DMARC – An Incomplete Journey!!

– **Venkata Satish Guttula**
Director of Security, Rediff.com India Ltd, venkatas@rediff-inc.com

With Digital India Campaign launched by the Government of India, apart from private services, more and more Government services are becoming digitalized, and almost all of them require Email address by the customer to avail these services. Email became a vital tool in our daily lives. But when email was created, just like the internet, security was never thought of and never a part of the email system.

Introduction

This lack of security in the email system gave rise to many security issues like spreading of malware, open-relay, which was used to spam and most dangerous of them - Email Spoofing.

Email Spoofing is a method where the sender makes it appear that the message originated from someone or somewhere and not from the actual source. Email Spoofing is a popular method used in phishing and spam campaigns because unsuspecting people will open emails thinking that they came from known or reliable sources.

According to a 2016 report, around $2.3 billion were lost phishing at least as many cases were not detected or reported to the authorities.

To fight email spoofing, a group of leading organizations came together to collaborate on a method to combat email spoofing at internet-scale. The primary mission was two-fold:

- Enable senders to publish easily discoverable policies on unauthenticated email
- Enable receivers to provide authentication reporting to senders so that they can improve and monitor their authentication infrastructure

Their common goal was to develop an operational specification, with the desire that it would be able to achieve formal standards status. The result was DMARC - Domain-based Message Authentication, Reporting and Conformance an email authentication protocol.

DMARC is widely implemented by banks and other financial institutions in India with encouragement from RBI in terms of guidelines. Organisations must enable SPF and DKIM for all the emails which originate from their servers and also set up DMARC policies in their domain DNS so that when these emails are received by the customers' email providers, they are checked for DMARC and take action according to the policy set in the DNS when the email fails DMARC. The policy can be either none – when they are in the initial stages of setup, quarantine – when they are in the final stages of the setup and reject – the final policy when DMARC is fully implemented.

Email providers like Gmail, Yahoo, Rediff honor DMARC when they are receiving emails, but the problem is many financial organizations and big organizations who have inhouse email setup and organizations who host have their email with other small email hosting providers not honorDMARC for their inbound emails, and so leaves them vulnerable to email spoofing. CEO Fraud or Business Email Compromise is one of the biggest Email spoofings where banks, corporates are falling prey losing billions of dollars, and they are not protected with the solution created to prevent this. Many opensource software, startups help the organizations implement DMARC for their outbound emails, but there is little information to implement DMARC for inbound emails. DMARC is also promoted as a brand reputation tool and not as a solution to prevent email spoofing.

Thus, the journey of DMARC is incomplete, and the regulators, corporates, banks all have to wake up to the dangers of Email Spoofing and implement DMARC for their inbound emails also not just for outbound emails.

Venkata Satish Guttula has over 19 years of experience in Information Technology. He has been part of core Rediff team for past 14 years and handled multiple projects. Having a flair for information security he started implementing security in the projects.

Currently he is heading Information Security in Rediff.com playing a crucial role in implementing and practicing information security. He is a speaker in many of conferences speaking on Incident Response, Ransomware, Datacenter Security, Zero Trust architecture, DevSecOps etc.

He is also an the Academic Board member for Welingkar's E-Business PGDM program .

He received CISO Platform 100 India's top IT Security influencer and community contributor award in 2018 and 2019, Award in the Data Security Category in the Datacenter Summits and Awards and Cybr Sentilel Award in 2019.

venkatas@rediff-inc.com