Exam Report: 9.8.8 Practice Questions

Date: 1/28/2020 6:56:01 pm
Time Spent: 4:11

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 53%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which aspect of a certificate makes it a reliable and useful mechanism for proving the identity of a person, system, or service on the internet?

- It is a trusted third-party.
- It is a digital mechanism, rather than a physical one.
- ~~It uses electronic signatures.~~
- It provides ease of use.

Explanation

The use of a trusted third-party (called a Certificate Authority or CA) is what makes certificates a reliable and useful mechanism for proving the identity of a person, system, or service on the internet. The CA issues proof of identity to each organization in the form of a certificate. The fact that all entities trust the CA makes the certificates trusted and valuable.

A certificate only proves identity; it does not prove reliability. Electronic signatures are a form of certificate that verifies identity. While electronic signatures prove identity, they do so only because both parties trust the authority of the CA, not because the signature exists. Certificates are easy to use. However, ease of use does not make them reliable. Certificates are a digital mechanism, which makes them suited for use on the internet. However, that alone does not make them reliable or useful.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_02]

Question 2: Correct

Which standard is most widely used for certificates?

- X.509
- SSL v.3.0
- HTTP 1.1
- 802.1x

Explanation

The standard for certificates that is most widely used is X.509. This standard defines the key elements that must exist within a certificate. This standard is used by PKI (Public Key Infrastructure), SSL, IPsec, DES, and many other infrastructure components and technologies.

HTTP 1.1 is the latest version of the protocol used to transmit web resources from a web server to a web client. SSL v.3.0 uses certificates, but this is the standard for the secure session protocol for protecting

web communications. 802.1x is a networking protocol that defines how to support EAP (Extensible Authentication Protocol) over a wired or wireless LAN.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_04]

Question 3: Incorrect

Which of the following items are contained in a digital certificate? (Select two.)

- [x] Public key
- [x] ~~Private key~~
- [ ] Root CA secret key
- [ ] Validity period

Explanation

Digital certificates create a link between identities and public keys. A certificate contains the information necessary to identify the public key owner. Certificates include fields detailing the issuing CA and the standards version used to generate the certificate, a certificate serial number, all approved uses for the certificate, the certificate owner, the public key and algorithm, the validity period, and the algorithms used to digitally sign the certificate. Additional functionality and data may be added through the use of certificate extensions.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_06]

Question 4: Incorrect

Which of the following conditions does **not** result in a certificate being added to the certificate revocation list?

- (●) ~~Committing a crime using the certificate~~
- ( ) Certificate expiration
- ( ) Invalid identity credentials
- ( ) Private key compromise

Explanation

When a certificate's valid time value expires, the certificate immediately becomes invalid because it has expired. Expired certificates are not added to the CRL because the timestamp serves as notification that the certificate is no longer valid.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_08]

Question 5: Incorrect

Which of the following is an entity that accepts and validates information contained within a request for a certificate?

- ( ) Registration authority
- (●) ~~Certificate authority~~
- ( ) Recovery agent

- Enrollment agent

Explanation

A Registration Authority (RA) can be used in large enterprise environments to offload client enrollment request processing by handling client verification prior to certificates issue. The RA accepts registrations, validates identity, and approves or denies certificate requests.

The Certificate Authority (CA) is an entity trusted to issue, store, and revoke digital certificates. Often, the role of CA is combined with that of RA. But technically speaking, a CA is the computer that issues the certificate. *Recovery agents* are users who are given the ability to restore private keys from the archive. An enrollment agent is someone who can request a certificate on behalf of another user. Enrollment agents are often used to request certificates used on smart cards.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_10]

Question 6: Correct

What is a PKI?

- A hierarchy of computers for issuing certificates.
- A program that generates key pairs.
- A protocol that defines secure key exchange.
- An algorithm for encrypting and decrypting data.

Explanation

A public key infrastructure (PKI) is a hierarchy of computers that issue and manage certificates.

A Cryptographic Service Provider (CSP) resides on the client and generates the key pair. Secure exchange of keys is provided by many protocols, including RSA, Diffie-Hellman, IKE, and KEA.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_12]

Question 7: Correct

A PKI is an implementation for managing which type of encryption?

- Asymmetric
- Steganography
- Hashing
- Symmetric

Explanation

A public key infrastructure (PKI) is a hierarchy of computers that issue and manage certificates. Certificates use asymmetric encryption with a public and a private key pair.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_14]

Question 8: Incorrect

Certificate revocation should occur under all but which of the following conditions?

- The certificate owner has moved their website to a new domain name

- The certificate owner has held the certificate beyond the established lifetime timer
- The certificate owner has changed their business name
- ~~The certificate owner has committed a crime while using the certificate~~

Explanation

A certificate does not need to be revoked once it expires. The possession of an expired certificate is useless.

A certificate should be revoked whenever the owner commits a crime using the certificate or when a significant aspect of the identity of the organization changes.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_16]

Question 9: Incorrect

Which technology was developed to help improve the efficiency and reliability of checking the validity status of certificates in large, complex environments?

- Certificate Revocation List
- ~~Key Escrow~~
- Online Certificate Status Protocol
- Private Key Recovery

Explanation

Online Certificate Status Protocol (OCSP) is the technology developed to improve the efficiency and reliability of checking the validity status of certificates in large complex environments. OCSP allows clients to query a CA or registration authority (RA) and quickly learn whether a certificate is valid or has been revoked.

OCSP is a significant improvement over the CRL mechanism. CRLs were static lists that were distributed periodically to CAs and RAs. However, CRLs were often out of date. Key escrow and private key recovery are not related to certificate status checking.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_18]

Question 10: Correct

Which action is taken when the private key associated with a digital certificate becomes compromised?

- The CA retracts all previously issued copies of the certificate.
- The certificate is revoked and added to the Certificate Revocation List.
- The RA requests a reissued digital signature based on the existing private key.
- All certificates are revoked from parties known to possess the matching public key.

Explanation

When a private key becomes compromised, the certificate authority revokes the certificate and adds it to the certificate revocation list (CRL). This list notifies anyone attempting to verify the digital signature that the certificate is not trustworthy. The CRL is designed to prevent impersonation by anyone obtaining unauthorized access to a private key.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_20]

Question 11: Incorrect

You have lost the private key that you have used to encrypt files. You need to get a copy of the private key to open some encrypted files. Who should you contact?

- Recovery agent
- ~~Certification Authority~~
- Enrollment agent
- Registration Authority

Explanation

Recovery agents are users who are given the ability to restore private keys from the archive. An enrollment agent is someone who can request a certificate on behalf of another user.

Enrollment agents are often used to request certificates used on smart cards.

A Registration Authority (RA) can be used in large enterprise environments to offload client enrollment request processing by handling client verification prior to certificate issue. The RA accepts registrations, validates identity, and approves or denies certificate requests.

The Certificate Authority (CA) is an entity trusted to issue, store, and revoke digital certificates. Often, the role of CA is combined with that of RA. But technically speaking, the CA is the computer that issues the certificate.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_22]

Question 12: Correct

To obtain a digital certificate and participate in a Public Key Infrastructure (PKI), what must be submitted and where?

- Identifying data with the 3DES block cipher to the hosting certificate authority (CA)
- Identifying data with the MAC and IP addresses to the root certificate authority (CA)
- Identifying data and a certification request to the registration authority (RA)
- Identifying data and a secret key request to the subordinate distribution authority (DA)

Explanation

The registration authority (RA) processes all requests for digital certificates. Registration and authentication requirements vary based on the class of certificate requested. Once the RA has successfully authenticated the requesting party, the request is forwarded to the certificate authority (CA) for certificate generation.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_24]

Question 13: Correct

An SSL client has determined that the Certificate Authority (CA) issuing a server's certificate is on its list of trusted CAs. What is the next step in verifying the server's identity?

- The post-master secret must initiate subsequent communication.
- The master secret is generated from common key code.

- The CA's public key must validate the CA's digital signature on the server certificate.
- The domain on the server certificate must match the CA's domain name.

Explanation

Once an SSL client has identified a CA as trusted, it uses the CA's public key to validate the CA's digital signature on the server certificate. If the digital signature can be verified, the client accepts the server certificate as a valid certificate issued by a trusted CA.

SSL clients verify a server's identity with the following steps:

1. The client checks the server's certificate validity period. The authentication process stops if the current date and time fall outside of the validity period.
2. The client verifies that the issuing Certificate Authority (CA) is on its list of trusted CAs.
3. The client uses the CA's public key to validate the CA's digital signature on the server certificate. If the digital signature can be verified, the client accepts the server certificate as a valid certificate issued by a trusted CA.
4. To protect against Man-in-the-Middle attacks, the client compares the actual DNS name of the server to the DNS name on the certificate.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_26]

Question 14: Correct

How many keys are used with Public Key cryptography?

- One
- Two
- Three
- Four

Explanation

Public Key cryptography uses two keys: one is referred to as the public key, and the other, the private key. This key pair overcomes the difficulties associated with the secure distribution of private keys. The communicating parties do not need to share secret information: only the public keys are shared. Public keys are associated with users through authentication, usually through a mutually trusted directory, such as a certificate authority. The sender transmits a confidential message using only the recipient's public key. The message can only be decrypted with the associated private key possessed solely by the recipient. Public Key cryptography not only provides encryption, but is the basis for authentication technologies such as digital signatures.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_27]

Question 15: Correct

When is the best time to apply for a certificate renewal?

- After a certificate has been revoked
- Near the end of the certificate's valid lifetime
- Just after a certificate expires
- Immediately after a certificate is issued

Explanation

Certificate renewal is a process by which a currently valid certificate is re-issued with an extended lifetime value. It is performed by submitting a renewal request and signing the request with the still-valid

certificate.

Attempting to renew a certificate close to its issuance date will not result in a renewal in most cases. There is no need to renew a certificate until you near the end of its valid lifetime. It is not possible to renew a certificate after it has expired or been revoked; these conditions require you to request a new certificate.

References

LabSim for Security Pro, Section 9.8.
[All Questions SecPro2017_v6.exm PUBLIC_KEY_30]