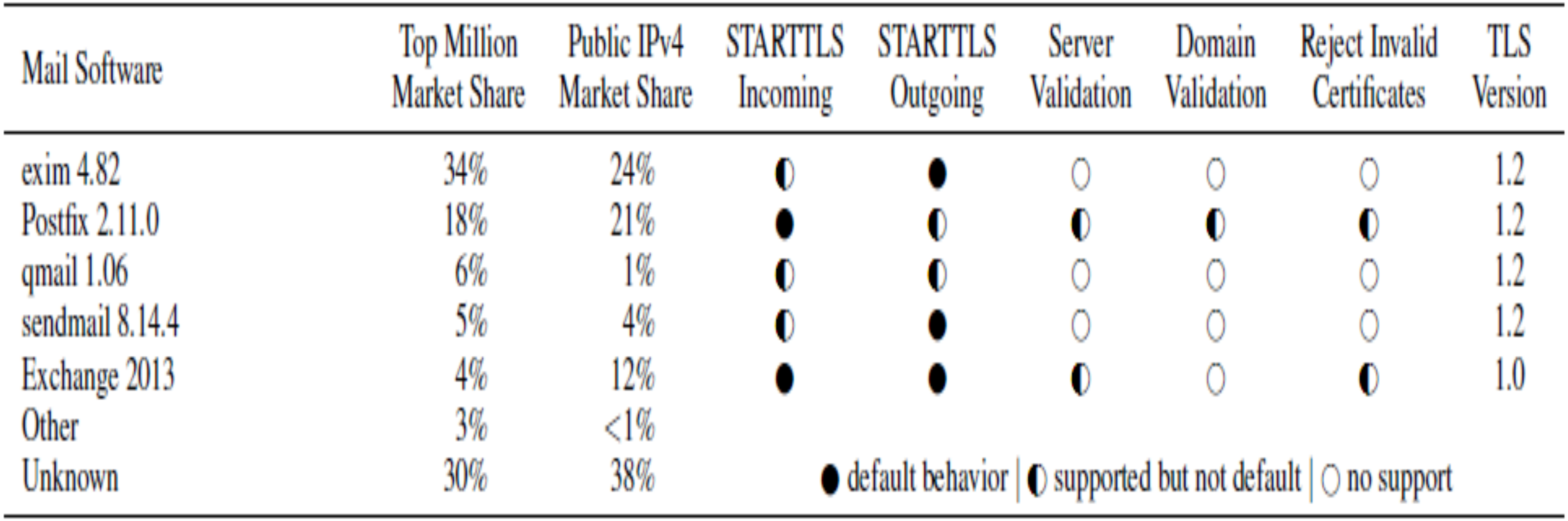


Status	Top Million Domains	
No MX records	152,944	(15.29%)
No resolvable MX hostnames	5,447	(0.55%)
No responding SMTP servers	49,125	(4.91%)
SMTP Server	792,494	(79.25%)

Implementation

The team tested whether:

- Each implementation initiated STARTTLS on each SMTP
- Supported incoming STARTTLS connection
- How it validated



Mail Software	Top Million Market Share	Public IPv4 Market Share	STARTTLS Incoming	STARTTLS Outgoing	Server Validation	Domain Validation	Reject Invalid Certificates	TLS Version
exim 4.82	34%	24%	◐	●	○	○	○	1.2
Postfix 2.11.0	18%	21%	●	◐	◐	◐	◐	1.2
qmail 1.06	6%	1%	◐	◐	○	○	○	1.2
sendmail 8.14.4	5%	4%	◐	●	○	○	○	1.2
Exchange 2013	4%	12%	●	●	◐	○	◐	1.0
Other	3%	<1%						
Unknown	30%	38%						

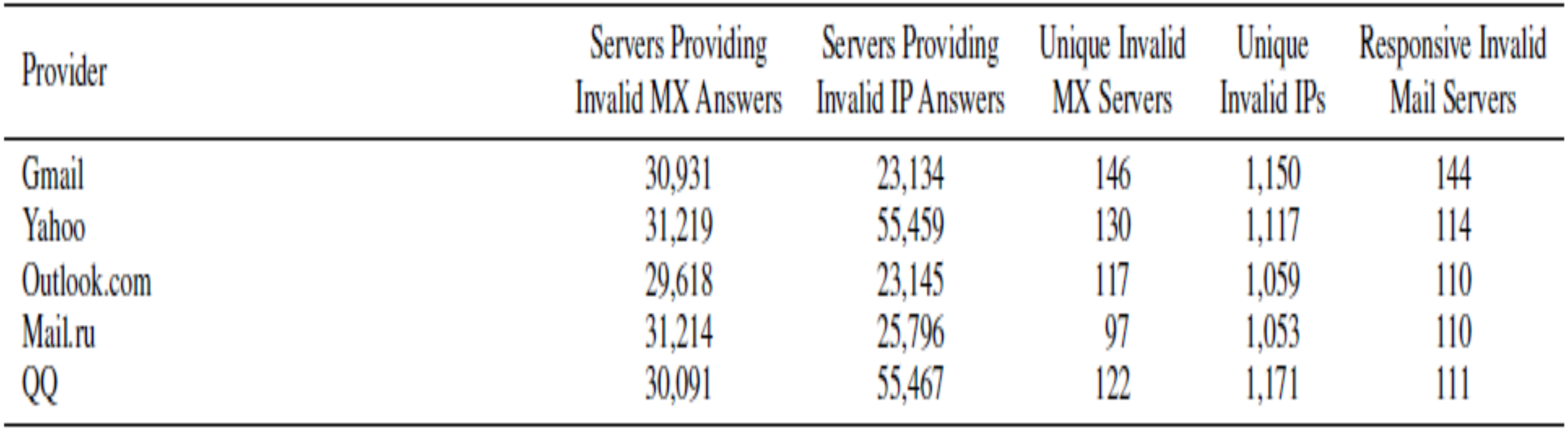
● default behavior | ◐ supported but not default | ○ no support

Threats to Confidentiality

STARTTLS protects from passive eavesdropper but not MITM

2 types of network attack:

- Downgrading STARTTLS session to insecure channel
- Falsifying MX record to re – route message



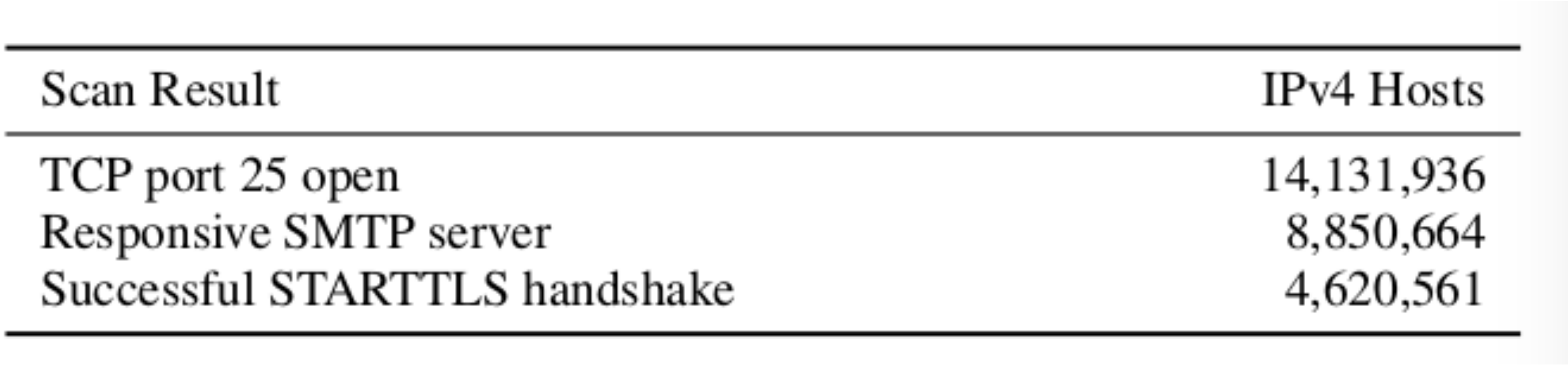
Provider	Servers Providing Invalid MX Answers	Servers Providing Invalid IP Answers	Unique Invalid MX Servers	Unique Invalid IPs	Responsive Invalid Mail Servers
Gmail	30,931	23,134	146	1,150	144
Yahoo	31,219	55,459	130	1,117	114
Outlook.com	29,618	23,145	117	1,059	110
Mail.ru	31,214	25,796	97	1,053	110
QQ	30,091	55,467	122	1,171	111

STARTTLS Corruption

- An active attack can prevent mail encryption by tampering with the establishment of a TLS session
- The attacker take an advantage of the fail – open STARTTLS when an error occurs during STARTTLS handshake then the attacker launch downgrade attack.

Scanning Methodology

- The team build SMTP servers that are frequently report back invalid command
- Performed a TCP SYN scan on port 25
  - Attempted to perform an SMTP and STARTTLS handshake with responsive hosts



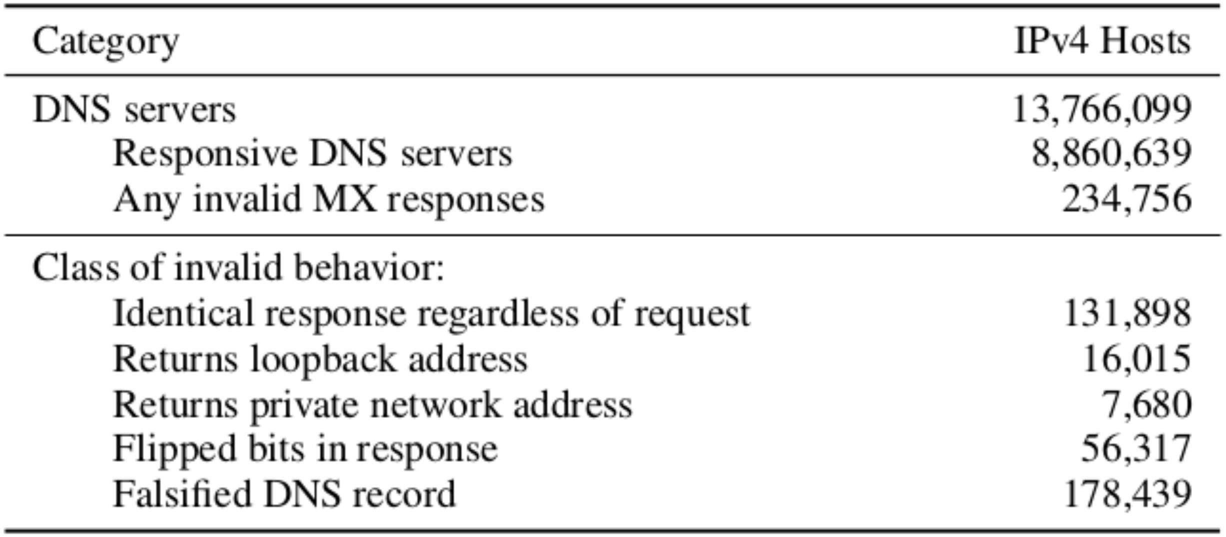
Scan Result	IPv4 Hosts
TCP port 25 open	14,131,936
Responsive SMTP server	8,850,664
Successful STARTTLS handshake	4,620,561

DNS Hijacking

- An active attacker can spoof the DNS records of destination mail server
- Then redirecting SMTP connections to a server under attacker’s control

Scan Methodology

- Use Zmap for identifying servers with falsified DNS records



Category	IPv4 Hosts
DNS servers	13,766,099
Responsive DNS servers	8,860,639
Any invalid MX responses	234,756
Class of invalid behavior:	
Identical response regardless of request	131,898
Returns loopback address	16,015
Returns private network address	7,680
Flipped bits in response	56,317
Falsified DNS record	178,439

Conclusion

- SMTP did not support confidentiality and integrity
- SMTP security extension
  - STARTTLS
  - SPF
  - DKIM
  - DMARC
- The authors used data from 2 perspectives:
  - SMTP connection to and from Gmail
  - SMTP configuration for Alexa Top Million
- Large providers play important role in improvement
- Fail – open STARTTLS leads to exposing users
  - Potentially for Man-In-The-Middle attack

THANK YOU