Advanced Web Security - Assignment 4A

December 2020

Questions

1. Is DER and CER always valid BER? Explain.
2. One BER encoding of the VisibleString “string” is given by 3A 80 1A 03 73 74 72 1A 03 69 6e 67 00 00 as can be seen in the lecture notes. Change this encoding so that short definite form is used for the outer TLV. Do not change the fragmentation.
3. Give the DER encoding of the INTEGER 10000 (ten thousand).
4. In ASN.1, what is the difference between DEFAULT and OPTIONAL?
5. List at least 5 protocols that employ CMS.
6. Describe the 4 possible key-encryption mechanisms supported by the EnvelopedData type. What art the prerequisites to use each mechanism?
7. A CRL can be a delta CRL. This is specified using an extension. Why is this extension critical? Give an example of a non-critical CRL extension and motivate why it is non-critical.
8. What is the main issue that IBC aims at solving?

Answers

1. Yes, DER and CER are subsets of BER. Firstly, They are both canonical, meaning that they describe unique encoding for the data, same as BER. BER can be either definite or indefinite. DER is uses shortest possible definite form, while in CER indefinite form is used. Since DER and CER are more or less subsets of BER they are always valid.

2.

3.

4. The difference between DEFAULT and OPTIONAL in ASN.1 is that DEFAULT will be an assumed value if it is not included, while OPTIONAL means as it is stated that the value is optional to include, aka. it does not have to exist.

5. The Cryptographic Message Syntax or CMS is employed by:

   (a) S/MIME

   (b) PKCS12

   (c) RFC 3161 Digital time-stamping

   (d) OpenSSL

   (e) S-HTTP [1]

6. The 4 possible key-encryption mechanisms supported by the Enveloped-Data type is: 1. key transport: which requires RSA encryption support.
   2. key agreement, which requires Ephemeral-Static Diffie-Hellman (DH)
   3. symmetric keys: we assume there is a key already shared between the recievers
   4. passwords: using a KDF function on a password or function

7. The extension is critical because the delta CRL contains only certificates that have been revoked after a given complete CRL has been issued. This is a critical extension because it is important to know that the certificate is a delta CRL. This CRL is different from a normal CRL, as it instead contains updates since the last CRL.
   A non-critical CRL extension is the CRL number, aka the sequence number of used for the CRL. Knowing this information is not super important and will not change the way the CRL is handled or read. s

8. The main issue that IBC aims at solving is the us of a PKI. The recipient of a message does not need to have a key pair in advance. There is also no need to CRL's, which means we can't revoke public keys.

[1] Cryptographic Message Syntax: $https://www.vocal.com/secure-communication/cryptographic-message-syntax-cms/$

[2] RFC6033: http://rfc.w3dt.net/rfc6033.html