LiTH, Linköpings tekniska högskola
IDA, Institutionen för datavetenskap
Nahid Shahmehri

Written exam

TDDD17 Information Security

2009-03-09

8-12

Permissible aids

Dictionary (printed, NOT electronic)

Teacher on duty

Shanai Ardi, 013-282608

Instructions

There are 5 general questions and 5 in-depth questions. The general questions are from G1 to G5, and the in-depth questions are from D1 to D5. The questions are grouped pair-wise under their corresponding topic.

You have to answer at most 3 general questions and 3 in-depth questions. You must answer at least one of the questions for each topic. A correct answer for a general question gives you 2 points, and a correct answer for an in-depth question gives you 6 points. To pass the exam you need to accumulate at least 3 points from general questions and 9 points from in-depth questions. The exam grading depends on the total number of accumulated points.

Attention

If you answer more than 3 (general) + 3 (in-depth) questions we will randomly choose 3 + 3 answers for correcting the exam, while the rest of the answers will be discarded.

System Security

G1 What is the purpose of a trusted platform module (TPM)? What is the role of the TPM in secure boot?

D1 Explain the purpose of the Biba integrity model, and explain how the model works, including its interaction with discretionary access control. Be precise in your explanation. Explain at least one practical difficulty in employing the Biba integrity model in a typical system

Identification and Authentication

G2 Tokens often employ cryptography to prevent attacks like phishing, skimming etc. But bad implementations of the algorithm can make it possible to find out the key with non-invasive attacks. Name and very shortly describe two such attacks, and indicate some step in algorithm implementation, which can prevent these attacks or at least make them significantly harder!

D2 The course literature (Maltoni et al.) contains a diagram stating that on a Receiver Operation Curve for a biometric system, you typically find forensic applications towards the low FNMR (=FRR) end, high security applications towards the low FMR (=FAR) end, and civilian applications in the area of EER. Of course you can ask yourself why "civilian applications" cannot be high security applications. But disregarding that point:

1) Discuss the advantages and disadvantages for each of these three types of applications if they are placed as indicated by that diagram!

   Especially discuss the relevance of placing "civilian" (=non-critical) applications near the EER point!

2) Changes in population sizes can change the desirability of the chosen operation point. For example a large company with many employees, a large airport with many passengers etc. may choose a different balance between the FMR and FNMR rates compared to smaller operations of the same kind, which have the same basic demands for security. Explain this phenomenon, for example via an example! Do so for both the case of choosing a smaller FMR and for choosing a smaller FNMR!

Network Security

G3 Physically separating a network from the Internet does not prevent attacks on the network. Briefly explain two ways an isolated network could be attacked that are reasonably probable in reality.

D3 Explain why DNS cache poisoning can be such a serious attack, giving at least one concrete example of potential consequences of a DNS cache poisoning attack.

Explain to what degree, and roughly how, IPSec and TLS can mitigate the effects of DNS cache poisoning attacks in general, and the consequences in your example in particular.

Risk Analysis

G4 What can an attacker learn by “admin | administrator” query in Google?

D4 Explain CORAS security risk analysis method, and through an example show how it can be applied.

Business Continuity Planning, Physical Security

G5 Define the term "disaster" in the context of a bcp.

Define what a bcp is.

Explain why an organization or company should have a bcp.

D5 What are the typical steps in creating a bcp? Discuss each step briefly and give examples.

Name and give examples from three different areas where an organization or a company needs to do recovery.

Explain three different methods for testing a bcp.