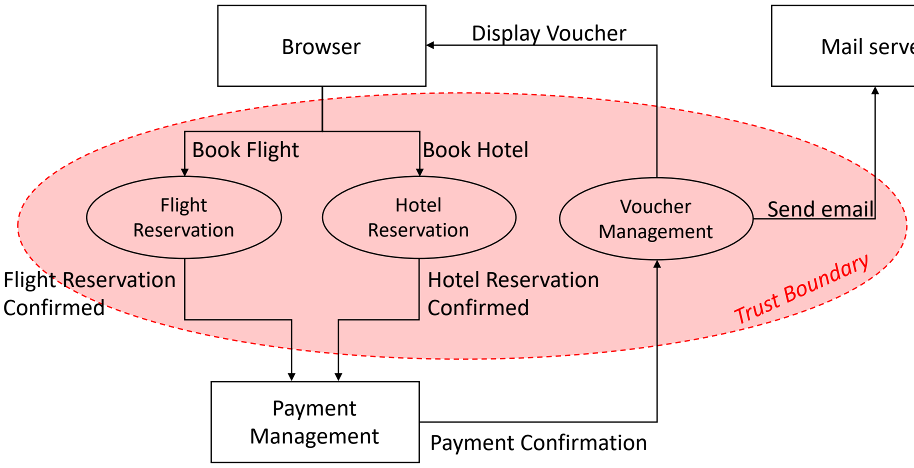
Security Governance – Exam Fac-Simile
Master of Science in Cyber Security
Master of Science in Engineering in Computer Science

DISCLAIMER: The goal of this document is just to provide an idea of possible types of question that can be posed during exam. This should not be considered in any case as a fixed template concerning both the structure of the exam and the possible topics covered that are indeed all those included in the syllabus.

Q1: Describe the main objectives of the NIST Cyber Security Framework and its structure.

Q2: With reference to depth dimension of Von Solms's ISG model, describe the main characteristics if the Directive vertical block.

Q3: Let's consider a software application supporting the travel reservation process. The application DFD is shown in the following Figure

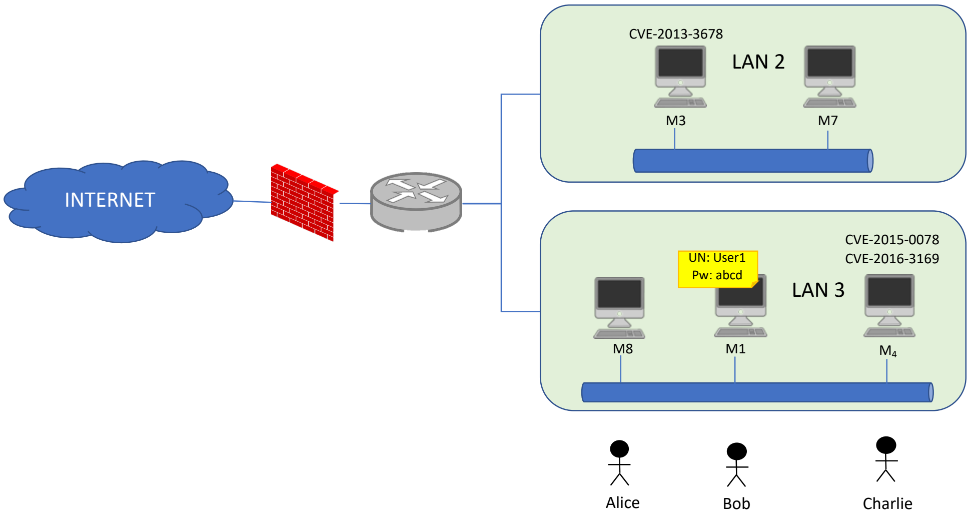


Elicit the main threats to the reservation system by assuming that:

- communications between the Browser and the reservation processes are implemented by using non-encrypted protocols
- Communications between the reservation processes and the payment management system are implemented trough secure communication protocols
- The mail server is hosted managed internally to the company but from another department.

For everything that is not clearly stated, the student should make assumptions and provide a consistent model.

Q4: Consider the fragment of the network depicted in the following Figure



Assess the risk that an attacker is able to compromise the availability of M3 by assuming that:

- M3 is reachable only from machines in LAN2 and from M4
- Alice has user access to M8 and she has the bad habits of sharing her credentials with all her colleagues.
- Bob has user access to M1 and he has poor memory. He leaves all his credentials written around on post it.
- Charlie has access to M4 and he is very careful in managing his credentials. However, he tends sometimes to leave his machine logged in while he is out for a coffee.
- The details of the three CVE are reported in the following

CVE-2013-3678	
Multiple unspecified vulnerabilities in SAP Governance, Risk, and Compliance (GRC) allow remote authenticated users to gain privileges and execute arbitrary programs via a crafted (1) RFC or (2) SOAP-RFC request.	
Base Score (CVSS v2)	9.0 HIGH
Access Vector (AV)	Network
Access Complexity (AC)	Low
Authentication (AU)	Single
Confidentiality (C)	Complete
Integrity (I)	Complete
Availability (A)	Complete
Additional Information:	Provides unauthorized access Allows unauthorized disclosure of information Allows disruption of service

CVE-2015-0078	
win32k.sys in the kernel-mode drivers in Microsoft Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly validate the token of a calling thread, which allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."	
Base Score (CVSS v2)	7.2 HIGH
Access Vector (AV)	Local
Access Complexity (AC)	Low
Authentication (AU)	None
Confidentiality (C)	Complete
Integrity (I)	Complete
Availability (A)	Complete
Additional Information:	Provides administrator access Allows unauthorized disclosure of information Allows disruption of service

CVE-2016-3169	
The User module in Drupal 6.x before 6.38 and 7.x before 7.43 allows remote attackers to gain privileges by leveraging contributed or custom code that calls the user_save function with an explicit category and loads all roles into the array.	
Base Score (CVSS v2)	6.8 MEDIUM
Access Vector (AV)	Network
Access Complexity (AC)	Medium
Authentication (AU)	None
Confidentiality (C)	Partial
Integrity (I)	Partial
Availability (A)	Partial
Additional Information:	Provides unauthorized access Allows unauthorized disclosure of information Allows disruption of service