Alin Tomescu, CSE408
Tuesday, Apri 26th, Lecture #22

DNSsec and DANE

DNSsec and DANE

In DNSsec, the client talks to the resolver, the resolver talks to a root name server, to a *.com* name server, to a *.amazon.com* name server, and so on.

Resolver will collect a bunch of certificates. Initially, it will only have the public key of the root server.

The client can check the IP address in the response messages with those certificates.

DANE, if we have a mechanism where we can verify DNS answers are correct and legitimate (PKI infrastructure) then we can also use that infrastructure to exchange public keys between *amazon.com* and the client for instance.

Example DNSsec run

- Client types in www.abc.com
- Web browser looks up the address, sends it to the local resolver?
    - Where is www.abc.com?
- Resolver is preloaded with the public key of the root server
    - the root server, has a table of the name servers for all the domains like *.com, .org* etc, mapping *.com* to the IP address of its NS and to a certificate which contains the public key of the *.com* DNS server:
        - $C_{A,B} = A, B, P_B, L, Sig_{S_A}(\dots)$. If you trust A, then you know B's public key.
- Resolver asks root NS what is the NS for *.com*
- Root sends address of *.com*, signed of course, and the certificate for the *.com*
    - So now s the client is in the same scenario with the *.com* NS as it was in with the root NS
    - Therefore, the protocol is repeated until www.abc.com is retrieved
- Finally, resolver asks *abc.com* NS for the IP of www.abc.com
- *abc.com* NS sends IP address signed under *abc.com*'s secret key
    - With DANE, a certificate containing the SSL public key for secure communication between the client and www.abc.com is also sent.

PGP web of trust

This was originally intended for use by a program called PGP, used to encrypt email. Users would download PGP, generating their own private-public key pair, bound to their email address.

$Certificate_{rob@cs.sunysb.edu,ali@cs.sunysb.edu}$ says that if you trust Rob, you can get Ali's public key safely.

You might have Alice trusting Bob and Charlie. She's trying to talk to David. David has $C_{Bob,David}$ and $C_{Charlie,David}$

If he sends these two certificates to Alice, then since Alice trusts the two, she can get David's public key.

What if Alice trusts Bob who trusts Francis. David has $C_{Bob,Francis}$, $C_{Francis,David}$ and $C_{Charlie,David}$. Then that would work by transitivity.

One disadvantage is that people need to carry on a lot of certificates.