LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2017-03-16
08-12

Permissible aids
English dictionary (printed, NOT electronic)

Teacher on duty
Marcus Bendtsen, 0733-140708

Instructions
There are 4 main questions on the exam. Your grade will depend on the total points you score. The maximum number of points is 34.

Answers in English only

Grading
The following grading scale is preliminary and might be adjusted during grading.

Grade	C (3)	B (4)	A (5)
Points required	20	26	30

1. System Security (10 points)

a) Explain what a DMA attack is, and give an example of how it may be used by an attacker. (2 points)

b) DMA attacks are made possible due to a design decision that violates at least one of Saltzer and Schroeder's secure design principles. Pick the **one** design principle whose violation you think most strongly contributes to the vulnerability. Name that principle, briefly explain it, and explain how it is violated in the context of DMA attacks. (Note: Answering with more than one principle will lead to a reduction of points.) (2 points)

c) Many modern programs, such as PDF readers and web browsers, utilize sandboxing to reduce the attack surface of software exploits. The complex rendering logic executes with minimum privileges, while privileged operations are mediated and carried out by a much smaller software component. This design embodies two of Saltzer and Schroeder' secure design principles. Name and explain these two principles, and explain how they are used in the above context of software sandboxing. (4 points)

d) In a sentence or two, explain the concept Root of Trust. In the context of the Trusted Computing Group architecture, what is the Core Root of Trust for Measurement? (2 points)

2. Identification and authentication, Biometric user authentication (8 points)

a) Define identification vs identity verification. (2 points)

b) What makes uniqueness an important quality when choosing a biometric trait? (2 points)

c) Attack on the template database of a biometric system: Describe what leakage is and what makes it a serious problem in biometric systems. (4 points)

3. Network security (10 points)

a) Suppose you are in charge of securing a new enterprise corporate network. List the main principles you will apply. (2 points)

b) Compare WiFi security modes WEP, WPA and WPA2. What is similar and different? Describe their use of ciphers. (4 points)

c) Much of Internet security especially e-commerce is based on TLS/SSL. (4 points)

   i. What is the difference between those two?

   ii. What are certificates, how those are used and validated, what are possible problems?

   iii. Describe, in two sentences each, five basic attacks prevented by proper use of TLS/SSL.

4. Risk analysis, cognitive bias, BCP/DRP and PS (6 points)

a) Explain how ALE values are calculated. Make sure that you explain each factor, and when possible, break down the factor to its individual components and explain these as well. (2 points)

b) Describe the experiment conducted by Tversky and Kahneman which showed how the cognitive bias "Anchoring" may manifest itself. Don't forget to explain what "Anchoring" entails. (2 points)

c) Explain, including an example, how attack trees are created. (Note: Just an example is not enough, you need to explain how the tree is created, annotated and the different components at your disposal). (2 points)