UTA   R. Mukhia
Internet-Draft   B. Rajendran
Intended status: Standards Track   BS. Bindhumadhava
Expires: December 12, 2019   CDAC Bangalore
                                                           June 10, 2019

An approach for end-to-end Email Security with DANE and DMARC
draft-smtp-dane-dmarc-00

Abstract

An end-to-end email security solution is proposed by implementing both DANE and DMARC protocols. DMARC enables the recipient's mail server, with a method to verify the sender's ingenuity. DANE intends to mitigate the MITM attack, by enabling the sender a method to authenticate the recipient's mail domain. DANE and DMARC therefore complement each other by allowing the sender to verify the recipient's domain, and the recipient to verify the sender's address respectively.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction 2
2. Architecture of DANE with DAMRC for secure Email 3
3. IANA Considerations 5
4. Security Considerations 5
5. Normative References 7
Authors' Addresses 7

1. Introduction

SMTP is a hop-by-hop mechanism. For a long time now, email servers have had the option of using TLS to transparently encrypt the message transmission from one server to other. Use of TLS with SMTP,when available ensures that the message content are secured during transmission between the servers.But not all servers support TLS.Some of the reasons many email providers doesn't support TLS are

1. Purchase of one or more SSL certificates is not done

2. Configuration of the email servers to use them (and keep these configurations updated)is not done

3. Allocation of additional computational resources on the email servers is not involved

There are some issues from sending computers or servers also like, They never use TLS or They use TLS if receiver side is also using it otherwise sends insecurely or They use TLS otherwise doesn't deliver at all.

Now comes the point that actually how secure is SMTP TLS.TLS protects the transmission of the content of the email messages,but it doesn't do anything for protecting the security of the message before it is sent or after it arrives at its destination .And for that, other encryption mechanisms are required.There are many reasons to say SMTP TLS doesn't provide end-to-end security.As there is no mandatory support for SSL/TLS in the email system.

A receiver's support of the SMTP TLS can be removed by a Man-in-the-middle. In such cases opportunistic TLS will deliver messages securely and forced TLS will not deliver the message.If any aspect of the TLS negotiation is garbled,then encryption is not used. It is

very easy for a man-in-the-middle to inject garbage into the TLS handshake(which is done in clear text) and have the connection downgraded to plain text(opportunistic TLS) or have the connection forced(forced TLS).Even when the SMTP TLS is offered and accepted,the certificate presented during the TLS handshake is usually not checked to see if it is really for the expected domain and unexpired.Most MTA's offer self signed certificates, therefore in many cases one has an encrypted channel to an unauthenticated MTA, which can only prevent passive eavesdropping.

To mitigate the mentioned problems with SMTP TLS, DANE and DMARC can be used with SMTP.DANE prevents middle man by giving sender a method secured using DNSSEC,it ensures that message goes only to the receiver.This is done when key provided by receiver's mail exchanges matches with the key he has authorized in DNS to receive mail for his domain.

Phishing is a very common type of threat,it can be avoided if DMARC is implemented, as both DKIM and SPF are part of DMARC.It is job of DKIM to authenticate the domain that affixed the signature of the message.Therefore DMARC intends to mitigate the threat of arbitrary sender.

As we know,SMTP is not designed keeping sender in mind,attacker can easily connect to receiver's mail server and send him email appearing to be coming from sender.In this case,DMARC provides the solution by giving receiver mail server a method to verify that the sender is genuine and this is done via two methods either via cryptographic signature using DKIM or via IP ACL using SPF.So DANE and DMARC are complimentary to each other, DANE ensures that the correct receiver receives the message while the messages are correctly encrypted in the transit and DMARC makes sure that messages are coming from legitimate sender.

2. Architecture of DANE with DAMRC for secure Email

1. The sender creates a message.

2. SHA-256 is used to generate a 256-bit message digest of the message. The combination of SHA-256 and RSA provides an effective digital signature scheme. Because of the strength of RSA, the recipient is assured that only the possessor of the matching private key could have generated the signature. Because of the strength of SHA-256, the recipient is assured that no one else could generate a new message that matches the hash code and, hence, the signature of the original message.

3. The message digest is encrypted with RSA using the sender's private key, and the result is appended to the message.

4. DNS Based Authentication of Named Entities(DANE) offers the option to use the DNSSEC infrastructure to store and sign keys an certificates that are used by TLS. This is to avoid a condition when many number of CA's are compromised then the attacker can obtain the private key of the CA, issues certificates under a false name, or introduce new bogus root certificates into a root certificate store.There is no limitation of scope for the global PKI, and a compromise of a single CA can damage the integrity of the entire PKI system.

5. Domain Keys Identified Mail (DKIM) permits a person,role,or organization that owns the signing domain to claim some responsibility for a message by associating the domain with the message.The domain can be an author's organization,an operational relay,or one of their agents.Responsibility is validated through a cryptographic signature and by querying the signer's domain directly to retrieve the appropriate public key which is provided to the receiving MTA.

6. DMARC works with SPF and DKIM.SPF enables senders to advise receivers, via DNS, whether mail purporting to come from the sender is valid, and whether it should be delivered, flagged, or discarded. DKIM authenticates the domain that affixed a signature to the message. SPF focuses on the SMTP envelope. DMARC requires that the From address match (be aligned with) an Authenticated Identifier from DKIM or SPF. In the case of DKIM, the match is made between the DKIM signing domain and the From domain. In the case of SPF, the match is between the SPF-authenticated domain and the From domain.

7. Signature is then passed onto the receiving MTA then to the MUA and following steps take place.

8. TLSA, DNS record type, which can be used for a secure method of authenticating Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates. The TLSA provides for:

    1. Specifying constraints on which CA can vouch for a certificate, or which specific PKI end-entity certificate is valid.

    2. Specifying that a service certificate or a CA can be directly authenticated in the DNS itself

The TLSA RR enables certificate issue and delivery to be tied to a given domain. A server domain owner creates a TLSA resource record that identifies the certificate and its public key. When a client receives an X.509 certificate in the TLS negotiation, it looks up the TLSA RR for that domain and matches the TLSA data against the certificate as part of the client's certificate validation procedure.

9.   The receiver uses RSA with its private key to decrypt and recover the content-encryption key.

10. The content-encryption key is used to decrypt the message.

3. IANA Considerations

This memo includes no request to IANA.

4. Security Considerations

The security of the DNS RRtype relies on the security of DNSSEC to verify that the TLSA record has not been altered. A better design for authenticating DNS would be to have the same level of authentication used for all DNS additions and changes for a particular domain name.DNSSEC forms certificates(the binding of an identity to a key) by combining a DNSKey,DS or DLV resource record with an associate RRSIG record.These records then form a signing chain extending from the clients trust anchors to the RR of interest. The risk that a given certificate that has a valid signing chaining fake is related to the number of keys that can contribute to the validation of the certificate the quality of protection each private key receives,the value of each key to an attacker and the value of falsifying the certificate.

DNSSEC allows any set of domains to be configured as trust anchors and/or DLVs, but most clients are likely to use the root zone as their only trust anchor.Also because a given DNSKey can only sign resources record for that zone,the number of private keys capable of compromising a given TLSA resource record and the nearest trust anchor,plus any configured DLV Domains.Typically this will be six keys,half of which will be KSKs. KSK is stored off-line and protected more carefully than the ZSK,but not all the domains do so. The Security applied to a zone's DNSKey should be proportional to the value of domain,but that is difficult to estimate.For Example the root DNSKey has protections and controls comparable to or exceeding those of public CAs.On the other hand,small domain might provide no more protection to their keys than they do to their other data.DNSKey are limited in what they can sign ,so a compromise of the DNSKey for"example.com" provides no avenue of attack against

"example.org".Therefore the impact of a compromise of.Com's DNSKey ,while considerable would be limited t .com domains.

Public CAs are not typically constrained in what names they can sign and therefore a compromise of even one CA allows the attacker to generate a certificate for any name in the DNS. Since TLSA certificate association is constrained to it's associated name,protocol and port,the PKIX certificate is similarly constrained,even if it's public CAs signing the certificate(if any) or not.If public CA is compromised,only the victim will see the fraudulent certificate.Implementation of DANE rely heavily on the DNS ,and therefore is prone to security attacks based on the deli berate mis-association of TLSA records and DNS names.The connection between TLSA records and DNS name should rely on DNS resolver,rather than depending on caching result of previous domain name lookups ,also it should depend on the TTL of that lookup,if it is more then only the information will be useful otherwise not.If this part is not taken care of then it can fall the victim of spoofing,having access denied when a previously accessed servers TLSA record changes,such as during a certificate rollover.Even with secure communications between a host and the external validating resolver,there is a risk that the external validator could become compromised.Nothing prevents a compromised external DNSSEC validator from claiming that all the records it provides are secure,even is the data is falsified unless the client checks the DNSSEC data itself.For this reason DNSSEC validation is best performed, on-host even when a secure path to an external validator is available.

In DMARC, URI is a format by which a domain owner specifies the destination for the two report types that are supported.Receivers may impose a limit on the number of URIs to which they will send reports,they must support the ability to send to at least two.DMARC and it's underlying techniques SPF and DKIM depend on the security of the DNS.To avois DNS-based exploits,the deployment of DNSSEC should be done parallel with the deployment of DMARC by both domain owners and mail receivers. A common attack in messaging abuse is the presentation of false information in the display name portion of the "FROM" field.This takes place when it is possible for the email address in that field to be an arbitrary address or domain name,while containing a well known name(a celebrity,company,eole etc.) in the display name to fool th receiver. This attack is based on the habit of common MUAs that they show the display name and not the email address when both are available. If email address is found with display name,execute the DMARC mechanism of the domain name found there rather than the domain name discovered before.but spoofers can cause the attack by simply not using an email address in the display name ,So this doesn't solve the problem.In the MUA display name should be shown only if the DMARC mechanism succeeds. This is also

easily defeated,the attacker can use another domain name in the display name to pass the DMARC Test.In the MUA,the display name should be shown if the DMARC mechanism passes and the email address thus validated matches one found in the receiving user's list of known addresses.

5. Normative References

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, DOI 10.17487/RFC6698, August 2012, <https://www.rfc-editor.org/info/rfc6698>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

Authors' Addresses

Ranjana
CDAC Bangalore
Bangalore
India

Email: ranjana@cdac.in

Balaji Rajendran
CDAC Bangalore
Bangalore
India

Email: balaji@cdac.in

Bindhumadhava BS
CDAC Bangalore
Bangalore
India

Email: bindhu@cdac.in