International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

Email Spoofing & Backlashes

A. Ajina, Ujwal kumar

Abstract: ***The email service is a core platform for Mass communication as a consequence of which, it becomes central Target of all the social engineering and phishing attacks. As a consequence, attackers can try to impersonate or fake a trusted identity to carry out highly sophisticated and deceptive phishing attacks via Email Spoofing. In this work, we analyze: (1) how different Email providers detect and deal with such attacks? (2) Existing protection techniques and what is its scope of effectiveness? (3) Under Which conditions do spoofed emails reach inbox and its potential consequences? (4) Best practices and Adaptability apart from existing methods to remain secure. We address this concern by considering the parameters of top 25 email services (Used by more than billions of users) and also real world experiments. The existing protocols, security layers and the restrictions based on detection methods. The scale of implications by allowing the forged emails to enter the inbox despite getting detected by layers of SPF, DKIM, DMARC and ARC. The extent of problems caused in different paradigms, and the potential of having just SMTP implemented without any additional security layers within the domains. The impact of Misleading UI for allowed spoofed emails by providers is also discussed briefly. We observe the impression of security when users are caught off guard in real world testing on domains (eg. Gmail, Hotmail, Yahoo mail, etc) by simple platforms to spoof (eg. emkei.cz) apart from discussing the anomalous behavior of gmail as a response. We have conducted experiment to analyze behavior of top email domains against spoofed emails of various types.***

Keywords— Authenticity, email, Spoofing, Protocols, Vulnerability.

I. INTRODUCTION

Considering the fact that lots of development has taken place across all domains of cyber security. Humans form the weakest link in the chain, and in the current setup, no matter what kind of changes might be made, one factor will still remain a matter of worry, that is, Social engineering based attacks. Phishing attacks are very predominant, and Email based phishing forms a ground for such attack vectors. According to Statista, number of emails sent every day in 2018-2019 stands close to 293 billion [1], expected to grow to around 347 billion or more, per day, by 2023[1]. As per a study by PhishMe, 91% cyber-attacks start with a phishing mail [2]. Close to 43% of data breaches alone in 2018, was caused due to Social engineering attacks [3].

Manuscript published on 30 September 2019.
*Correspondence Author(s)
***A. Ajina,** Department of Computer Science and Engineering, Sir M. Visvesvaraya Institute of Technology, Bangalore, India. Email: ajinajaya@gmail.com,
Ujwal kumar, Department of Computer Science and Engineering, Sir M. Visvesvaraya Institute of Technology, Bangalore, India. Email: ujwalkrpro@gmail.com

Email Spoofing is a prominent step in phishing, where the attacker impersonates a trusted identity to gain the victims trust and then uses it to exploit it. Unfortunately, current email transfer protocol SMTP has no built-in methods to prevent spoofing, accredited to the fact that it was developed back in 1982 and not many security based modifications have been made [4]. It predominately relies on email providing domains to implement SMTP extensions like SPF, DKIM, DMARC, ARC and (EOP) to authenticate the sender. Adoption of these extra extensions is Voluntary due to which its adoption rate is relatively low and unsatisfying. Of the top 1,000 sites as ranked by Alexa on March 15th-2017, 75% had published SPF records and 22% had DMARC records – and a little over 19% had both [5].

Turning to the 10th 1,000 sites (again, those ranked between 9,001 and 10,000 by Alexa) only 54% had published SPF records and 4% had DMARC records, while only **3.5**% had both. The number of sites using only SPF was very similar between the two samples, 50% for the top 1,000 and 48% for the 10th 1,000. And in the latter sample, a full 45% of the sites appeared to not use email authentication at all (with the same caveat for DKIM) [5]. However, at the end of 2018, there were over 6,30,000 domains with valid DMARC records, which was around 250% surge in the DMARC policies across domains [6].

As per Bishop Fox, a global cybersecurity consulting firm, recently analyzed the Alexa top million Internet domains and analyzed that 98% – nearly the entire Internet – are potentially vulnerable to email spoofing [7,8]. There's a trade-off between delivering the mail or preferring the security and block the detected mail. There are always ambiguities about, would the spoofed mail be taken as a spam or not? Would they be blocked or delivered? Would they be delivered with a warning or without it? Would the UI make it look realistic and valid when delivered? Consider example of a spoofed email of Gmail to another Gmail account, the mail is delivered normally (Not considered as spam) but with a warning message due to the detection by the security extensions, it reads as, "This message may not have been sent by: *****@gmail.com ". Since each domain have their own set of policies, we treat each of them as a black box and do certain checks on each of them. In this paper, we describe our experience in verifying the effects of varying policies and implementations of security policies and protection against email spoofing. First, to understand how SMTP works? What are the loopholes due to which spoofing takes place? How exactly does the spoofing take place? Each methods of preventions and how exactly SPF, DKIM, DMARC and ARC works? And further countermeasures for the same.

II. WHAT IS SMTP & HOW IT WORKS?

A. *What is SMTP & How it Works?*

The Simple Mail Transfer Protocol (SMTP) is a communication protocol for mail transmission. As an Internet standard, SMTP was initially defined in 1982 by RFC 821, and later updated in 2008 by RFC 5321.

SMTP is an application layer protocol. Client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection conveniently. The SMTP server is endlessly on listening mode. As it listens or detects for a TCP connection from any of the client, the SMTP functioning initiates a connection on that port (25). Post successful establishment of the TCP connection the client process sends the mail instantly [9].

SMTP Protocol

The SMTP model can be of two types:

1. End to end method
2. Store and forward method

The end to end model is utilized to communicate between multiple different organizations, and the store and forward method is utilized within the organization. In our paradigm, we are interested in end to end model. A SMTP client which wants to send the mail will establish a contact with the destination's host SMTP directly with motive to send the mail to the destination address. The SMTP server confines the mail to itself until it successfully copies to the receiver's SMTP [9].

The client SMTP is the one which initiated the session, we term it as client- SMTP and the server SMTP responds/reacts to the session request and we term it as receiver-SMTP. The client- SMTP starts the session whereas the receiver-SMTP responds to the request accordingly [9].

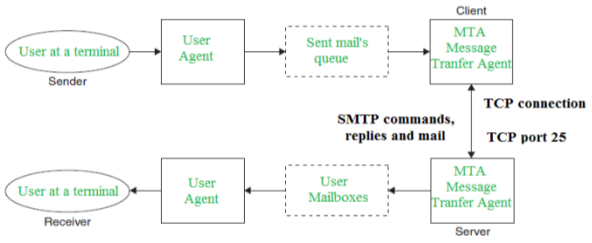

Figure 2.1 Functioning of SMTP

SMTP-client and MSTP-server both have 2 constituents:

1. User agent (UA)
2. Local MTA

Briefly, Senders and the user agent prepares the messages and further sends it to the MTA. The MTA's work is to transfer the mail across the network to the receivers MTA with ease.

B. *Security lapse in SMTP leading to spoofing (Loopholes)*

Though, there is a possibility that attackers might brute force login of SMTP servers. However, the Open port causes a major challenge and easy vulnerability to the hackers, SMTP uses the default port 25, generally. In other cases, the ISPs block this port themselves based on their policies or IDS configurations. Port 587 may be a better alternative [10-13]. As this port supports TLS encryption. Port 25 is a primary target for malware and spam. An attacker can break through open ports which can lead to hackers sending spam. Exposing port 25 to the internet can lead to a large amount of inbound spam. PHP scripts accomplishes the task of exploiting the above weaknesses with great efficiently. PHP scripts are explicitly used to make a connection to the SMTP server or MX servers. Connections to MX easily allows to bypass the ISPs as acting as the middle agent. This skips the mails from reaching ISPs SMTP servers. PHP Scripts exploits these features to inject spam to the recipient. This is achieved to avoid and nullify detection in MTA queues.

SMTP inherently does not check weather a certain IP is Authorized to send email from a particular given domain or not, or whether the IP is in list of sending domain or not. SMTP does not use even separate private and public keys to authorize the sender which can be checked by MTA. Lack of setting of poor policies and lazy implementation also pushes to further weaken the security and lead to convenient spoofing by the attackers.

C. *What is SPF? How it works?*

The sender policy framework (SPF) defines which email servers are actually authorized to send mails for the particular organization's Domain. It is the mail authentication technique which is used to prevent spammers from sending emails from your organizations domain. An SPF record is a DNS record that is added to DNS zone of the domain, in SPF record we can specify which hostname/IP address are authorized to send email from a particular specific domain. The mail receiver used a Return path header to identify the whereabouts of the email coming from. If the sending email server is not included in the SPF record of receiving domain then a suspicion can be detected and based on this either a warning message is received or email is blocked/rejected by the receiving server based on the policies. Briefly, every time a message is sent "Envelope from" to a receiving domain using SPF, the sender's domain address is checked in the DNS records, based on the SPF record, in response either the message is delivered if authentic, or delivered with a warning, or delivered but placed in spam or blocked. Entirely dependent on the policies of individual domains. However, there still remains major backlashes of SPF usage, Primarily, SPF doesn't validate the "From" header. This header is visible in most clients as the original sender of the message, instead uses the "envelope from" to find out about the sending domain, due to which issues may pertain and it can be subject to exploitation. Also, SPF will cease when the email is forwarded. Upon this instant, the 'forwarder' becomes a new 'sender' of the mail and fails the SPF checks which are performed by the new destination. If they are used alone, any other domain, which uses the same hosting provider, can still forge the mail of other domains, also there is no inherit mechanism to determine if the message was rejected or bounced. The SPF DNS TXT record typically looks something like

Retrieval Number: J93100881019/19©BEIESP
DOI: 10.35940/ijitee.J9310.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

<domain>.IN TXT "v=spf1 mx ~all"

where the tag v=spf1 represents SPF version 1 is currently available, the MX tag signifies which domains are authorized to send mail for the domain.

D. *What is DKIM? How it works?*

Domain keys identified mail is a mail authentication method that enables us to check whether a particular email was sent and authorized by the actual owner of that domain. DKIM is one of the two ways which DMARC used to link an email to a domain. Briefly, Sender attaches DKIM-signatures to email, the DKIM-signatures can be verified/authenticated by the mail receivers, and each signature contains everything needed to verify the signature. DKIM ensures that the message integrity or originality is preserved and not tampered with, apart from this, DKIM also can survive forwarding which ceases in SPF. A DKIM signature is created as, (a) All trivial parts of the email is boiled off (like removal of extra lines in front of the header, extra spaces, etc.), (b) Hashes are created of the email body and headers. (c)Sender has access to private key (Its matched with the public key which is available at the receiving end to obtain original contents). (d)The sender creates a crypto signature. (e)DKIM signature is added to the mail. (f)DKIM signature has everything to verify and further email is sent on its way. After receiving the email, the DKIM signature can be verified by the public key in the DNS by the receiving party. It used that key to decrypt the hash value to recalculate the hash value from the email it received, if these two DKIM values matches the MTA knows that the email contents haven't been modified, and this gives the user confirmation that it has been received from an authentic sender. In case where DKIM Check fails, the receivers still continue to process the email, as the email might be real but, Email was modified in transit, or the sender isn't attaching DKIM signatures to all emails or the email might be carrying fake signature, similarly there may be many other possible outcomes due to which DKIM check might fail.

E. *DMARC and its functioning*

Domain based Message authentication, reporting and conformance (DMARC) is a mail authentication protocol, and it creates a link between email and the domains effectively. SPF and DKIM are utilized to generate domain level identifiers, DMARC ties these outcomes to the 'FROM: header' of an email. The 'from: header' of the email is the domains policy key for DMARC. Both SPF and DKIM provide domain level identifiers as SPF is Path-based (RFC 7208) and DKIM is Signature based (RFC 6376), the former authorizes servers published in DNS and the latter requires crypto operations by email gateways. Both together empower DMARC and make it robust. "Identifier alignment" is the process of matching the results of SPF and DKIM to the DMARC's policy key- "From: header" domain. If there is any positive outcome by either SPF or DKIM, based on the policy its delivery is decided. DMARC record discovery works as, consider, receiver gets a piece of email with from: domain equal to INDIA.HIN.EXAMPLE.in. Receiver makes a DNS query for the TXT record at label: _dmarc.india.hin. example.in. The DMARC records are discovered in one of the two ways:

(a) Directly: _dmarc.india.hin. example.in

(b) If no DMARC record at exact location, checks at the organizational domain: _dmarc.example.in

More than 2 DNS queries doesn't happen even if the label is large.

Sample list of values/tag are, eg: v=DMARC1; p=none; rua=mailto:reports@example.in

Options are fairly simple, attributes are v(Protocol version), p(Policy for the domains), sp(Policy for the subdomains), pct(% of messages subject to policy), adkim(DKIM alignment mode), aspf(SPF alignment mode)m rua(Aggregate reporting URI), etc.

- DMARC Policies:

Receivers will enforce the policy against the unauthenticated mails, in one of 3 ways:

(a) None ("Monitor mode: doesn't impact the mails)

(b) Quarantine (Delivers to spam folder or equivalent)

(c) Reject (Rejects or blocks the email)

The "pct" tag allows for slow/delayed rollout:

(i)"pct=20" will mean "Apply the policy to 20% of unauthenticated emails"

(ii)If the policy is not applied due to the pct tag then next lesser or equivalent policy is applied.

F. *ARC and its Functioning*

Authenticated received chain (ARC) is a standard created in 2016 to help the fact on how SPF and DKIM results are passed from one mail server to the next during the process of forwarding. ARC effectively preserves the email authentication results over subsequent intermediaries that might modify the message and would cause email authentication measured to fail to verify when it reaches its final destination. If an ARC chain was to be present and validated, then the receiver who would discard the messages otherwise might choose to evaluate the ARC results and make an exception further allowing the messages from these indirect sources to be delivered normally, which the SPF would fail to authenticate otherwise. On a forensic note, forwarding causes a lot of DMARC failures, after the use of ARC, forwarding does not impact the results of DKIM or SPF and if we used reject policy for DMARC, the mail would now pass. Along with the ARC-Authentication-results(AAR) headers, two new headers are also passed along, namely, ARC-seal(AS) and the ARC-Message-Signature(AMS), and these two headers will allow the ARC chain to be validated as it is passed along. Its usage currently is very limited, but over time, as ARC supports DMARC the reports of the latter will look much better and accurate.

III. SPOOFING EXPERIMENTATION ACROSS VARIOUS PLATFORMS

There's a major challenge for domain providers to explicitly automate the process of choosing between the deliveries of the email compared to the authenticity of the sender and related security issues.

Retrieval Number: J93100881019/19©BEIESP
DOI: 10.35940/ijitee.J9310.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

A. *Experimentation setup*

We conduct spoofing across domains which are used by billions of users and are very popular providers. We ourselves created over 15 different email accounts. We had to set up an experimental server to send impersonated or forged mails to the receivers account, our server directly interacted with target mail server using SMTP and runs a Postfix mail service. We also used domains such as Emkei.cz, anonymousemail.me, anonymailer.net and spoof my email to ensure if it breaks through loopholes of SMTP and the spoof detection systems. By controlling the input mail (forged mail) and observing the response (receivers account), we evaluate the decision making process inside the target mail domain service. Each individual results of a particular domain stands independent of other domains.

Selection of target email providers was done purely on basis of magnitude of its usage and popularity among users along with their policy of claims of security and encryption. we find that over 75% emails are from 34 domains, we select top 12 of them which constitutes a major chunk of it.

B. *Parameters in consideration*

Senders address plays a crucial role and is a major stake holder in the process. We use three different Domains as a "FROM" end, of which we choose Gmail due to its advanced security methods which are supported by great detection methods as they are empowered by powerful Machine learning algorithms to detect if it's a normal message or a spam and if it's original or spoofed. Of course, along with pre-existing policies of SPF, DMARC where delivery seems to have upper hand. We then choose to Spoof from proton mail, due to its strict DMARC policies and powerful encryption and security claims. Further, we choose Excite.com as third domain attributing to its null implementation of SPF, DKIM and DMARC as of now.

Email content was primarily of 4 types, first, a blank message. Second, a generic email which looks original without using words which might evaluate it as spam and a URL attached to it. Third, a generic email as above along with an Attachment of word file with it. Fourth, we write a generic email as above and attach a phishing email to check if it's detected or not and record the responses to it.

Email receiver is evaluated based on the facts, if it's sent to inbox with warning, or sent to inbox without warning. Either if it's sent to spam with warning or if it's sent to spam box without warning. If the attachments sent is accessible or not, or downloadable or not. If the URL sent is clickable or it's only as a text form. Among the other factors we check how it is conceived by the web interface and the mobile app of the same domain (selective domains only). Another important fact is, we send only 12 to 20 emails to each domain with time gap of over few minutes between each emails, to ensure there is no disruption or any special exceptions as these numbers are very small compared to the magnitude of mail sharing that happens on these domains.

Table I
OBSERVATION ON SPOOFING

To \ From				**Spoof *gmail.com* (SPF/DKIM/DMARC/ARC)**				**Spoof *protonmail.com* (SPF/DKIM/DMARC=Strict)**				**Spoof *excite.com* (No SPF/DKIM/DMARC)**			
	SPF	**DK**	**DM**	**Blank**	**Gen URL**	**Gen Att**	**Phish**	**Blank**	**Gen URL**	**Gen Att**	**Phish**	**Blank**	**Gen URL**	**Gen Att**	**Phish**
Yahoo.com	✓	✓	✓	**S**	**S**	**S**	**S***(c)*	**S**	**S**	**S**	**S***(c)*	**S**	**S***(c)*	**S**	**S***(c)*
Outlook	✓	✓	✓	**S**	**S***(c)*	**S***(d)*	**S***(c)*	**S**	**S***(c)*	**S***(d)*	**S***(c)*	**S**	**S***(c)*	**S***(d)*	**S***(c)*
Gmail.com	✓	✓	✓	*<Anomalous behavior>*											
Aol.com	✓	✓	✓	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**S**	**0**	**0**	**0**
Rediffmail	✓	✓	✓	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Protonmail	✓	✓	✓	**S***(w)*	**S**(w)(c)	**S***(w)(d)*	**S***(w)*	**S***(w)*	**S***(w)(c)*	**S***(w)*	**S***(w)(d)*	**S**	**S***(c)*	**S**(d)	**S**
Fastmail.com	✓	✓	✓	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Seznam.cz	✓	✓	✓	**1**	**S***(w)(c)*	**1***(d)*	**1***(c)*	**S***(w)*	**S***(w)(c)*	**0**	**0**	**1**	**1***(c)*	**S***(w)(d)*	**S***(w)(c)*
Gmx.com	✓	✓	✗	**S**	**S***(c)*	**S***(d)*	**S***(c)*	**S**	**S***(c)*	**S***(d)*	**S***(c)*	**1**	**1***(c)*	**1***(d)*	**1***(c)*
Freemail.hu	✗	✗	✗	**1**	**0**	**0**	**S**	**1**	**0**	**0**	**S**	**1**	**1***(c)*	**1***(d)*	**1***(c)*
Zohomail.in	✓	✓	✗	**S***(w)*	**S***(w)*	**S***(w)*	**S***(w)*	**S***(w)*	**S***(w)*	**S***(w)*	**S***(w)*	**S***(w)*	**S***(w)*	**S***(w)*	**S***(w)*
Excite.com	✗	✗	✗	**1**	**1***(c)*	**1***(d)*	**1***(c)*	**1**	**1***(c)*	**1***(w)*	**1***(c)*	**1**	**1***(c)*	**1***(d)*	**1***(c)*

TABLE II
CONVERSION ON OBSERVATION (TABLE I)

0	***Blocked** without delivery*		**(W)**	*Warning served about the mail being spoofed or spam*
1	*Delivered to **inbox***		**(C)**	*Clickable link*
s	*Delivered to **Spam***		**(D)**	*Downloadable and Accessible attachment*

Retrieval Number: J93100881019/19©BEIESP
DOI: 10.35940/ijitee.J9310.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

*First three boxes indicate SPF (S), DKIM (DK), DMARC (DM), & gen URL represents generic mail along with URL, same applies to Gen Att, where generic mail is sent with an Attachment with it. 'Phish' stands for Message with a phishing link. *Google's anomalous response is addressed separately.	*To be noted that, wherever (W) isn't present, it clearly indicates warning not being served. On absence of (d) the attachment wasn't accessible or downloadable. Wherever (c) isn't present, it indicates that the URL was not clickable.

C. *Spoofing Experiment Observations*

Primarily we measure the authentication parameters of SPF, DKIM, DMARC of the "TO' and "FROM" providers. We explain how the mail providers handle the impersonated emails. We infer that when spoofed emails are sent to yahoo mail, it is directly sent to the spam folder in all the cases which we considered, but the important fact is, none of the emails showed any sort of warning of it being from an unauthorized sender, but none of the attachment was downloadable and if an attempt was made to download the same, it showed warning related to compromise of security. Similar point related to the URLs, where they were not clickable. We sent same emails from real senders which we impersonated with the same content, then the emails were normally delivered to the inbox, and the attachment was easily downloadable and URL was easily clickable without any issues or any sort of warnings. This explicitly shows that the security mechanisms are detecting the emails to be impersonated but there may be a larger trade-off to deliver the mail rather than blocking it.

From the observations made from Hotmail and outlook combined (outlook.live.com), we found that most emails were delivered to spam without any warnings or disability in downloading the attachments, but when same emails were sent by real senders, they were directed to inbox directly.

Gmail showed very anomalous behavior.

Rediffmail has rapidly scaled its delivery and security, across test conducted two years back, it did not have any security cue, compared to great implementation of SPF, DKIM, DMARC and ARC (rare) due to which every spoofed email was directly blocked.

Emails spoofed to GMX classified most messages as spam and the messages impersonated on behalf of excite was delivered normally to the inbox.

Spoofed emails to freemail.hu also showed mixed properties, few were sent to spam, few were delivered to inbox, and few were blocked before delivery.

Shezam.cz showed mixed properties, few messages were explicitly delivered to inbox without any warnings and looked original, upon which few were sent to spam folder and a warning was served, few attachments based emails and phishing emails were blocked too. However, for the mails impersonated on behalf of excite domain, all the four categories were delivered and warning was not served.

Fast mail exhibited blocking of all messages irrespective of criteria upon test of impersonation against any delivery.

Proton mail delivered every spoofed email, but explicitly in the spam folder with warnings of it to be fake or impersonated. However, the attachments were downloadable and URL was clickable. The image of warning is attached below.

Figure 4. Warning by Zohomail

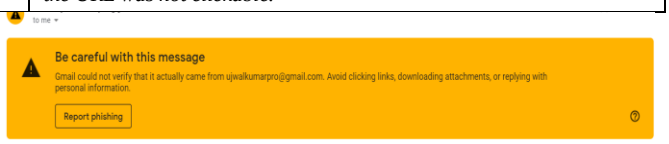

Figure 5a. Anomalous Response of Gmail

Figure 5b. Anomalous Response of Gmail

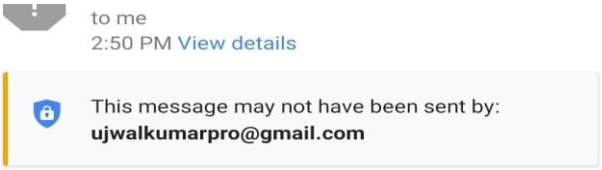

Figure 5c Anomalous Response of Gmail in Mobile app

Every time a spoofed mail was sent to Gmail, it showed varied responses. Primarily if a blank message was sent from one Gmail account to another Gmail account (Accessed via mobile UI), it was delivered to inbox normally with the warning as showed in Figure 5c but the UI did not support it, as the original account holder's photo wasn't displayed. If second spoofed email is sent via same address name, it is blocked and not delivered. We tried to send multiple emails (Span of breaks of few minutes) from same address but it was blocked after delivery of first message, when we send the spoofed emails after a gap of 5-6 hours from the same sender's address, it is delivered with a warning to inbox, but again subsequent messages are blocked if same senders address is used. However, if we use different senders address, it is delivered, but in the spam folder and warning of a different kind is served, such as Figure 5b. It's important to note that, first spoofed message is explicitly delivered, irrespective of being a blank message or a mail with attachment, but any subsequent mails are blocked against any delivery for some time span. Even if the second mail is a blank message without any threat, it is still blocked. This anomaly might be attributed to the powerful Machine learning algorithms which Gmail uses to ensure balance between security and delivery, which possibly other domains are yet to use. Extracting a clear picture of Gmail's policies in the black box setup becomes extremely difficult and we infer the fact that only first message may be delivered either to inbox or mostly to spam and further message from same address may be blocked for some time, other messages sent at that point might be identified as spam as well. However, the security mechanism of Gmail against spoofing is excellent even though the mails go through constant keyword checks.

D. *Countermeasures*

If the email providers decide to deliver the message to the users, we inherently believe that it is import to give an explicit warning to the users if not blocking it.

User awareness against increasing leverage of cyber-attacks is must. Implementation of security cue should be mandatory and it must act as a forcing function for sender to configure SPF/DKIM/DMARC/ARC correctly along with implementation of Spam and phishing detection systems which can be a threat vector. Another important aspect is to work on misleading UI (Such as "Profile photo" or "Email history") which might make the fake email look more real, which should be disabled if there is little chance of email being fake and yet delivered considering the importance of delivery of mails for the provider. Developers should also ensure that there can be a cryptographic transmission of messages and if anyone tries to spoof it via a third party domain, it becomes impossible for them to replicate the same and it gets detected. End to end encryption will be readily appreciated and can be a great solution to the existing problems where breach may happen mid-way.

IV. CONCLUSION

Across last 5 years, there have been several enhancements in implementation of security cues. It's been rapid and huge in magnitude, compared to implementation of SPF and DKIM over 5 years back to the current status, it has almost doubled and majority of email providers are now looking forward to provide a safe and secure environment against spoofing, spamming and phishing. Our work reveals the current picture of unauthorized delivery of emails and responses of top domains and their existing security extensions. With expectations of appropriate policy changes across email domains to ensure integrity and authenticity of the email content and check over valid sender's credentials. We have observed that in current scenario various domains have applied SPF, DMARC, but majority of them haven't understood the essence of appropriate policies and valid implementation, against which we hope that there is appropriate awareness of policies and consequences against poor implementation techniques. The extensions applied to SMTP to provide the extra dimension of security is gaining pace which is a great sign of development against the underlying everlasting unethical cyber-attacks.

ACKNOWLEDGEMENTS

This research was supported by Sir M. Visvesvaraya institute of technology. We want to thank everyone who supported us and motivated us during the course of the research. We also show the gratitude to everyone who reviewed and suggested insightful feedbacks. At last, we also want to motivate other readers of the work to carry out further research in numerous fields of cyber security and make Internet a safer & better place for everyone.

REFERENCES

1. J. CLEMENT, HTTPS://WWW.STATISTA.COM/STATISTICS/456500/DAILY-NUMBER-OF-E-MAILS-WORLDWIDE/
2. HTTPS://WWW.DARKREADING.COM/ENDPOINT/91--OF-CYBERATTACKS-START-WITH-A-PHISHING-EMAIL/D/D-ID/1327704
3. EITAN KATZ, HTTPS://BLOG.DASHLANE.COM/DATA-BREACH-STATISTICS-2018-FORECAST-EVERYTHING-YOU-NEED-TO-KNOW/
4. HTTPS://EN.WIKIPEDIA.ORG/WIKI/SIMPLE_MAIL_TRANSFER_PROTOCOL
5. HTTPS://DMARC.ORG/2015/04/TOP-ALEXA-WEBSITES-AND-EMAIL-AUTHENTICATION-PART-1/
6. HTTPS://DMARC.ORG/2019/02/DMARC-POLICIES-UP-250-IN-2018/
7. HTTP://DOMAININGAFRICA.COM/98PC-OF-TOP-1-MILLION-INTERNET-DOMAINS-MAY-VULNERABLE-EMAIL-SPOOFING/
8. HANG HU, GANG WANG, "END TO END MEASUREMENTS OF EMAIL SPOOFING ATTACKS", IN PROC OF USENIX SECURITY ,2018
9. HTTPS://WWW.GEEKSFORGEEKS.ORG/SIMPLE-MAIL-TRANSFER-PROTOCOL-SMTP/
10. HANG HU, GANG WANG, "REVISITING EMAIL SPOOFING ATTACKS", IN ARXIV :1801.00853V1, JAN 2018
11. ADRIEN RAULOT, "BYPASSING PHISHING PROTECTIONS WITH EMAIL AUTHENTICATIONS", IN UNIVERISTY OF AMSTERDAM, MASTER SECURITY AND NETWORK ENGINEERING, FEB 2019
12. SHAHRZAD SEDAGHAT, "CERT STRATEGY TO DEAL WITH PHISHING ATTACKS" IN ARXIV:1706.02610
13. HANG HU, PENG PENG, GANG WANG, "TOWARDS THE ADOPTIONS OF ANTI-SPOOFING PROTOCOLS" IN ARXIV 1711.06654, FEB 2018.

AUTHORS PROFILE

A. Ajina Completed her B.E degree in Computer Science and Engineering from Manonmaniam Sundaranar University, Tirunelveli in 2004. In 2008 she joined for M.E in Computer Science and Engineering from Anna University, Coimbatore. She is extremely passionate about Wireless sensor networks, Network Security and Machine Learning. A.Ajina, has a vast experience of 14 Years in academics. She has published 6 paper in various Scientific Journal and presented 15 papers in various scientific National and International conference/workshops.

Ujwal kumar is a student pursuing Undergrad in Computer science engineering. He is extremely passionate about Cyber security and machine learning. Apart from research in ML-Sec, he is extremely interested in hunting for bugs in various bug bounty programs, as he is placed in hall of fame of various programs. He is also a voracious reader and is very fond of taking part in various parliamentary debates. Other areas of interest include Economics, Philosophy, History, Polity and Spirituality. He is also a part time speaker, and has addressed thousands of people across various computer science based topics. He is also involved with NGOs which work for social causes across underprivileged rural areas.