1. What are the main components of a real-time NIDS (network intrusion detection system)? Why is it important that a NIDS performs full TCP/IP stream assembly? Describe two ways to render a real-time NIDS ineffective.

2. Virtualization is back and this time computer security folks are claiming that it could be used to provide better security for applications and services. Virtualization architectures assume a trusted hypervisor that supports a number of virtual machines. Since the hypervisor is trusted, its complexity should be kept to a minimum and it should only support minimum functionality that must be implemented at this level. Briefly describe what such functionality is and how its execution is isolated from the execution of the other components of the system.

Device drivers require access to hardware resources which must be mediated by trusted software. On the other hand, large and buggy device drivers do not belong in the hypervisor. How device drivers are typically implemented in such systems?

In the last part of this question, you have to explore how one can monitor virtual machine execution in a secure way. There may be mechanisms in the hypervisor or one or more designated virtual machines may implement certain monitoring functions. Such functions may observe a target virtual machines activities such as resource requests as well as its internal execution. Comment on approaches for such monitoring and what benefits it may offer.

3. Imagine a very useful cryptographic scheme has been designed and published together with a proof of security. Since then it got widely deployed. Unfortunately, in a few years the scheme got broken, and it was all over the news. Describe possible scenarios of how it can happen (that a provably secure scheme gets broken).

4. A key security problem enterprises face is the labeling of proprietary and sensitive data. Such labels can be helpful in enforcing policies that certain data may not cross designated machine or application boundaries. Consider a commercial setting where data labels may reflect the type of information (e.g., pay-roll, employee evaluations, marketing plan etc.). Users in the organization have roles and a policy may be defined in terms of what roles can access what kind of information. Discuss the feasibility of developing a data labeling scheme for such an environment and how it can be implemented? In your answer, clearly define the types of labels, how they can be combined, compared and related. Sketch an example policy based on such labels and discuss how it can be enforced. Also, discuss if current operating systems or services implemented on top of them can allow the enforcement of such a mandatory policy.
5. Describe how to build and deploy a HIDS (host-based intrusion detection system) that monitors program executions via system call analysis. Describe two types of attacks that can evade such a HIDS.

6. You were hired to consult for a company, which developed a public-key encryption for their security needs. The scheme is very similar to well-known ElGamal. The secret key \( x \) is a random element of \( \mathbb{Z}_p^* \), where \( p \) is a large prime. The public key \( y \) is \( g^x \mod p \), where \( g \) is a generator of \( \mathbb{Z}_p^* \). Assume that \( p \) and \( g \) are publicly known. To encrypt a message \( m \) from \( \mathbb{Z}_p^* \), the encryption algorithm picks \( r \) at random from \( \mathbb{Z}_p^* \), and outputs a ciphertext \((y^r \mod p, g^r \cdot m \mod p)\). One can check that decryption can be properly defined. The company wants to know if this scheme is secure. What is your assessment of the schemes security? You do not have to provide formal proofs or attacks, but try to be as detailed as possible in your verdict, justification and recommendation.

7. A large portion of attack traffic on the Internet comes from insecure home computers. It is said that this is because average home users don’t care about security. Do you agree with such a statement? What needs to be done to make home computers secure?

8. You participate in a very important security project. You are asked to suggest cryptographic schemes to be implemented with the main criteria of them staying secure for at least 40 years. Please describe how will you approach the task of selecting suitable schemes and their parameters. What do you need to know about the application? What kind of guarantees can you give? You can provide examples.