Email Transport Ecryption: STARTTLS vs. DANE vs. MTA-STS

Scope of the Document

The scope of this document is limited to the encrypted transport between two email servers. The connection between Email Client and Server or End-to-End encryption is not included, but should also be taken into consideration for the security of the entire system. Transport encryption between email servers is essential to increase the security of email communication.

STARTTLS

The connection between mail servers can be secured by means of STARTTLS. However, the procedure is beset by glaring weaknesses. Firstly, the certificate of the email server is generally not checked during the establishment of the connection. In many cases it would not even be possible to check it, because self-signed certificates are used. Added to this, the initial establishment of a connection in STARTTLS occurs unencrypted, and the email servers negotiate the encryption. This is said to be an opportunistic encryption, given that communication is only encrypted when both email servers support STARTTLS. With a Man-in-the-Middle attack, an attacker could filter out the STARTTLS command. The emails would then be transmitted in plain text and the attacker can read the content.

DANE

With DNS-Based Authentication of Named Entities (DANE), the weaknesses of STARTTLS are addressed. DANE can be used for a range of applications; however, in this document we will focus on encrypted email transport. DANE enables a domain owner to issue certificates and to link these with corresponding entries in the Domain Name System (DNS). A communication partner can in this way verify the certificate without needing to fall back on a Certificate Authority (CA). However, in this design, it is necessary for the DNS entries to be protected against manipulation by third parties. DANE therefore requires DNS-Security Extensions (DNSSEC). Looked at from a global perspective, DNSSEC is unfortunately not currently widespread, and as a result, neither is DANE. From the perspective of the sender, however, DANE does not require DNSSEC, given that only the sender verifies the certificate of the receiving email server.

Don Owens from Cisco Talos Intelligence Group about DANE: "*DANE is a great way to encrypt traffic while avoiding MITM (man-in-the-middle) attacks. If DANE isn't supported by the receiver, then it is possible to use MTA-STS to make MITM attacks more difficult. Another option is to use opportunistic TLS to provide a layer of security, even though it is*

more vulnerable to MITM attacks. But really, receivers should set up DANE where feasible to support the best security for email traffic."

MTA-STS

An alternative to DANE, which also represents a considerable improvement on STARTTLS, but does not require DNSSEC, is SMTP MTA Strict Transport Security (MTA-STS). MTA-STS is based on a so-called "Trust on first use" (TOFU) model.
Put simply, in the first connection to a new server, the fingerprint of the certificate is saved in a local database for future reference. In every subsequent establishment of a connection to this server, the certificate will be checked against this local fingerprint. The TOFU model also typically has a role in ssh connections and in HTTP Strict Transport Security (HSTS). Although MTA-STS does not offer 100% protection against a Man-in-the-Middle attack, one could only be successful if the initial establishment of a connection were to be attacked.

Summary and Conclusion

Although STARTTLS protects against the passive reading of a connection between email servers, it can be relatively easily demoted to an unencrypted connection through a downgrade attack. DANE solves this problem and considerably increases security, but requires DNSSEC. MTA-STS is at first glance a good alternative to DANE. However, it should be noted that in most cases, rather than investing time and resources required into the implementation of MTA-STS, it would be more sensible to invest these into the implementation of DNSSEC and subsequently DANE. Because MTA-STS offers an (admittedly small) attack surface that DANE does not exhibit, and in addition, several further protocols, such as SPF and DKIM, depend on DNS entries. As a result, a greater prevalence of DNSSEC would be an advantage for everyone.

Author: Alexander Zeh,
Engineering Manager Certified Senders Alliance