UC Computer Science and Software Engineering

COSC362 Data and Network Security
Semester Spring, 2021

Lab Quiz 6

Quiz relates to Lectures 15 and 16. Questions might have been seen in a different order on LEARN.

QUESTION 1

Digital certificates are signed by a certification authority. In order to make certificate verification as fast as possible, it is common for this purpose to use:

(a) RSA signatures

(b) Elgamal signatures

(c) DSA signatures

(d) ECDSA signatures

RSA signatures

QUESTION 2

An alternative to a hierarchical PKI is to use *web of trust*. An important property in a web of trust, that does not apply in a hierarchical PKI, is that:

(a) private keys can be generated by any party

(b) public keys can be signed by any party

(c) subjects can remain anonymous

(d) a variety of different signature algorithms can be used to sign certificates

---

public keys can be signed by any party

---

cont/...

QUESTION 3

Two commonly used digital signatures schemes are RSA signatures and ECDSA. RSA is commonly used to sign digital certificates. This is because, for the same security level:

(a) RSA public key lengths are shorter

(b) RSA signatures are shorter

(c) RSA signature generation is faster

(d) RSA signature verification is faster

RSA signature verification is faster

QUESTION 4

In order to produce a digital certificate, a certification authority computes:

(a) an encryption of the subject's private key and identity

(b) an encryption of the subject's public key and identity

(c) a signature on the subject's private key and identity

(d) a signature on the subject's public key and identity

---

a signature on the subject's public key and identity

QUESTION 5

An X.509 digital certificate is issued by a certification authority. In order to verify such a certificate it is necessary, in addition to the certificate itself, to have:

(a) the subject's private key

(b) the subject's public key

(c) the certification authority's private key

(d) the certification authority's public key

---

the certification authority's public key

---

cont/...

QUESTION 6

The original Needham-Schroeder protocol is known to be vulnerable to a replay attack. This means that:

(a) an honest party accepts a session key used in a previous run of the protocol

(b) an honest party re-uses its nonce used in a previous run of the protocol

(c) the attacker obtains the long-term key of an honest party

(d) the attacker obtains the nonce used by an honest party

---

an honest party accepts a session key used in a previous run of the protocol

---

QUESTION 7

The basic ephemeral Diffie–Hellman protocol can be strengthened by adding to each message a digital signature of the sender. The effect of this on the protocol is to:

(a) provide entity authentication

(b) allow shorter Diffie–Hellman parameters

(c) prevent replay attacks

(d) prevent attacks which can find discrete logarithms

---

provide entity authentication

QUESTION 8

Forward secrecy is the property that:

(a) if a user's long term key becomes known to an attacker, session keys established earlier are not compromised

(b) if a user's long term key becomes known to an attacker, session keys established later are not compromised

(c) if a user's session key becomes known to an attacker, that user's long term key is not compromised

(d) if a user's session key becomes known to an attacker, that user's long term key is also compromised

---

if a user's long term key becomes known to an attacker, session keys established earlier are not compromised

---

cont/. . .

QUESTION 9

The basic ephemeral Diffie-Hellman protocol can be authenticated by adding to each message a digital signature of the sender. The protocol then provides forward secrecy because:

(a) revealing the Diffie-Hellman shared secret does not reveal the signing keys

(b) revealing the signing keys does not reveal the Diffie-Hellman shared secret

(c) revealing the Diffie-Hellman ephemeral secret keys does not reveal the Diffie-Hellman shared secret

(d) revealing the Diffie-Hellman ephemeral secret keys does not reveal the signing keys

---

revealing the signing keys does not reveal the Diffie-Hellman shared secret

---

QUESTION 10

When assessing the security of a key establishment protocol such as the Needham-Schroeder protocol, we assume that an attacker is able to:

(a) obtain any session keys used in previous runs of the protocol

(b) obtain the long-term key of the parties involved in the protocol run under attack

(c) break any encryption algorithm used in the protocol

(d) force any protocol participant to repeat nonce values

---

obtain any session keys used in previous runs of the protocol

---