ABSTRACT

The continuous and exponentially increasing use of email as the primary means of communication between two parties is also increasing risk to the involved parties due to the easily possible attacks on the email system. The core of the whole email system depends on the SMTP protocol, which came into existence only after the 1980s. At the time of the development of SMTP, present-day highly computational security attacks couldn't have been considered, which resulted in the security loophole in the present email system.

In today's world, email (or electronic mail) has become one of the most widely used means of communication, whether one-to-one or broadcast, including personal and professional work. Email has been a cost-efficient tool for information sharing and communication. With the increasing use of technology and internet usage among users, the number of daily emails is growing exponentially. It is estimated that more than 300 billion e-mails are expected to be communicated each day in the year 2020. Also, the number of emails sent daily will be more than 370 billion by 2025.

Email spoofing is an attack in which an attacker sends an email modified to seem as if it originated from a different trusted source other than the original sender. Email spoofing is a widespread attack used in spam campaigns and phishing attacks, as a user gets confidence that the email comes from a genuine sender. The primary purpose of email spoofing is to trick recipients into opening or responding to the email sent from a spoofed sender. Email spoofing aims to trick users into believing that the email has come from some person that they know or someone whom they can trust. Once the recipient is convinced about the email's sender, the attacker asks about some information that he can misuse in some way.

In my PhD research, we study the working and effectiveness of various anti-spoofing protocols in present-day email systems like SPF, DKIM and DMARC and work to propose a much more effective way to countermeasure the problem of spoofing of email.