Exam Report: 3.5.8 Practice Questions - Section 3.5

Date: 11/24/2015 3:34:20 pm
Time Spent: 3:07

Candidate: Belskis, Tomas
Login: t0mas9lt

Overall Performance

Your Score: 13%

Passing Score: 80%

Certification Ranking

Within your class: Within your school: Nationally:

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

What is the purpose of key *escrow*?

- To provide a means to recover from a lost private key
- ~~Collection of additional fees over the life of using a public digital certificate~~
- To grant the certificate authority full control over the communication environment
- To provide a means for legal authorities to access confidential data

Explanation

Key escrow is an arrangement in which encryption keys are held in escrow so that an authorized third party can access those keys to decrypt an individual's data. For example, a business may need to access an employee's encrypted work files. Likewise, law enforcement officers investigating a crime may need to view an individual's personal encrypted data.

References

LabSim for Security Pro, Section 3.5.
[Questions.exm SSCP-2 SP [411]]

Question 2: Incorrect

Which aspect of certificates makes them a reliable and useful mechanism for proving the identity of a person, system, or service on the Internet?

- It is a digital mechanism rather than a physical one
- Trusted third-party
- ~~Electronic signatures~~
- 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 only 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 3.5.
[Questions.exm SP02_1-2 [29]]

Question 3: Incorrect

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

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

Explanation

Digital certificates create a link between identities and public keys. A certificate contains the information needed for verifying the identity of 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 3.5.
[Questions.exm SP02_4-3 [108]]

Question 4: Incorrect

In what form of key management solution is key recovery possible?

- ( ) Centralized
- ( ) Hierarchical
- ( ) Decentralized
- (•) ~~Public~~

Explanation

Only a centralized key management solution provides a key escrow service that allows for key recovery to occur. A decentralized key management solution does not provide for key escrow and thus key recovery is not possible. A hierarchical trust model may employ a centralized or decentralized key management solution. A public certificate system may be a centralized or decentralized key management solution.

References

LabSim for Security Pro, Section 3.5.
[Questions.exm SP02_4-5 [77]]

Question 5: Incorrect

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

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

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 time stamp itself serves as notification that the certificate is no longer valid.

References

LabSim for Security Pro, Section 3.5.
[Questions.exm SP02_4-5 [109]]

Question 6: Incorrect

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

- Certificate authority
- Recovery agent
- ~~Enrollment agent~~
- Registration authority

Explanation

A Registration Authority (RA) can be used in large, enterprise environments to offload client enrollment request processing by handling verification of clients prior to certificates being issued. 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 3.5.
[Questions.exm SP08_5-5 4]

Question 7: Incorrect

Which of the following would you find on a CPS?

- A declaration of the security that the organization is implementing for all certificates
- A list of revoked certificates
- A description of the format for a certificate
- ~~A list of issued certificates~~

Explanation

The Certificate Practice Statement (CPS) is a declaration of the security that the organization is implementing for all certificates issued by the CA holding the CPS.

The Certificate Revocation List (CRL) resides at the CA and consists of a list of certificates that have been previously revoked. The Online Certificate Status Protocol (OCSP) is a protocol used for checking the status of an individual digital certificate to verify if it is good or has been revoked. X.509 is the standard that identifies the format for certificates.

References

LabSim for Security Pro, Section 3.5.
[Questions.exm SP08_5-5 6]

Question 8: Incorrect

What is a PKI?

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

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 3.5.
[Questions.exm SP08_5-5 7]

Question 9: Correct

A PKI is a method for managing which type of encryption?

- Asymmetric
- Hashing

- Steganography
- 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 3.5.
[Questions.exm SP08_5-5 9]

Question 10: Incorrect

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

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

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 get quick and distinct status information as to the validity or revoked status of a certificate.

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 3.5.
[Questions.exm SP02_4-5 [45]]

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?

- Enrollment agent
- Registration authority
- Recovery agent
- ~~Certification 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 verification of clients prior to certificates being issued. 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.

References

LabSim for Security Pro, Section 3.5.
[Questions.exm SP08_5-6 2]

Question 12: Incorrect

You have a Web server that will be used for secure transactions for customers who access the Web site over the Internet. The Web server requires a certificate to support SSL.

Which method would you use to get a certificate for the server?

- ~~Have the server generate its own certificate.~~
- Obtain a certificate from a public PKI.
- Create your own internal PKI to issue certificates.
- Run a third-party tool to generate the certificate.

Explanation

Computers must trust the CA that issues a certificate. For computers that are used on the Internet and accessible to public users, obtain a certificate from a public CA such as VeriSign. By default, most computers trust well-known public CAs.

Use a private PKI to issue certificates to computers and users within your own organization. You configure computers to trust your own PKI, so certificates issued by your internal CAs are automatically trusted. A certificate generated by a server is called a *self-signed* certificate. A self-signed certificate provides no proof of identity because any other server can claim to be that server just by issuing itself a certificate.

References

LabSim for Security Pro, Section 3.5.
[Questions.exm NP09_6-4 MCS3]

Question 13: Incorrect

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

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

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 3.5.
[Questions.exm SSCP-2 SP [475]]

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 provides not only encryption, but is the basis for authentication technologies such as digital signatures.

References

LabSim for Security Pro, Section 3.5.
[Questions.exm SP [331]]

Question 15: Incorrect

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

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

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 3.5.
[Questions.exm SP [499]]