← Back   **Security: Web Security**
Graded Assignment • 30 min

⚙ **Due** Mar 2, 11:59 PM CET

Your grade: 91.66%

Your latest: **91.66%** • Your highest: **91.66%** • To pass you need at least 80%. We keep your highest score.

[Next Item →]

1. Which of the following is false about the two keys used in public key encryption?   1 / 1 point
   ○ One key is public and the other is private
   ○ The public key is openly revealed while the private key must be kept secret
   ○ The public key alone is used for encryption and the private key alone is used for decryption
   ● If you have the public key it is easy to compute the private key

   ⊘ Correct

2. When you are using secure http and sending data between your computer and your bank's computer, where is   1 / 1 point
   the data encrypted and decrypted?
   ○ Encrypted and decrypted each time your message passes through a router
   ● Encrypted in your computer and decrypted in the bank's computer
   ○ Encrypted in your bank's computer before they store the data in a database
   ○ Encrypted in your network card and decrypted by the bank's Internet Service Provider (ISP)

   ⊘ Correct

3. In regards to security, what do we assume about the Internet?   1 point
   ○ That no one can view Internet traffic without a subpoena
   ○ That neither the routers nor the links between the routers are secure
   ● That the entire Internet is completely secure other than WiFi connections
   ○ No one should ever send sensitive information like Credit Card numbers over the Internet

   ⊘ Incorrect

4. This week we've updated our model of how we communicate information via the internet to add in a fifth   1 / 1 point
   mini-layer to the structure in order to protect the confidentiality of transmissions. What is the new list of
   layers and in what order do we list them?
   ○ * Application
       * TCP
       * IP
       * Packet Encryption
       * Link
   ○ * ZIP+Secure
       * Application
       * TCP
       * IP
       * Link
   ○ * Application
       * TCP
       * IP
       * Link
       * Dark Fiber
   ● * Application
       * Secure Sockets
       * TCP
       * IP
       * Link

   ⊘ Correct

5. What is packet sniffing?   1 / 1 point
   ○ When we use detection equipment to see if link speeds are being exceeded
   ● Computers watching packets being transmitted across the network in hopes of finding important or
     valuable data
   ○ When a router looks at the first part of packet to to the routing lookup before the entire packet is
     received
   ○ When a receiving system anticipates a packet before it is received and pre-sends the acknowledgement
     to save time

   ⊘ Correct

6. Which of the following is FALSE about using secure sockets (i.e. https) to send sensitive information like a   1 / 1 point
   credit card across the Internet?
   ○ It requires complex math to decrypt your data
   ○ When using an unsecured WiFi, your data is still protected because of https
   ○ It requires large amounts of computing power to decrypt your data
   ● It is impossible to decrypt your data

   ⊘ Correct

7. Which of the following is NOT a major threat to your data when using secure sockets?   1 / 1 point
   ○ You can be unknowingly redirected to a server different from the one you would like
   ● Someone may see your public key
   ○ There may be a virus on your computer monitoring your keystrokes

   ⊘ Correct

8. Which of the following is not an equivalent name to 'digital certificate'?   1 / 1 point
   ○ Identity certificate
   ○ Public key certificate
   ○ Digital certificate
   ● Private key certificate

   ⊘ Correct

9. What is a digital certificate?   1 / 1 point
   ○ A real-life document used to certify the security of your computer
   ○ An electronic document used to give both public and private keys an identity
   ● An electronic document used to give a public key an identity
   ○ An electronic document used to give a private key an identity

   ⊘ Correct

10. What is a certificate authority?   1 / 1 point
    ● An entity that certifies the ownership of a public key by the named subject of the certificate
    ○ An entity that certifies that you have no virus on your computer
    ○ An entity that tries to ensure secure transactions by attempting to crack encrypted messages online
    ○ An entity that certifies the mathematical relationship between the public and private keys of a system

    ⊘ Correct

11. Which of the following is NOT an indicator of the effectiveness of Verisign as a certificate authority?   1 / 1 point
    ○ Verisign goes to great lengths to store their private keys securely
    ● Verisign publishes its private keys on a little-known web site only available to key owners
    ○ Verisign is used by major manufacturers like Apple and Microsoft
    ○ Verisign has a high success rate for maintaining secure transactions

    ⊘ Correct

12. How does your computer typically know the public key of a certificate authority during secure   1 / 1 point
    communications?
    ● The public key is stored in the operating system by the manufacturer before you buy or install it
    ○ The public key has to be downloaded when you are setting up the computer's web browser
    ○ The public key is emailed to the computer the first time you switch it on
    ○ The computer doesn't use a public key

    ⊘ Correct