Exam Guidelines

1. This exam consists of 5 questions for 10 points each.
2. You have 3 hrs to attempt this exam. If you have special permissions, you are allowed 25% more time.
3. This is a bring your own device exam. Hence, you are allowed to use your laptop for the exam.
4. This is an open-resource exam. You are allowed to use all academic resources (articles, book chapters, Mitre Att&CK framework, lectures and lecture notes) for the exam.
5. Please provide proper references for the arguments presented by you.
6. You are allowed to use https://translate.google.com and https://www.dictionary.com .

Topic: Economics

Model question:

Consider the following document to answer this question:

https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_25.pdf

According to Anderson et. al (2019):

"It would be economically rational to spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more on response."

Do you agree with this statement? Explain your reasons. In your opinion what is the potential of cybercrime to damage small and medium sized companies? Explain in terms of the costs incurred due to cybercrime.

Answer guide:

1. Give your opinion + State two reasons to justify your opinion + Explain (with example/ reference) the stated opinions **(2 + 2 points)**. **Note that explanations of the arguments given are in addition to stating your reasons.**
2. **3 points** for mentioning the damages cybercrime can cause to SMEs. Give a list of damages that cybercrime can inflict on SMEs. Reason why some of these damages might be specific for SMEs. You can also provide justification on the oasis of project experience, taking Speakup as an example.

3. **3 points** for validating your answers with cost estimates from the paper. Potential may be explained in term of severity and potential harm done to the company. Citing relevant losses from the paper is necessary.
4. Deduction of upto **3 points** if relevant references are not provided.

Topic: Security Management Models

Model question:

Habibzadeh et. al. suggests that, “Smart city applications are poised to create security vulnerabilities”. Taking into account the discussion in this paper answer the following questions:

1. Use an attack tree to analyse the steps an attacker may take to impact the availability of IT systems in a smart city. In your opinion, what measures can smart city management take in order to defend against availability attacks. (6 points)
2. Discuss the role of security management frameworks like NIST and ISO 27000s in validating security of smart city residents. (4 points)

Answer guide:

1. A. Attack tree (4 points)
    a. Vulnerabilities/attacker actions considered and their relevance for smart cities. **(3 points)**
    b. Referencing to Mitre Att&CK framework. **(1 point)**

➢ B. Identify measures to be taken by smart city management to protect against availability attacks. Opinion of the student on why these measures are relevant. **(2 points)**

2. A. Discuss how a PDCA cycle approach can ensure validity of security solutions in place. **(2 points)**

➢ B. Give examples from at least two of the frameworks on how they can be helpful in validating security in smart cities. (**2 points)**

➢ C. Deduction of **2 points** if the answer is not smart city specific.

Topic: Real World Security

Taking into account the lecture by Sorin Iacob on “Security management in defence”, Elaborate on how the security practices in a defence organisation different from that in a business? On the basis of at least three points state the difference between a business and a defence organisation. Explain with examples how these differences in organisations correspond to risk mitigation strategies? In your opinion, do you think Gordon and Loeb model can be use by a defence organisation to decide on security investments? Explain why?

Answer guide:

1. Three differences between a business and defence organisation. **(3 points)**
2. Mapping identified differences to change in security strategy. **(2 points)**
3. Examples and explanation of changes in security strategy. **(2 points)**
4. Opinion on gordon and loeb model use with reason. **(1 point)**
5. Reasons for why or why not gordon and loeb model maybe used to decide on security investments. **(2 points)**

Topic: Cryptographic Tools and Protocols

Model questions:

TLS is a very common cryptographic protocol that achieves multiple security goals. Assume a banking app that is secured using TLS.

1. TLS provides server authenticity. How does that work and give an example why this is useful for the banking app? Discuss potential issues with the current solution. **(3pts)**
2. TLS provides server confidentiality? How does that work and give an example why this is useful for the banking app? **(2pts)**
3. With the new version TLS 1.3 the number of ciphersuits has been reduced. Specifically, only ciphersuits that use the Diffie-Hellman key exchange are supported by TLS 1.3. ETSI proposed an extension for TLS 1.3 they called eTLS. Particularly, ETSI summarizes the TLS 1.3 handshake as follows together with the proposed modifications (https://www.etsi.org/deliver/etsi_ts/103500_103599/10352303/01.01.01_60/ts_10352303v010101p.pdf page 9):
    a. *The client generates an ephemeral Diffie-Hellman public and private key. The public key is transmitted to the server in a “key_share” message with a random client nonce.*
    b. *The server generates an ephemeral Diffie-Hellman public and private key. The public key is transmitted to the client in a “key_share” message with a random server nonce.*

c. The client and server each use a combination of their own private keys and the public key received from the other side of the connection to generate a shared secret.

d. The client and server then use the shared secret along with the initial handshake messages, which include the nonces, to generate a set of handshake traffic keys for encryption of the remainder of the handshake.

e. During the remainder of the handshake, the server sends its certificate encrypted using a handshake traffic key.

f. Upon completion of the handshake, the client and server then use the shared secret along with various elements of the handshake messages, which again include the nonces, to generate a set of application traffic keys for the session.

g. The application traffic keys are used to encrypt further data exchanged between the client and server.

The eTLS key exchange shall use exactly the same messages and procedures to establish a set of session keys as a TLS 1.3 ephemeral Diffie-Hellman key exchange, except for two differences.

i. the server shall use a static public/private key pair at Step 2 [...] and
ii. the server's certificate at Step 5 shall contain visibility information [...] to indicate to the client that eTLS is in use.

The eTLS server shall be provisioned with a static key pair for each elliptic curve (or finite field length) supported by the server. These key pairs may be shared with middleboxes that are authorized to decrypt sessions from the server.

Given this description, what security property can be achieved with a key exchange protocol as explained in steps a-g. Explain this security property. Explain how the modifications in i. and ii. enable middleboxes to decrypt sessions. Discuss the consequences of this modification; include the security property from the previous question into your discussion. **(5pts)**

Answer guide:

1. Explanation of certificates and PKI **(1pt)**
   User can verify that he is connected to bank server (mitigating phishing) **(1pt)**
   Discussion on root certificates and implicit trust in ALL root certificates that are pre-installed **(1pt)**
2. Secret key between client and server established and then symmetric crypto is applied (**1pt)**
   Sensitive information like account balance is protected and cannot be eavesdropped. (**1pt)**

3. Mentioning and explaining Perfect-forward secrecy and time component **(2pt)**
   Middleboxes can act as person-in-the-middle, hence reconstructing the secret key and then eavesdrop all messages. (**1pt)**
   General discussion on weakening security **(1pt)**
   Realizing that PFS is not given anymore, since the static private key from server can be leaked and hence affect past sessions (1pt)

Topic: Web-, Internet- and System Security

Model questions:

1. What is the domain name system (DNS) used for? Give an example. **(2pts)**
2. Your company's internet web page is reached via www.company.nl. Your client enters this namespace into his browser's address bar to visit the web page. Explain what is happening in the background so that the client is connected to your company's server. **(2pts)**
3. The web pages can be accessed via http://login.company.nl and asks the user to enter her password. Why is this not a good idea and what should be used to improve the situation? Assume you are an attacker who targets a user logged in to an open WiFi network in a cafe. Sketch your attack strategy. **(3pts)**
4. In case the user has forgotten her password, she can click a button for password recovery via e-Mail. Here, the service sends the originally used password in plaintext to the registered e-mail address. Explain, why this password recovery service is fishy. What is used in practice instead? **(3pts)**

Answer guide:

1. Correct explanation of mapping from names to IP addresses **(1pt)**
   Correct example **(1pt)**
2. Explanation of the hierarchical structure of DNS **(1pt)**,
   correct mapping of this structure to the example, i.e. root NS → nl domain zone → company domain zone resolves the actual IP address **(1pt)**
3. Discussion that payload via HTTP is transmitted in plaintext **(1pt)**,
   stating httpS (/TLS) as a secure alternative (**1pt**).
   Description of a Person-in-the-middle attack with the open WiFi by tricking the user to connect to a fake WiFi or eavesdropping the open WiFi connection **(1pt)**
4. E-mails are transferred in plaintext (**1pt)**
   The password should be stored in hashed form on the server and explanation of one-wayness **(1pt)**

Explaining password reset functionality via random token sent to the e-mail address (**1pt)**