The Promise of DANE

Russ Housley and Sean Turner

1. Introduction (or the Swinging Pendulum)

Public Key Infrastructure (PKI) makes use of a trusted third party to bind the subject name to a public key. At one time there was a lot of hype about PKI because there was no way for the party responsible for creating or assigning the subject name to securely associate a public key to it. Many companies jumped at the opportunity to fill this trusted role.

When people learned how much it would cost to "properly" perform this trusted role, there was significant consolidation in the offerings. Many organizations that tried to run their own Certification Authority (CA) discarded their efforts and turned to a few central CAs.

It turned out that some of these central CAs were not run well, and the confidence in central CAs has diminished. So, the pendulum is swinging once again toward more localized trust.

2. DANE (or Enabling The Next Swing of the Pendulum)

DNSSEC [RFC4033][RFC4034][RFC4035] offers an opportunity to eliminate complicated off-line processes for validation of the subject name. This relationship can be easily demonstrated by having the zone administrator for the subject domain post the public key in the DNS and digitally sign the resulting zone.

The IETF DANE WG defined a straightforward way for the administrators of domain names to specify the keys used in that domain's TLS servers; however, matching improvements in TLS client software in the web browser.

2.1 How It Works

The TLS client in the browser establishes a secure connection with a TLS handshake. This begins by the client looking up the server's name in the DNS to get the server's IP address, and then opening a TCP a connection to a particular port at the server's address, and then sends the initial TLS handshake message over the TCP connection. At this point, the client does not know whether the expected TLS server has been reached.

The first response from the server in the TLS handshake may contain the server's certificate. The client authentication of the server requires validation of that certificate, including matching the subject name in the certificate to the server name.

The DANE WG specified a different way to authenticate the server using DNSSEC [RFC6698]. The DNS administrator is responsible for managing names within the domain, and if the domain is signed, the same administrator can include a public key for the server as well. In this way, the same administrator that is responsible for the name is also responsible for the binding of a public key to that name.

The DANE WG also specified a way to obtain a certificate from the DNS. This allows the CA to act as third party when it adds value.

2.2 Pros and Cons of the DANE Approach

The biggest pro to the DANE approach is that it puts the power to be secure in the hands of the people who control the DNS entry for the servers. If the person wants to generate their own keys, then they can do so. If they don't want to, then they can still outsource to a commercial CA that will generate the keys for them.

Obviously, the DANE approach is not a panacea; a couple of issues still remain. ignoring the possibility of a compromised the DNSSEC resolver, there are three notable issues are:

First, how well does the server administrator run their own CA? Commercial CAs write CPs (Certificate Policies) and CPSs (Certification Practice Statements), and then they are audited to ensure that these are followed. It is not clear that a locally run CA will pay attention to all of these details. Then again, recent news stories make it clear that not all commercial CAs followed their CPs/CPSs.

Second, even for small and medium sized companies the person that controls the domain name is not always the person that is in charge of network security. If the keys are not installed when the DNS entry is created, there exists a window of time when an adversary could attempt to obtain a certificate for the domain from another CA. The DNS CAA (Certification Authority Authorization) resource record defined by the IETF PKIX working group can reduce this concern [RFC6844]. The resource record includes information about the CA from which the domain's certificate should be issued, so a savvy CA will refuse to issue a certificate unless they are listed in this resource record.

Third, status checking, regardless of whether CRL or OCSP is used, for some people the extra time to fetch and process the revocation information is still too much.

3. Conclusion

There is never a one-size-fits all solution for security. Commercial CAs should not be the only choice in the online trust game. Putting the power to secure more websites in the hands of those people who run them (and are savvy enough to generate certificates) is a good thing.

4. References

RFC4033
Arends, R., R. Austein, M. Larson, D. Massey, and S. Rose.
DNS Security Introduction and Requirements. RFC 4033, March 2005.

RFC4034
Arends, R., R. Austein, M. Larson, D. Massey, and S. Rose.
Resource Records for the DNS Security Extensions. RFC 4034, March 2005. (Format:

RFC4035
Arends, R., R. Austein, M. Larson, D. Massey, and S. Rose.
Protocol Modifications for the DNS Security Extensions. RFC 4035, March 2005.

RFC6698
Hoffman, P., and J. Schlyter.
The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA.
RFC 6698, August 2012.

RFC6844
Hallam-Baker, P., and R. Stradling. DNS Certification
Authority Authorization (CAA) Resource Record. RFC 6844, January 2013.