Verifications for Email Systems

Can Taylan Çapraz, 36493

A. Introduction

In mail systems, there would be email spoofing attacks that manipulates content or sender of the email. In this type of attack, receiver thinks that an email is coming from a trusted server although mail is sent from malicious people. Thus, verification is necessary for email to avoid email spoofing attacks. There are many methods to verify if origin of the email is manipulated. DKIM and S/MIME are two of these verification methods.

B. Mechanisms Used to Verify Emails

1. DKIM

DKIM (DomainKeys Identified Mail) is a cryptographic method to detect if the origin of the mail is manipulated. In sender server, public and private keys are generated. Private key is kept in email server while public key is published in a DNS txt record. When an email is sent, server generates a digital signature using private key and inserts this signature to messages. In receiver server, receiver obtains the public key from DNS system and verifies the digital signature using the public key. If mail is not verified, email system would delete this mail or it would give warning. [2]

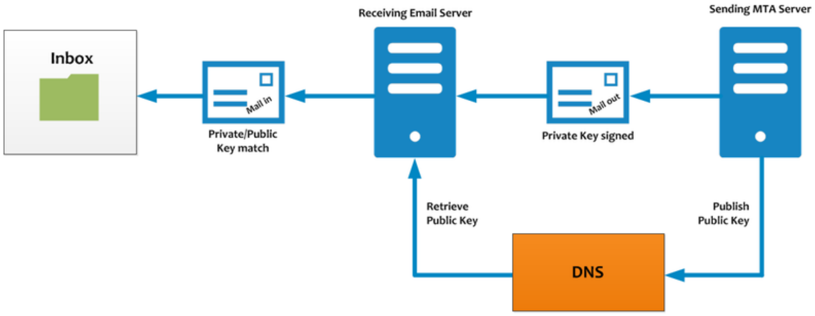

Figure 1: Working Mechanism of DKIM

2. S/MIME

S/Mime (Secure/Multipurpose Internet Mail Extensions) is another cryptographic mechanism that protect emails from unauthorized read and prevent email spoofing. It is based on asymmetric cryptography. Sender and receiver shares a secret key for encryption and decryption. Sender both signed and encrypted the email and sends it. Since it is encrypted, nobody who doesn't have secret key can read mail content. Then, receiver decrypt email using private key and verify it using a public key.

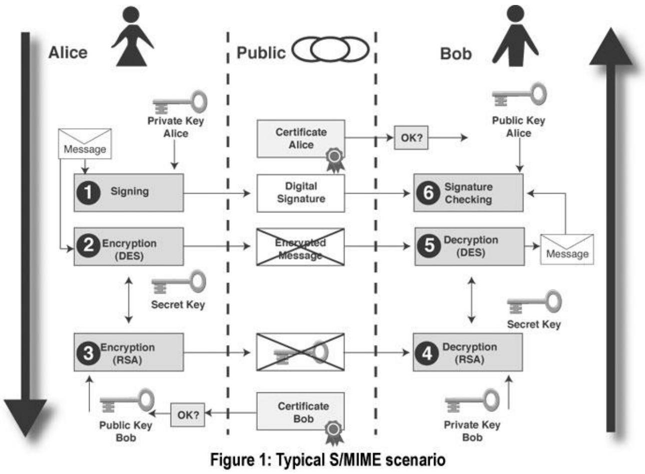

Figure 2: Working Mechanism of S/MIME

C. DKIM and S/MIME Against DNS Cache Poisoning Attack

DNS cache poisoning attack is a type of attack that corrupts DNS data. This type of attack can deceive email server if mail server verifies email using DKIM. The reason for that is DKIM obtains public key to verify email from DNS server. However, S/MIME provides security against DNS cache poisoning attack since it uses private key, both sender and receiver hold, to verify email. This private key is shared via secure channel and is not effected from DNS poisoning attacks.

D. Modification Makes DKIM Secure Against DNS Cache Poisoning

An attacker can modify public key in DNS server with DNS Cache Poisoning Attack and send email with fake sender address. Since public key is changed by attacker, mail server cannot detect email spoofing and verify email. DKIM would be modified to protect from DNS poisoning attack. There are many possible solution increases security.

Solution 1: One of the possible solution for this is holding public key in DNS server in encrypted form. Sender and receiver can share a secret key. Public key can be encrypted using the secret key and receiver can decrypt this key using the secret key. In this method, attacker cannot produce decrypted version of his public key, so receiver doesn’t verify fake email.

Solution 2: One of the other solution is using secure DNS server to keep public key in secure. DNSSEC is a secure DNS server uses digital signatures signed with trusted certificate. DNSSEC uses this certificate to check authenticity for new data.

Solution 3: In addition to first two solution, public key can be hold in another trusted server. Mail server request public key from both trusted server and DNS server. If public keys obtained from trusted server and DNS server matches, mail server will assume that there is no modification in public key. If they are not matched, receiver would be warned.

E. CONCLUSION

In conclusion, DKIM is an easy technic to defend email spoofing that doesn’t need a lot of keys to verify emails. Receiver only need one public key to verify email. However, DKIM is not able to detect if there is a DNS cache poisoning attack since it keeps the public key used to verify email in DNS server. S/MIME can detect if there is a DNS cache poisoning attack. However, sender and receiver needs to keep private, public and secret key. However, it provides more secure systems. DKIM can also be modified to detect email spoofing attack even if there is a DNS spoofing attack. There are many ways such as holding public key in encrypted packet in DNS server, using DNSSEC which uses trusted certificates to defend DNS poisoning, and comparing public key with the version of public key which is hold in another trusted server.

F. References

[1] "DomainKeys Identified Mail (DKIM)," DomainKeys Identified Mail (DKIM). [Online]. Available: http://www.dkim.org/. [Accessed: 18-Apr-2017].

[2] "DKIM - How it Works," DKIM - How it Works. [Online]. Available: https://www.icewarp.com/support/online_help/341.htm. [Accessed: 18-Apr-2017].

[3] Bondesson R. Deployment and analysis of DKIM with DNSSEC. [serial online]. 2008;Available from: Networked Digital Library of Theses & Dissertations, Ipswich, MA. Accessed April 18, 2017.

[4] DNS Protection against Spoofing and Poisoning Attacks. 2016 3Rd International Conference On Information Science And Control Engineering (ICISCE), Information Science And Control Engineering (ICISCE), 2016 3Rd International Conference On, Icisce [serial online]. 2016;:1308. Available from: IEEE Xplore Digital Library, Ipswich, MA. Accessed April 18, 2017.

Figure 1) J. C. Mingo, "Best Practices on Email Protection: SPF, DKIM and DMARC," Best Practices on Email Protection: SPF, DKIM and DMARC - Zimbra :: Tech Center. [Online]. Available: https://wiki.zimbra.com/wiki/Best_Practices_on_Email_Protection:_SPF,_DKIM_and_DMARC. [Accessed: 18-Apr-2017].

Figure 2) J. D. Clercq, "Secure Email with S/MIME," Security content from Windows IT Pro. [Online]. Available: http://windowsitpro.com/security/secure-email-smime. [Accessed: 18-Apr-2017].