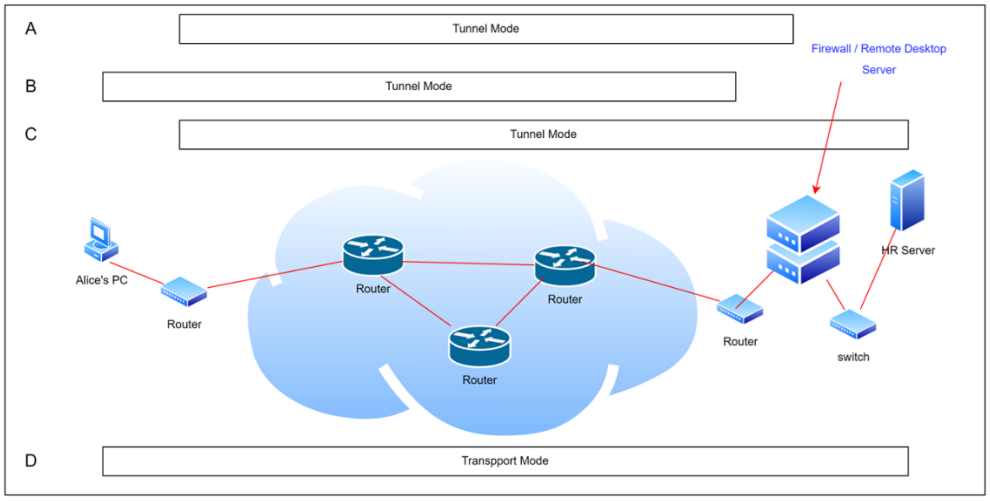
ST2612 Tutorial 6 (Week 16)

Recap of Practical 6, Practical 7, Lecture 6 (Part 2), Lecture 7

Self-evaluation Check list

- What is your view of Lecture 6 slides 24? The question on whether the IPsec applied in that scenario is redundant.

Suggested Answer:



For scenario D, the transport mode IPsec offers protection from Alice's PC to the HR servers. If there is already a VPN channel setup from Alice's PC to the Office network it may be seen as the IPsec setup is reductant. However, the protection of the VPN only covers between Alice's PC and the office network (The end points are Alice's PC and the Firewall/Terminal Server). There is no protection between the firewall/terminal servers to the HR servers. The IPsec setup is to ensure that there is no unprotected gaps between Alice's PC to the HR servers. Thus, this setup is not reductant.

- The following few items should always be found in a valid digital certificate. Would you briefly explain what will be the impact/issues if they are missing from the design of a digital certificate?

-Serial number

CRL and OCSP cannot work as the Serial number is a unique identifier for the status checking. Using other means to identify a particular certificate will be troublesome if not impossible.

-Subject

Without the subject field, we cannot verify the certificate is used by the rightful party.

-Public key

The whole purpose of digital certificates in PKI is to distribute authenticated public keys for different parties to establish confidential electronic communication channels. It will defeat the purpose of setting up PKI if the Public Key is not defined in the digital certificate.

-Digital Signature

Without the digital signature, we cannot verify the authenticity of the content of the certificate.

-Expiry Date

Without the Expiry Date, there will be two serous issues.

- The Key(s) will be subjected to higher risk of successful brute force attack.
- The size of the CRL will keep growing and become not feasible to maintain and/or operate in any effective manner.

- What will be the impact(s) to an https enabled website when its corresponding certificate authority server (The SSL cert issuer) is having an outage?

The operations of the website should not be affected by the outage. The SSL certification validation should be carried out without the presence of the Cert Issuer's server. If the OCSP responder is down, it may affect the level of accuracy the status check. However, OCSP responder are usually running on a different (and multiple) server(s) other than the certificate issuer server.

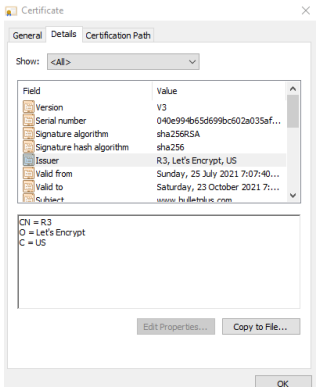
- PKI framework is very much depending on the 'Trust'. From the end users' point of view, what should be the main factor for them to decide which certificates to be trusted?

The end user usually depends on the content of the Trusted RootCA repository to determine the acceptance of certificates that signed by different digital certificate issuers. The content of the repository is either based on the default and/or system administrators' control.

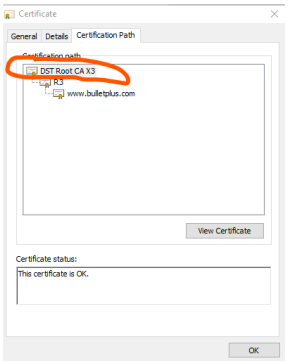
- Can you figure out why our windows browser(s) are accepting the certificates issued by letsencrypt.org.

It is based on cross-site trust model.

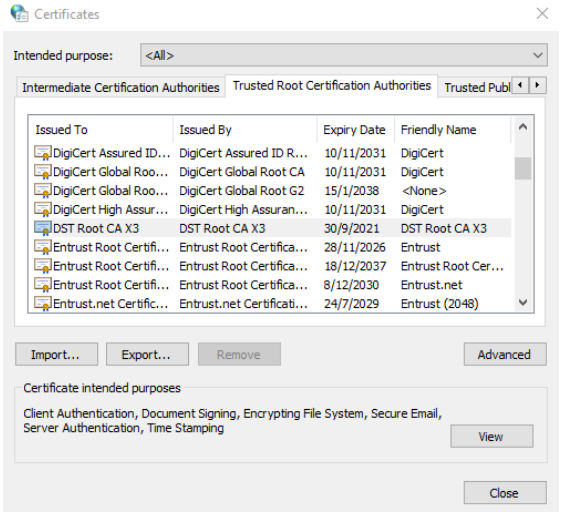
For example, the follow certificate is issued by one of the Letsencrypt servers, which is not a Trusted RootCA for a default windows system.



However, when we check its detail certification path, we can see R3 is endorsed by DST Root CA X.3.



We can find DST Root CA X.3 is one of the Trusted Root CA in our Windows system:



- In page 21 of the lecture slide, what is the purpose or the effect of installing the downloaded certificate chain to the Trusted Root Certificate Authority Repository?

  This is to download all the certificates of the issuer servers of the RootCA to the repository. With these certificates in place, the system will trust and accept digital certificates that have been issued and signed by any of these issuer servers. [ie. The trusted relationship is established.]

- In slide 41. It mentioned self-signed certificate and self-issued certificate. Both of them are only used for in-house applications and they are not accepted by general public, but what is their difference?

  In most of the cases, they are referring to the same thing. To be more précised: a self-signed certificate is issued by the host itself and the self-issued certificate may be interpreted as the certificate is issued by another in-house certificate issuer. In general, neither of the self-signed nor self-issued certificates will be accepted by any external bodies.

~ The End ~