Computer Security Coursework October 2020 Session

Version: 27/10/2020

Part 1: Operating System and Network Security

1. Airport Security

You are chief security officer for the main airport in your city. Computer Security for airports is both very complex and very important. It is important because airports are high profile pieces of national infrastructure that are frequently targeted by criminals, protestors and terrorists. It is complex because a lot of different types of people use their networks and computer systems:

- Airport staff that are directly related to high security activities such as air traffic control or passenger security checks
- Other airport staff, for example, back office staff and baggage handlers
- Staff of companies that operate from the airport, including airlines as well as shops and restaurants
- Passengers, who use airport WIFI and need to know about flight times and other information

Many of the systems used by these different people will be different from each other (e.g. the baggage handling system or a restaurants booking system), but there are systems, such as the flight take off and arrival schedule that almost everyone needs access to, though in different forms and with different levels of access.

As a security officer you need to keep up to date on possible threats to the organisation. For this coursework, you should research 3 specific threats that could affect an airport (e.g. a specific piece of malware or a specific type of DDoS attack), describe that threat and suggest a security mechanism to protect against it, and explain how it will defend against the attack.

You could, for example use articles in the Online library for your research. All sources must be fully referenced. Here are some starting points for your research:

Quarterly reports of threat statistics from Kaspersky

https://web.archive.org/web/20200912123817/https://securelist.com/all/?category=919

IEEE Security & Privacy

https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013

IEEE Access

https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639

Mark Scheme

For each of the three attacks:

Has the student explained the attack?

- 0: No, or the explanation is incorrect
- 4: Yes, but the explanation is missing elements, or has minor errors or the attack is not relevant to the situation
- 5: Yes, but the explanation shows little evidence of independent research
- 7: Yes, the explanation is clear and correct as far as I can tell, and include good evidence of independent research
- 8: Yes, the explanation is clear and correct as far as I can tell, and include evidence of deep independent research and important insights
- 10: Wow, this is a professional level analysis of a security threat citing many sources and adding new insights to the research

Has the student suggested realistic defences, and explain how they protect against the attack?

- 0: No, or the explanation is incorrect
- 4: Yes, but the explanation is missing elements, or has minor errors, or is not fully appropriate to the attack
- 5: Yes, but the explanation shows little evidence of independent research
- 7: Yes, the explanation is clear and correct as far as I can tell, and include good evidence of independent research
- 8: Yes, the explanation is clear and correct as far as I can tell, and include evidence of deep independent research and important insights
- 10: Wow, this is a professional level analysis of the application of a defensive technique citing many sources and adding new insights to the research

Part 2: Cryptography

2. Search the internet and learn about t the Trifid Cypher.

       a. Make the appropriate grids using the key phrase *Baseball is my favourite sport*

                                                                                            [5]

       b. Encrypt your name using those grid and block size 5. Show your work

                                                                                        [5]

       c. Decrypt the string: RLQREERRLVVTV

                                                                                       [10]

3. We wish to use the RSA to encode the message: 20.

       a.   Explain why N cannot be 3*7

                                                                                          [2]

   Let N be 5*7

       b.   Compute $\Phi(N)$

                                                                                          [2]

       c.   Compute an appropriate value for e. Explain your answer

                                                                                          [4]

       d.   Compute an appropriate value for d. Explain your answer

                                                                                          [4]

       e.   Encode the message = 20. Explain your answer

                                                                                      [4]

       f.   Decode the encoded message. Explain your answer

                                                                                      [4]