CS447-002 - Networks and Data Communications
Possible Quiz Questions (Quiz #10)
For April 22nd, 2024

The following is a list of possible questions for our quiz on April 22nd. Some of the questions will not be asked in the quiz. All the questions that will appear in the quiz will appear exactly as shown below (however, numeric parameters may be changed). The quiz is closed textbook, closed notes and closed neighbors. Note that the questions, which did not appear in this quiz, still may appear in the exams. You will find a solution for these questions during lectures.

#1: One particular factor that makes "network security" hard to achieve lies in "unreliable message transmissions" in the Internet. Mention three (different) examples of "unreliable message transmissions"

#2: Routers can be a cause of more serious security issues than switches. Why (mention the property of routers that makes a clear contrast with switches for their security risks)?

#3: What are "active (network security) attacks"?

#4: What are "passive (network security) attacks"?

#5: What are the four (most) popular existing active (network security) attacks?

#6: What are the two (most) popular existing passive (network security) attacks?

#7: What is (are) the major protection(s) against the release of message contents attacks?

#8: What is (are) the major protection(s) against the modification of message contents?

#9: What is (are) the major protection(s) against the masquerading the identity of information sender and receiver?

#10: What are the three required properties for cryptography methods?

#11: What is "the symmetric cryptography"? What is its primary weakness (mention the one identified as its primary weakness in the previous CS447 lecture)?

#12: What is "the asymmetric cryptography"? What is its primary advantage (mention the one identified as its primary advantage in the previous CS447 lecture)?

#13: If a payload data is encrypted using a private (secret) key (or a asymmetric cryptography), what (security) protection does it offer to (legitimate users)?

#14: If a payload data is encrypted using a public key (or a asymmetric cryptography), what (security) protection does it offer to (legitimate users)?

#15: What is "authentication"?

#16: What is “authorization”?

#17: What is “access control”?

#18: What is “data confidentiality”?

#19: What is data integrity”?

#20: What is “nonrepudiation”?

#21: What is (are) the major protection(s) against modification of message attacks?

#22: What is (are) the major protection(s) against replay attacks?

#23: What is (are) the major protection(s) against masquerade attacks?

#24: What is (are) the major protection(s) against traffic analysis attacks?

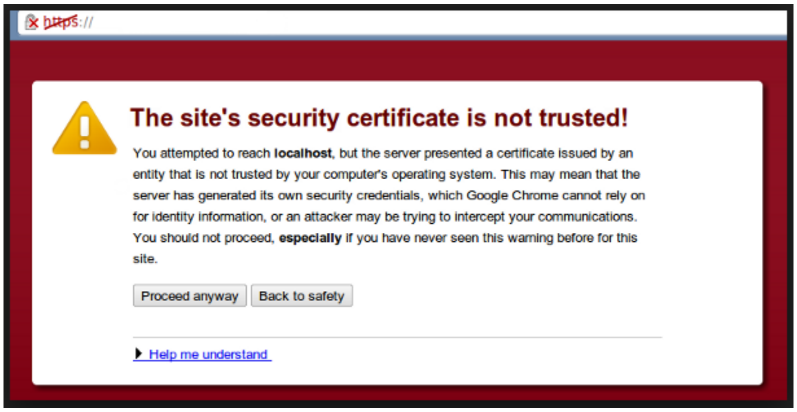
#25: What is “message digest”?

#26: Why is it necessary to encrypt the message digest by the private (secret) key of a sender?

#27: What does “digital certificate” certify?

#28: Regarding digital certificates, after your local web browser downloads a digital certificate, describe how the local browser confirms the correctness of the public key (describe the procedure)?

#29: How is the following “certificate error” caused (technically explain how the “certificate error” is caused)?



The site's security certificate is not trusted!

You attempted to reach **localhost**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.

#30: How are “the root CAs” different from “(other) CAs”?

#31: What is (are) the major protection(s) against denial of service (DoS) attacks?

#32: What is (are) the major protection(s) against distributed denial of service (DDoS) attacks?