March 2022

REMOTE ATTESTATION TO ENHANCE EMAIL SECURITY

NIRANJAN M M

REMOTE ATTESTATION TO ENHANCE EMAIL SECURITY

AUTHOR:
NIRANJAN M M

ABSTRACT

According to the data collected from 2013, impostor email attack/threads/scam has siphoned more than $2.3 billion from more than 17,000 victims. Impostor email attacks succeed as they look and feel legitimate, they do not include malicious link or malware attachments, and they do not arrive in high enough volumes to raise red flags in most anti-spam tools. Hence, impostor emails can evade solutions that look for only malicious content or behaviour. Detection of these emails is a major challenge for email security providers as well as difficult to recognise these emails by the end user (when sent from look-alike domains, having valid Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting & Conformance (DMARC) records). There are techniques which uses methods such as dynamically analysing the attributes of all emails as it arrives and detect anomalies that point to an impostor, but they are not fool proof. The technique presented herein propose method to use remote attestation for providing trustworthiness to the emails exchanged between sender and recipient, hence preventing impostor attacks/frauds.

DETAILED DESCRIPTION

According to the FBI's Internet Crime Complaint Canter (IC3), impostor email attacks/threats/scam has siphoned more than $2.3 billion from more than 17,000 victims, after they started tracking these types of scams from 2013 (and these are just reported incidents). Many messages will be quickly recognised by recipients as phishing and discarded, but the small few that succeed can yield millions of dollars in fraudulent transfers. Impostor email attacks succeed as,

· They look and feel legitimate.
· They do not include a malicious link or malware attachments.
· They do not arrive in high enough volumes to raise red flags in most anti-spam tools.

Impostor emails have grown to target companies both large and small in every part of the world. They constitute for mainly two types of frauds:

- Supply Chain Fraud (when an attacker can take over the legitimate email account of a trusted third-party supplier, they can get a big return without ever interacting with a C-level executive).
- CEO fraud (also known as business email fraud).

Here is a small sampling of recent impostor attacks during the last few years:

• A Hong Kong subsidiary at Ubiquiti Networks, Inc. discovered that it had made more than $45 million in payments over an extended period to attackers using impostor emails to pose as a supplier.

• Crelan, a Belgian bank recently lost more than $70 million due to impostor emails, discovering the fraud only after the company conducted an internal audit.

• In New Zealand, a higher education provider, TWoA, lost more than $100,000 when their CFO fell victim to an impostor email, believing the payment request came from the organization's president.
• Luminant Corp., an electric utility company in Dallas, Texas sent a little over $98,000 in response to an email request that they thought was coming from a company executive. Later it was learned that attackers sent an impostor email from a domain name with just two letters transposed.

As these threats do not use malicious attachments or URLs, impostor emails can evade solutions that look for only malicious content or behaviour. Hence detection of these emails is a major challenge for email security providers as well as difficult to recognise these emails by the end user (when sent from look-alike domains, having valid Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting & Conformance (DMARC) records).
There are techniques which uses methods such as dynamically analyzing the attributes of all emails as it arrives and detect anomalies that point to an impostor, but they are not fool proof.
Following are few types of impostor email threats:

- Spoofed Name: The name of the spoofed executive in the "From" field. But the email address is an outside email account that belongs to the attacker. This is around 21%.
- Reply-To Spoofing: The "From" name, address field and reply-to name are the real ones of the executive being impersonated. But the "Reply-to" address is that of imposter's. This is around 75%.
- Spoofed Sender (with no reply-to address): The impostor email uses the name and email address of the spoofed executive. But the email does not contain a "Reply-to" address. This is around 2%.
- Lookalike Domain: The attacker's "From" address is close enough in appearance to the impersonated executive's to fool busy recipients. This is around 2%.

Detection of such impostor emails is a challenge for email security providers, as these emails does not contain malware, may not contain attachments and no hyper-links. These are low in volume, targeted to specific user and hand crafted, hence it is very difficult to detect. There are authentication methods such as DMARC, SPF and DKIM can prevent domain spoofing, but authentication can be difficult and may end up blocking legitimate email.

The technique presented herein propose method to use remote attestation for providing trustworthiness to the emails exchanged between sender and recipient, hence preventing impostor attacks/frauds.
Few Definitions:

- Sender/Recipient: The sender or recipient can be an email client, Secure Email Gateway (SEG), Mailbox Connectors (MC) (or mailbox solutions).
- Remote Attester: Remote attester is responsible for establishing trust between sender and recipient by generating unique attestation token for every email at the sender side and validating the attestation token at the recipient side. The recipient of an impostor attacks always receives mails from impostor (spoofed trusted users) i.e., users from the same organisation or trusted organisation or partner organisation). Hence remote attester can be deployed in an organization enterprise network or on cloud or service offered by multi-tenant service provider.

As per this method, remote attester is used to generate attestation token for each email using metadata (email header) sent by the Sender and later it would be validated by the recipient.

Figure-1 describe remote attestation method for enhancing email security.

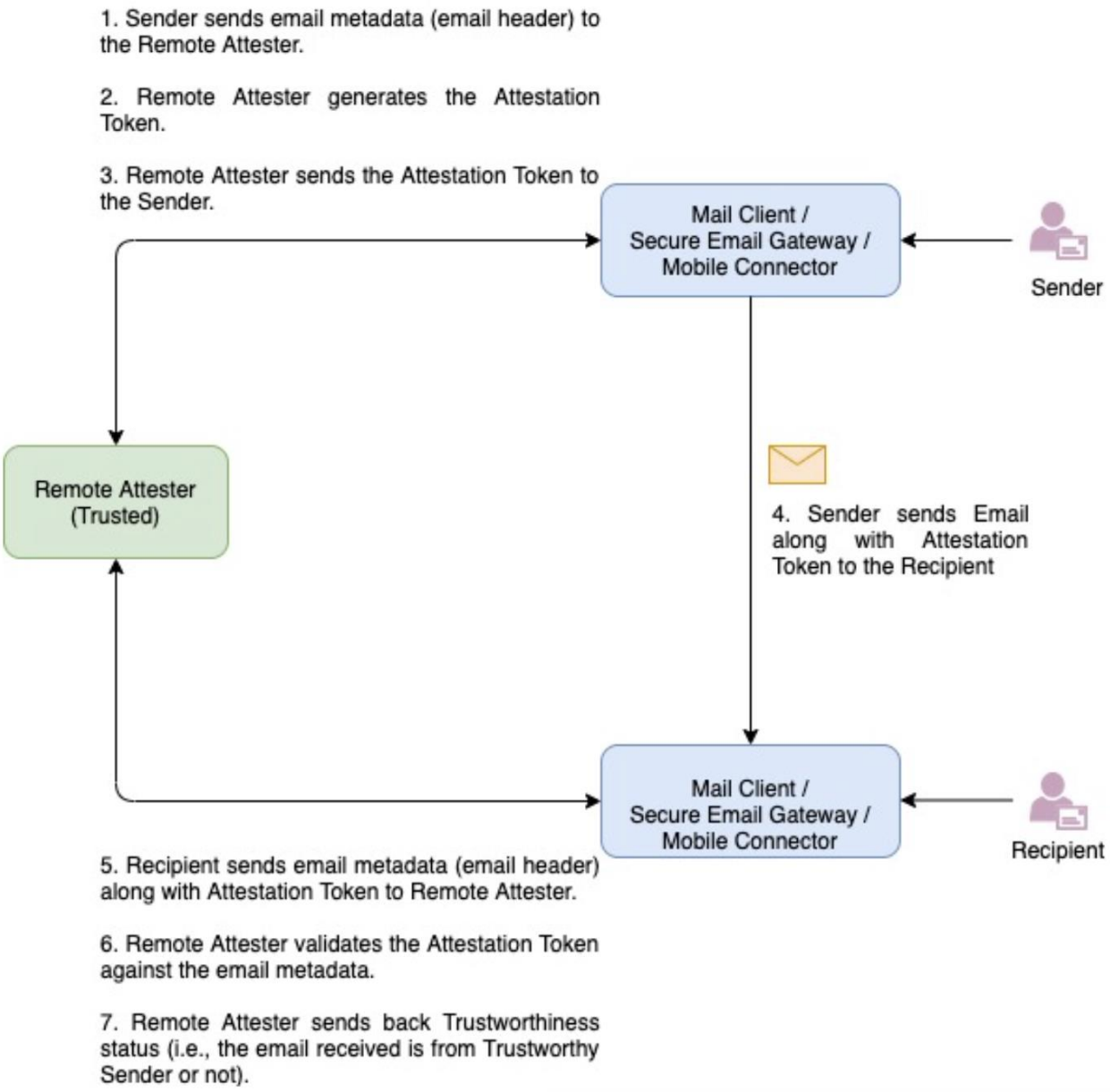

Figure-1

The technique presented herein is explained with the following steps:

- Mail clients or Secure Email Gateway or Mailbox Connector (both sender and recipient) registers with the remote attester.
- Sender sends mail header (metadata) of every email to the remote attester before sending to the recipient.
- Remote attester generates attestation token using metadata for every email.

- Remote attester returns the attestation token to the sender.
- Sender includes the attestation token in the email headers.
- Sender sends the email to the recipient.
- Upon receiving the email, it sends the mail header (metadata) along with attestation token to the remote attester.
- Remote attester validates the attestation token against the metadata.
- Remote attester returns 'whether sender is trustworthy or not' to the recipient.

If the recipient is a Secure Email Gateway or Mailbox Connector, then the un-trusted mail will be dropped and not delivered to the end user (based on the configurable policy). If the recipient is a mail client, then the mail is not presented to the mail until it gets the response from the remote attester. Upon getting the response from the remote attester, action is taken to drop or present the email to the mail client (based on the configurable policy).

The technique presented herein uses simple remote attestation method to prevent impostor attacks/frauds to enhance email security with respect to supply chain and CEO frauds. As per this method, remote attester generates attestation token for each email using metadata (email header) and validates that email sender is trustworthy or not.