Assessment criteria TDDE62

Module **TEN1**

Learning goal	Criteria for grade 3		Criteria for grade 5
1. explain and use the security terminology and security principles presented in the course	- Be able to name and briefly describe attack methods and defense mechanisms within system and network security. - Know and be able to describe important principles for the design of secure computer systems and networks.		- Be able to describe in detail attack methods and defense mechanisms within system and network security. - Be able to relate security principles within system and network security to techniques and use cases in practice.
2. in a given context, a. identify security weaknesses in a given system or network, b. identify, and explain in detail, the security threats against the system or network, c. suggest suitable technologies, methods, or design decisions for mitigating the security threats against the system or network	Network security	- Be able to briefly describe security weaknesses in common network protocols and communication techniques. - Be able to briefly describe protocols and techniques for secure communication. - Be able to explain the operation of common network protection mechanisms and protection techniques (e.g. firewalls, IDS) and the types of threats they can mitigate.	- Be able to explain in detail security weaknesses in common network protocols and communication technologies. - Be able to explain in detail protocols and techniques for secure communication.
	System security	- Be able to account for classic security architecture and access control methods in hardware and system software, as well as their limitations. - Be able to briefly describe modern techniques for enhanced security in hardware and system software (e.g. trusted computing, isolation, protection against specific attack methods) - Be able to describe the most common types of malicious code, and the threats they pose to a computer system. - Be able to briefly describe common methods for detection and protection against malicious code on different types of devices.	- Be able to explain in more detail modern techniques for enhanced security in hardware and system software. - Be able to describe in more detail common methods for detection and protection against malicious code. - Reason in detail about the interaction between attackers and defenders in terms of malicious code, and how this has affected the technical development of both attack and defense techniques. - Be able to reason about difficulties and pitfalls when using machine learning/AI for malware detection.
	- Be able to describe the consequences of a successful attack against a given system/network.		- Be able to contrast different technologies for protection against a certain type of threat, and reason about its pros and cons when it comes to, e.g. performance, ease of use, resource usage and cost.
3. explain and apply the techniques and methods covered in the course for ensuring user privacy	- Be able to explain important concepts in privacy (e.g., anonymity, unlinkability, hard vs soft privacy) - Know the most important types of risks/threats in privacy. - Be able to briefly describe well-known techniques for ensuring privacy in digital communication. - Be able to briefly describe important methods for maintaining privacy when processing data in databases, and to be able to apply these methods to simple “toy” problems		- Be able to explain in detail important methods for maintaining privacy when processing data in databases, as well as reason about the degree of protection they offer in a given situation.

For grade 4: all criteria for grade 3 met, as well as most of the criteria for grade 5.

Module **LAB1**

Learning goal	Criteria for grade G (Pass)
4. using some selected technologies, design and implement solutions to given security problems, based on a set of security requirements	Based on a given requirement specification for each task, be able to: (1) implement a firewall and intrusion detection policy for a typical small business network and (2) design and implement an authentication solution using an established trusted computing technology, and document the respective solution in a written laboratory report.

Examination

The exam includes 4 parts, corresponding to the 4 subjects *network security*, *system security (hardware and system software)*, *system security (malware)*, and *privacy*.

For grade 3, at least 40% of the maximum score is required on each of the 4 parts, as well as 55% of the total score.

For grade 5, at least 70% of the maximum score is required on each of the 4 parts, as well as 85% of the total score.

For grade 4, requirements for grade 3 must be met, as well as 75% of total points.

Preliminary total score is 32, with preliminary score distribution:

	network security	system security	malware	privacy	**Total**
Max	**10**	**10**	**6**	**6**	**32**
For grade 3	4	4	2.5	2.5	18
For grade 4	”	”	”	”	24
For grade 5	7	7	4	4	27