Lab Assignment 5 Write-up : Public-Key Cryptography and the PKI

Abhinav Kumar (abkuma@iu.edu)

1.How does Let’s Encrypt verify that a certificate signing request came from the correct entity for their Domain Validation (DV) certificates? What are two disadvantages/limitations to using method of validation?

Let's Encrypt offers domain-validated certificates, meaning they have to check that the certificate request comes from a person who actually controls the domain. They accomplish this by delivering the client a unique token and then retrieving a key generated from that token via an HTTP or DNS request.

Domain validated certificates are less secure than other types of SSL certificates. Any hacker can get a domain validated SSL certificate and then use it to conceal their identity. If attackers poison DNS servers, this is also true for websites. When it comes to domain verified certificates, there is no way to know for sure who is who. As a result, users may be less trusting of your site than they would be if you had a certificate that required you to validate your business. With this type of certificate, potential customers may be hesitant to send over their payment information.

2.What are Extended Validation certificates? What are two advantages and disadvantages to using extended validation certificates?

An Extended Validation SSL Certificate which is also known as EV SSL for short is the highest form of SSL Certificate on the market. While all levels of SSL – Extended Validation (EV), Organization Validated (OV), and Domain Validated (DV) – provide encryption and data integrity, they vary in terms of how much identity verification is involved. It is a certificate conforming to X. 509 that proves the legal entity of the owner and is signed by a certificate authority key that can issue EV certificates. EV certificates can be used in the same manner as any other X.

Benefits of using extended validation certificates:
1)Protect customers from phishing and cybercriminals.
2)Increase customer trust by displaying the EV green address bar & HTTPs padlock.

Disadvantages of using extended validation certificates:
1)They are more expensive and generally valid for shorter duration.
2)There is hassle of going through the whole validation process.

3.What steps could you take to ensure that you have the correct root certificate for Let’s Encrypt in your browser

We can check the correct root certificate by ensuring the key pair generated matches with the Let's Encrypt Certificate Authority that the web server use to control the domain. And ensure that the Let's Encrypt is signed with correct private key.

4. Compare and contrast the OCSP and CRL approaches for certificate revocation.

The CRL (Certificate Revocation Lists) contains a list of certificate serial numbers that the CA has revoked. OCSP is a protocol for checking the revocation of a single certificate using an OCSP responder, which is an online service.

CRL can result in a significant amount of overhead. client has to search through the entire revocation list, whereas in OCSP the client has to check the status of a single certificate, rather than downloading and parsing a whole list.

CRL is substantially faster than OCSP; that is, comparing a certificate to a list on disk is faster than contacting a separate server over the network to validate each certificate.

5. What X.509 field does a browser to check to determine if a received certificate is allowed to be used for the site that sends it?

Browser checked the signature of the certificate using the public key info. Also, it checks the basic constrains where the certificate is that of CA or not. Otherwise it checks whether, the certificate belongs to an "end-user" or "end-entity" , and also for verifying server or client identities, signing or encrypting e-mail or other content, signing executable code etc.

6.Why do certificates have an expiration date if there are other certificate revocation mechanisms (i.e. OCSP and CRL)?

Certificates with long lifecycles could be misleading when identity or domain control changes.
In this way to control the CRL size under control otherwise revoked certificates would accumulate for longer time.
To help ensure that all certificates are using the latest security standards and in fact controlled by the current certificate owner, it is required to expire them. New certificates are issued using the latest security standards, processes and a re-confirmation of domain control and organization identity.
Shorter life certificates also promote the creation of new keys. Frequent key changes help mitigate compromises associated with them. That's why certificates have an expiration date.