Exam Report: 3.6.4 Practice Questions - Section 3.6

Date: 11/24/2015 4:43:11 pm
Time Spent: 2:41

Candidate: Belskis, Tomas
Login: t0mas9lt

Overall Performance

Your Score: 33%

Passing Score: 80%

Certification Ranking

Within your class: Within your school: Nationally:

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

What is the main function of a TPM hardware chip?

- Generate and store cryptographic keys
- Provide authentication credentials on a hardware device
- Control access to removable media
- Perform bulk encryption in a hardware processor

Explanation

A Trusted Platform Module (TPM) is a hardware cryptoprocessor that resides on the motherboard that stores and generates cryptographic keys. These keys are used for encryption and authentication, but the TPM does not perform the actual encryption.

A smart card is a hardware device containing a digital certificate. The smart card can be used for authentication. Special hardware processors have been designed which perform bulk encryption in hardware rather than software. These processors typically encrypt data using AES or to encrypt network traffic using IPSec.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm SP08_5-1 1]

Question 2: Correct

Which of the following is a direct protection of integrity?

- Symmetric encryption
- Asymmetric encryption
- Digital signature
- Digital envelope

Explanation

A digital signature is a direct protection of integrity as it includes the use of hashing which detects changes to integrity.

Digital envelopes, symmetric encryption, and asymmetric encryption do not provide direct integrity protection nor do they use hashing to provide integrity protection.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm CISSP-302 NEW [55]]

Question 3: Incorrect

Which of the following statements is **true** when comparing symmetric and asymmetric cryptography?

- Asymmetric key cryptography is used to distribute symmetric keys.
- Symmetric key cryptography should be used for large, expanding environments.
- Asymmetric key cryptography is quicker than symmetric key cryptography while processing large amounts of data.
- ~~Symmetric key cryptography uses a public and private key pair.~~

Explanation

Asymmetric key cryptography can be used to distribute symmetric keys. This is known as a *hybrid* cryptography system. A hybrid cryptography system combines the strengths of both the symmetric and asymmetric cryptography systems (i.e. symmetric systems can process large amounts of data relatively fast, and asymmetric systems can securely distribute keys).

Symmetric cryptography uses a single key pair, with each partner using the same key. Asymmetric cryptography uses a public and a private key pair. Symmetric key cryptography processing is about 1000 times faster than asymmetric cryptography. In large, expanding environments, managing keys with symmetric key cryptography is difficult.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm SSCP-2 NEW [90]]

Question 4: Incorrect

Which of the following is **not** true in regards to S/MIME?

- Authenticates through digital signatures
- ~~Uses X.509 version 3 certificates~~
- Uses IDEA encryption
- Included in most Web browsers

Explanation

Secure Multi-Purpose Internet Mail Extensions (S/MIME) uses RSA (not IDEA) encryption. Based on RFC 1521, S/MIME employs encryption to provide for confidentiality. S/MIME can be used to protect both the body of e-mail messages as well as any file attachments.

Secure Multi-Purpose Internet Mail Extensions (S/MIME) authenticates through digital signatures, uses X.509 version 3 certificates, and is included in most Web browsers.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm SP02_2-2 [13]]

Question 5: Incorrect

Which of the following technologies is based upon SSL (Secure Sockets Layer)?

- L2TP (Layer 2 Tunneling Protocol)
- ~~IPSec (Internet Protocol Security)~~
- TLS (Transport Layer Security)
- S/MIME (Secure Multipurpose Internet Mail Extensions)

Explanation

TLS is based on SSL, but they are not interoperable. TLS (Transport Layer Security) operates over TCP port 443 or port 80. TLS was developed by Netscape to secure Internet based client/server interactions. TLS authenticates the server to the client using public key cryptography and digital certificates. TLS encrypts the entire communication session between a server and a client. TLS can be used to protect Web (HTTP) traffic as well as telnet, FTP, and e-mail.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm SSCP-3 SP [552]]

Question 6: Incorrect

Which of the following can be used to encrypt Web, e-mail, telnet, file transfer, and SNMP traffic?

- EFS (Encryption File System)
- IPSec (Internet Protocol Security)
- ~~SSL (Secure Sockets Layer)~~
- SHTTP (Secure Hypertext Transfer Protocol)

Explanation

IPSec (Internet Protocol Security) can be used to encrypt any traffic supported by the IP protocol. This includes Web, e-mail, telnet, file transfer, and SNMP traffic as well as countless others. IPSec is fully capable of providing a secure means to communicate for any LAN or Internet based system using TCP/IP.

EFS is not a communication protocol, thus it cannot be used to encrypt traffic. Rather it is a file encryption tool. SHTTP is used only for Web traffic. SSL is able to encrypt most Internet based communication sessions, it is not designed to protect all TCP/IP LAN traffic like IPSec.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm SSCP-3 SP [946]]

Question 7: Incorrect

What is the primary use of Secure Electronic Transaction (SET)?

- Protect credit card information transmissions
- ~~Encrypt e-commerce traffic~~
- Validate the integrity of database changes
- Secure electronic checking account transactions

Explanation

Secure Electronic Transaction (SET) was developed by VISA and MasterCard to secure transactions. Credit card data and a digital certificate are stored in a plug-in to the user's Web browser. An order received by a SET-enabled merchant server passes the encrypted payment information to the bank. Approval is electronically sent to the merchant. SET uses DES and RSA in addition to digital signatures.

Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are commonly used to protect e-commerce data transmissions between clients and servers. The concept of a *transaction* or transactional processing ensures the integrity of database changes.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm NEW [122]]

Question 8: Correct

Secure Multi-Purpose Internet Mail Extensions (S/MIME) is used primarily to protect what?

- E-mail attachments
- Newsgroup postings
- Instant messages
- Web surfing

Explanation

Secure Multi-Purpose Internet Mail Extensions (S/MIME) is used primarily to protect e-mail and the file attachments on e-mail messages. Based on RFC 1521, S/MIME uses RSA encryption. S/MIME employs encryption to provide for confidentiality.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm SP [539]]

Question 9: Incorrect

The PGP or Pretty Good Privacy encryption utility relies upon what algorithms? (Select two.)

- [ ] Blowfish
- [x] 3DES

IDEA

~~AES~~

Explanation

The PGP or Pretty Good Privacy encryption utility relies upon the IDEA or 3DES algorithm. PGP is an encryption solution available for free use to individuals. Corporate users can purchase a license to employ PGP in business communications. PGP is a very popular e-mail protection tool on the Internet.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm SP [547]]

Question 10: Incorrect

Which public key encryption system does PGP (Pretty Good Privacy) use for key exchange and digital signatures?

~~El Gamal~~

Elliptic Curve

Merkle-Hellman Knapsack

RSA

Explanation

PGP uses the RSA public key encryption system for key exchange and digital signatures. PGP is an encryption solution available for free use to individuals. Corporate users can purchase a license to employ PGP in business communications. PGP is a very popular e-mail protection tool on the Internet.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm SP [555]]

Question 11: Correct

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) can be used to provide security for what type of traffic?

Telnet

E-mail

FTP

Web

Explanation

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) can be used to provide security for only Web traffic. HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) works over TCP port 443. HTTPS uses a 40-bit key for the RC4 stream encryption algorithm. HTTPS uses a slightly different Uniform Resource Locator (URL) than that used by HTTP: https://. HTTPS

should not be confused with SHTTP (Secure Hypertext Transfer Protocol) which is a proposed standard for security enhanced HTTP.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm SP [571]]

Question 12: Incorrect

Which of the following communications encryption mechanisms has a specific version for wireless communications?

- HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)
- TLS (Transport Layer Security)
- ~~SSL (Secure Sockets Layer)~~
- IPSec (Internet Protocol Security)

Explanation

TLS has a specific version for wireless communications known as WTLS or Wireless Transport Layer Security. TLS (Transport Layer Security) operates over TCP port 443 or port 80. TLS was developed by Netscape to secure Internet based client/server interactions. TLS is based on SSL, but they are not interoperable. TLS authenticates the server to the client using public key cryptography and digital certificates. TLS encrypts the entire communication session between a server and a client. TLS can be used to protect Web (HTTP) traffic as well as telnet, FTP, and e-mail.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm SP [576]]

Question 13: Incorrect

Which security mechanism can be used to harden or protect e-commerce traffic from Web servers?

- ~~Access control lists~~
- Penetration testing
- Removing unneeded protocols
- SSL

Explanation

SSL is the best solution for protecting e-commerce traffic. SSL provides an encrypted communication tunnel between the Web server and the Web client.

ACLs do not provide protection for e-commerce traffic. ACLs may limit who can initiate such traffic, but it does not protect the traffic itself. Penetration testing may find vulnerabilities in a system, but it does not directly protect e-commerce traffic. Removing unneeded protocols may improve the security of the Web server overall, but it does not directly protect e-commerce traffic.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm SP [800]]

Question 14: Incorrect

What form of cryptography is **not** scalable as a stand-alone system for use in very large and ever expanding environments where data is frequently exchanged between different communication partners?

- Symmetric cryptography
- Hashing cryptography
- ~~Public key cryptography~~
- Asymmetric cryptography

Explanation

Symmetric cryptography is not scalable as a stand-alone system for use in very large and ever-expanding environments where data is frequently exchanged between different communication partners.

Hashing is scalable since everyone uses the same hashing algorithm, but it is not used for secure data exchange, rather it is used to verify integrity. Asymmetric cryptography and public key cryptography are scalable for use in very large and ever-expanding environments where data is frequently exchanged between different communication partners.

References

LabSim for Security Pro, Section 3.6.
[Questions.exm SP [283]]

Question 15: Correct

What form of cryptography is scalable for use in very large and ever-expanding environments where data is frequently exchanged between different communication partners?

- Symmetric cryptography
- Asymmetric cryptography
- Private key cryptography
- Hashing cryptography

Explanation

Asymmetric cryptography is scalable for use in very large and ever-expanding environments where data is frequently exchanged between different communication partners.

Hashing is not used to exchange data securely, rather it is used to verify that integrity has been maintained. Symmetric cryptography, also known as private key cryptography, is not scalable because every set of communication partners needs a shared private key. With only 100 communication partners 4950 shared private keys are needed [n*(n-1)/2].

References

LabSim for Security Pro, Section 3.6.
[Questions.exm SP [323]]