

Exame de Segurança de Sistemas e Dados (SSD)

Época Normal – 2023/2024

Data: 07/06/2023 | Duração: 2h

Question 1

What do you understand by "high water line" and "low water line" in the context of a MLS (Multilevel Security)?

Question 2

Explain what Chord is, and its differences from Kademlia, explaining the internal processes of Chord.

Question 3

In the context of SS7 architecture, describe 4 possible attacks on SS7, and globally what is the impact for its use in 2AF (Two-Factor Authentication).

Question 4

Explain the advantages of using FIDO in a Federated authentication system, showing the diagram for a typical usage scenario, explaining all entities involved.

Question 5

Describe the problem described in the paper "The Confused Deputy", giving a solution for its mitigation.

Question 6

Describe the k-anonymity model, explaining what a quasi-identifier is, and finally 3 attacks against the model.

Question 7

Explain what the purpose of Stuxnet is, enumerating the attack vectors used and the physical mechanism where it finally acted.

Question 8

Explain what a rootkit is, listing the 3 classification categories, giving an example (with description) for each category.

Question 9

Say if a program can be completely obfuscated, justifying your answer.

Question 10

Explain what a DRM system is, detailing its relationship with cryptography and "scrambling", and finally an example of its implementation.

End of Exam