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

`IMC2015`

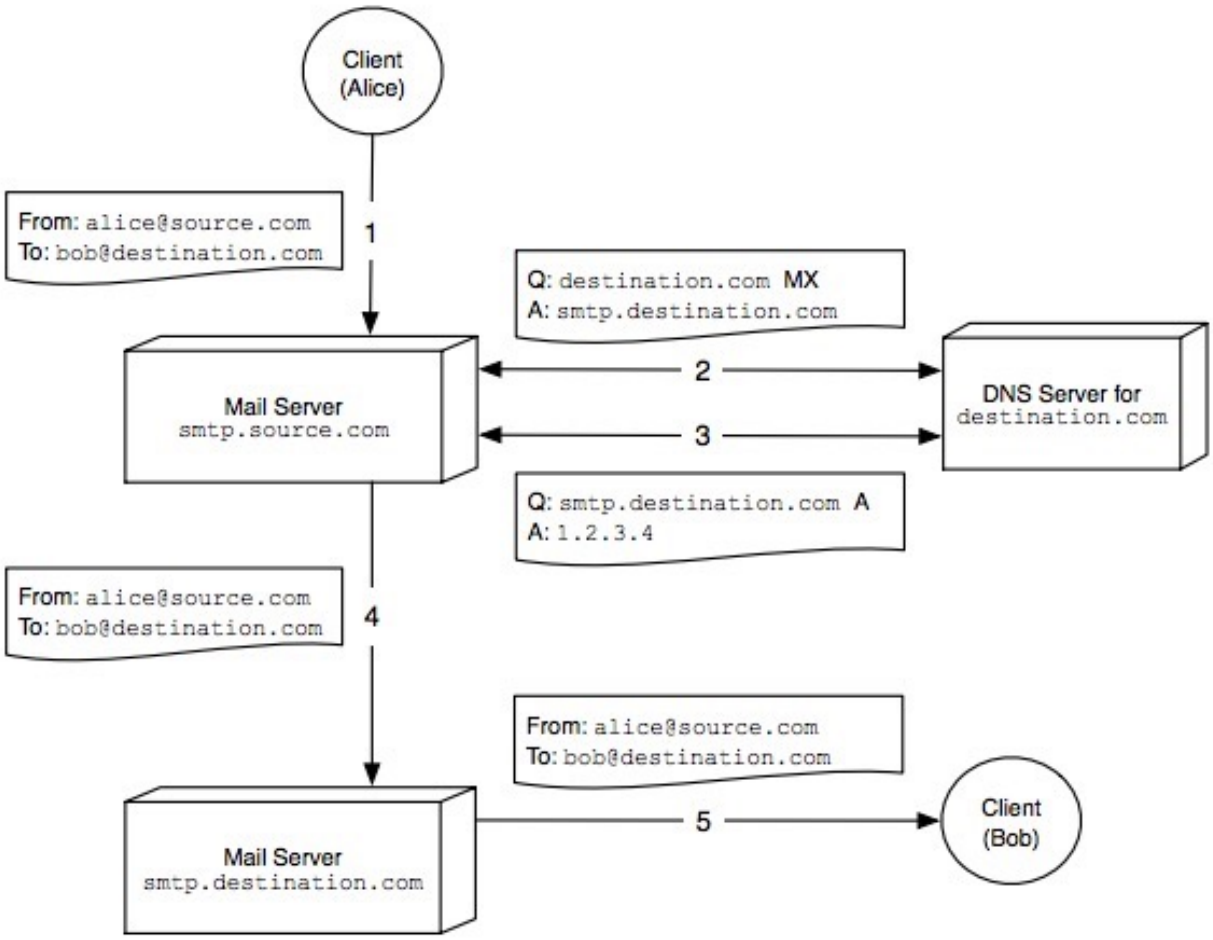
link

作者单位Zakir Durumeric† David Adrian† Ariana Mirian† James Kasten† Elie Bursztein‡ Nicolas Lidzborski‡ Kurt Thomas‡ Vijay Eranti‡ Michael Bailey§ J. Alex Halderman†
† University of Michigan ‡ Google, Inc. § University of Illinois, Urbana Champaign
【其中来自密歇根大学的作者是ZMAP、Mining your Ps and Qs及Logjam的作者】

1.Abstract

SMTP协议是提供邮件发送和中转的协议。像其他网络协议一样，对消息认证性和机密性的保护都是在事后才考虑并加入的。本文是第一个对SMTP安全扩展的全球接受和使用情况进行研究的文章。SMTP安全扩展包括STARTTLS，SPF，DKIM和DMARC，用于加密消息内容及认证消息发送方。文章的实验数据包括两个部分：Alexa前一百万域名的SMTP服务器配置，及一年中发往和来自Gmail的SMTP连接。
这些数据用于估计支持加密和认证的服务器数量及安全发送的消息数目，发现服务器配置缺陷，以及揭示因不严格的安全策略而导致大规模监听和消息伪造的安全威胁。

SMTP



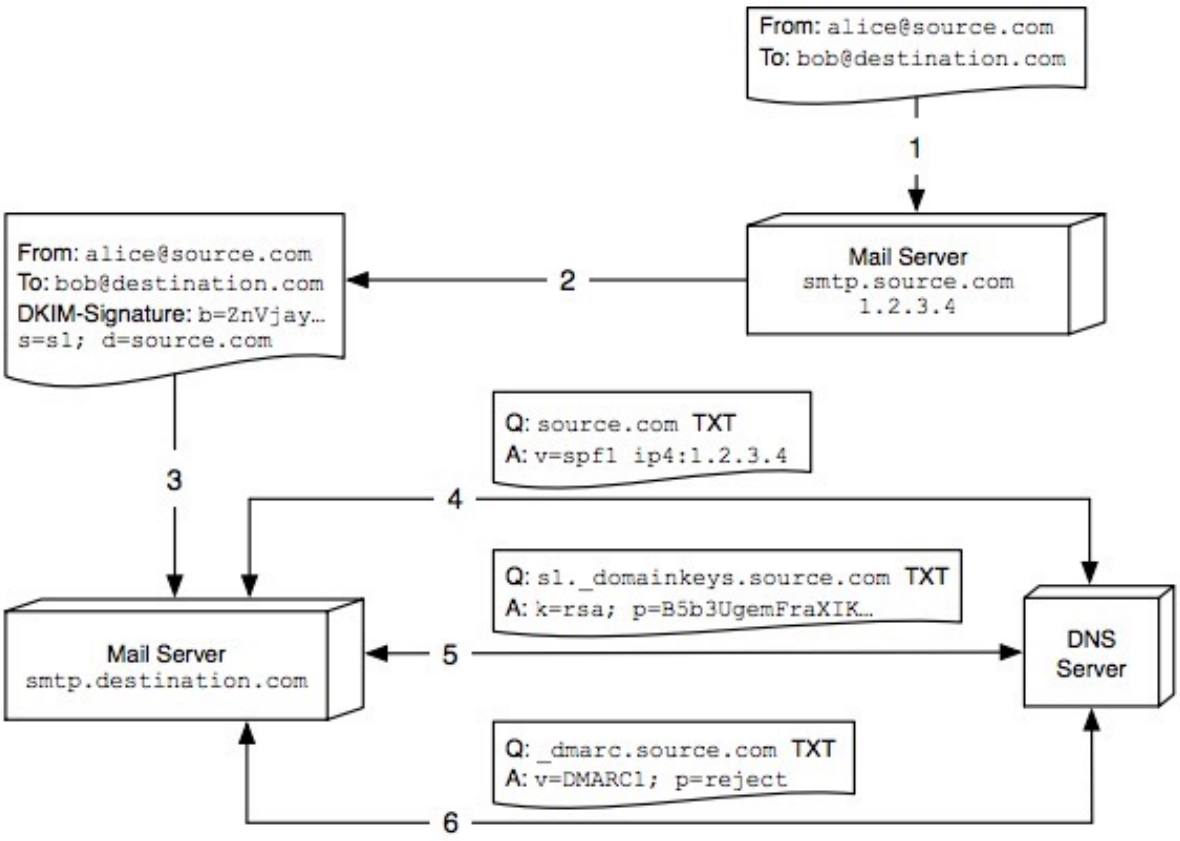
2.SMTP安全扩展

2.1保护传输消息

STARTTLS扩展：客户端先与服务器建立smtp连接，然后向服务器发送starttls命令，发起tls握手，之后在tls通道中传输数据。
STRATTLS保护的是两个SMTP服务器之间的通信，且它的主要目的并不是验证通信目的邮件服务器的身份，而是提供机会加密。大多数情况下，通信源邮件服务器不会验证目的邮件服务器的证书，并且在STARTTLS不支持的情况下，使用明文通信。此外，每个中继服务器都可以随意读和修改消息。

2.2邮件认证【source authentication】

其他一些扩展用于认证收到的邮件及检查邮件的完整性（邮件没有被伪造及修改），并且提供可以报告伪造消息的机制。



2.2.1 DKIM（DomainKeys Identified Mail）

可以让服务器检查到收到的消息在传输过程中是否被修改或伪造。发送者在消息头部附加由发送者私钥签名的DKIM-Signature，私钥已与发送者的域名绑定。接收者收到后，通过DNS请求检索到发送者的公钥并验证签名。

【的确是某个服务器所发】

2.2.2 SPF（Sender Policy Framework）

让域名的拥有者通过DNS记录发布已被授权可以为其域名发送邮件的一系列主机名。接收者通过DNS查询到SPF策略，如果消息不是来自指定的服务器，则拒绝接受。

【邮件是否应该来自某个服务器】

2.2.3 DMARC（Domain-based Message Authentication，Reporting and Conformance）

基于DKIM和SPF，允许发送者建议验证收到邮件的策略。发送者发布DNS TXT记录，表明发送者是否支持邮件认证（DKIM，SPF）以及认证失败时接收方应该怎么做。此外DMARC还允许域名拥有者请求每天其他服务器收到的伪造消息。

3.数据集

- 201401–201404，与Gmail SMTP通信记录
- 201504，Alexa前一百万域名的SMTP服务器配置快照。首先查询域名MX记录，之后向DNS查询邮件服务器支持的安全扩展，最后用ZMAP与服务器进行STARTTLS通信以确定服务器是否支持加密。79.2%的域名有邮件服务器。

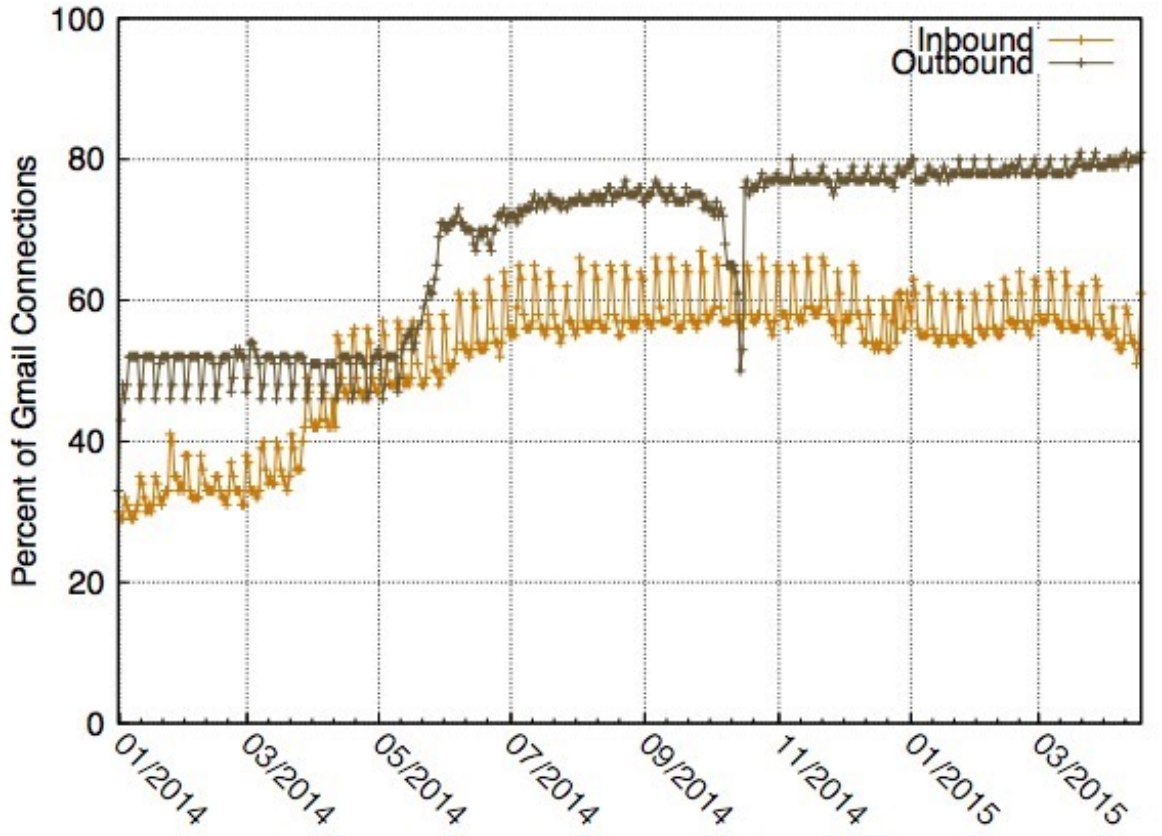
Status	Top Million Domains	
No MX records	152,944	(15.29%)
No resolvable MX hostnames	5,447	(0.55%)
No responding SMTP servers	49,125	(4.91%)
SMTP Server	792,494	(79.25%)

4. 实际中的机密性

研究实际中被STARTTLS保护的Gmail通信，以及支持和正确配置了加密的服务器比例。

4.1 Gmail加密情况

201401至201504，outbound从52%增长到80%，inbound从33%增长到60%，但并不是持续增长，而是爆发式增长



上图中Outbound在5月10日到30日之间有一个大增长，这是因为Yahoo和Outlook部署了STARTTLS，而10月8日到17日之间的大幅下跌，则是因为Poodle攻击爆发，在停用SSLv3时可能进行了误配置。

此外，使用加密的邮件服务器主要集中在主流的服务提供商那里，因此图中锯齿状的出现，有可能是因为在周末商务邮件较少，人们转而使用由主流服务提供商提供的个人账户。

20150430日流量分析得出的协商密码套件情况：84.2%的TLS连接选择了PFS密码套件，45.63%使用RC4

TLS Version	Key Exchange	Symmetric Cipher	HMAC	Inbound Traffic
TLSv1.2	ECDHE	AES-128-GCM	SHA-256	51.500%
TLSv1	ECDHE	RC4	SHA-1	29.225%
TLSv1	RSA	RC4	SHA-1	14.403%
TLSv1.2	ECDHE	AES-128	SHA-1	1.586%
TLSv1.2	RSA	RC4	SHA-1	1.147%
TLSv1	ECDHE	AES-128	SHA-1	0.999%
TLSv1.1	ECDHE	RC4	SHA-1	0.723%
TLSv1.2	RSA	AES-128-GCM	SHA-256	0.203%
SSLv3	RSA	RC4	SHA-1	0.060%
TLSv1.2	ECDHE	RC4	SHA-1	0.060%
TLSv1	RSA	AES-128	SHA-1	0.050%
TLSv1.1	RSA	RC4	SHA-1	0.024%
TLSv1.1	ECDHE	AES-128	SHA-1	0.011%
TLSv1.1	ECDHE	AES-256	SHA-1	0.004%
TLSv1.2	RSA	AES-256	SHA-1	0.003%
TLSv1.2	RSA	AES-128	SHA-1	0.001%
TLSv1	RSA	RC4	MD5	0.001%

4.2 服务器部署情况

81.8%的服务器支持STARTTLS，在TOP50的域名中，只有5个不支持：wikipedia.org, vk.com, weibo.com, yahoo.co.jp, 360.cn

RSA密钥长度，支持的密码套件，证书有效性情况

Status	Top Million Domains	
SMTP Server—No STARTTLS support	144,464	(18.2%)
SMTP Server—STARTTLS support	648,030	(81.8%)

Table 3: **STARTTLS Deployment by Top Million Domains**—Our scan results show that 79% of Alex Top Million domains have incoming SMTP servers, of which 81.8% support STARTTLS.

Mail Provider	Domains	STARTTLS	Trusted Certificate	Certificate Matches
Gmail	126,419 (15.9%)	Yes	Yes	server
GoDaddy	36,229 (4.6%)	Yes	Yes	server
Yandex	12,326 (1.6%)	Yes	Yes	server
QQ	11,295 (1.4%)	Yes	Yes	server
OVH	8,508 (1.1%)	Yes	Yes	mismatch
Other	597,717 (75.4%)	–	–	–

Table 4: **Top Mail Providers for Alexa Top Million Domains**—Five providers are used for mail transport by 25% of the Top Million domains. All five support STARTTLS for incoming mail.

	Matches Domain	Matches Server	Matches Neither
Trusted	4,602 (0.6%)	270,723 (34.2%)	143,113 (18.1%)
Untrusted	4,345 (0.6%)	21,057 (2.7%)	181,242 (22.9%)
Total	8,947 (1.1%)	291,780 (36.8%)	324,355 (41.0%)

Table 5: **Certificates for Top Million Domains**—While 52% of domains' SMTP servers present trusted certificates, only 34.2% of trusted certificates match the MX server, and only 0.6% are valid for the recipient domain.

4.3 软件实现

所有实现在STARTTLS失败时都是用明文（fail open to cleartext)。也就是说STARTTLS只提供机会加密（opptunistic encryption)

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					

Table 6: **Popular Mail Transfer Agents (MTA)**—We investigated the default behavior for five popular MTAs. By default, Postfix and qmail do not initiate STARTTLS connections. All five MTAs we tested fail open to cleartext if the STARTTLS connection fails.

5.机密性受到的威胁

5.1 STARTTLS失败（降级攻击）

Tunisia	96.13%	Reunion	9.28%
Iraq	25.61%	Belize	7.65%
Papua New Guinea	25.00%	Uzbekistan	6.93%
Nepal	24.29%	Bosnia and Herzegovina	6.50%
Kenya	24.13%	Togo	5.45%
Uganda	23.28%	Barbados	5.28%
Lesotho	20.25%	Swaziland	4.62%
Sierra Leone	13.41%	Denmark	3.69%
New Caledonia	10.13%	Nigeria	3.64%
Zambia	9.98%	Serbia	3.11%

Table 15: **Countries Affected by STARTTLS Stripping**—We measure the fraction of incoming Gmail messages that originate from the IPs that we found were stripping TLS from SMTP connections. Here, we show the countries with the most mail affected by STARTTLS stripping and the affected percentage of each country's incoming mail between April 20 and 27, 2015.

5.2 DNS劫持

伪造目的邮件服务器的dns记录。

作者在20150425扫描了整个ipv4地址空间10次，找到公开的解析器，并请求一些域名的MX和A记录，得到的结果如下。

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

Table 14: **Invalid or Falsified MX Records**—We scanned the IPv4 address space for DNS servers that provided incorrect entries for the MX servers for five popular mail providers.

Slovakia	0.08%
Romania	0.04%
Bulgaria	0.03%
India	0.02%
Israel	0.01%
Switzerland	0.01%
Poland	0.01%
Ukraine	0.01%

Table 16: **Countries Affected by Falsified DNS Records**—We measure the fraction of mail received by Gmail on May 21, 2015 from IP addresses pointed to by false Gmail DNS entries. Here, we show the breakdown of mail from each country that originates from one of these addresses for the countries with the most affected mail.

6. 实际中的认证性

Provider	SPF Policy	DMARC Policy
Gmail	soft fail	none
Yahoo	neutral	reject
Outlook	soft fail	none
iCloud	soft fail	none
Hushmail	soft fail	–
Lycos	soft fail	–
Mail.com	fail	–
Zoho	soft fail	–
Mail.ru	soft fail	none
AOL	soft fail	reject
QQ	soft fail	none
Me.com	soft fail	none
Facebook	fail	reject
GoDaddy	fail	none
Yandex	soft fail	–
OVH	neutral	–
Comcast	neutral	none
AT&T	–	–
Verizon	neutral	–

Table 17: **SPF and DMARC Policies**—The majority of popular mail providers we tested posted an SPF record, but only three used the "strict fail" policy. Even fewer providers posted a DMARC policy, of which only three used "strict reject."