UNIVERSITY OF OSLO

Faculty of Mathematics and Natural Sciences

<u>Paper version of digital exam</u>
Version 2017.06.10

Exam in	**INF3510 – Information Security**
Day of exam:	**9 June 2017**
Exam hours:	**9:00h – 13:00h**
This examination paper consists of:	**X pages**
Appendices:	**None**
Permitted materials:	**Language dictionary**

Make sure that your copy of this examination paper is complete before answering.

Answer all 10 questions in this examination paper.

Answers can be written in English or in Norwegian.

The 40 questions are grouped under 10 themes that correspond approximately to 10 of the lectures in this course. Each group of questions gives 10 points. The whole exam gives a total of 100 points.

Be concise. When answering a question it is often sufficient to write a single expression or sentence to describe

Section 1: General Security Concepts.

1. Write the definition (approximately) of *information security* according to ISO27000. (2p)
2. Write the definition (approximately) of *availability* according to ISO27000. (1p)
3. Which is the most relevant *threat against availability*? (1p)
   i) Cryptanalysis, ii) Zero-day exploit iii) SQL injection, iv) Phishing email, v) DDoS attack
4. Select the two (2) *most general* categories of authentication. (2p)
   i) Entity authentication
   ii) Knowledge-based authentication
   iii) Data authentication
   iv) Token-based authentication
   v) User authentication
   vi) Server authentication
5. Explain *authorization* in a way consistent with the definition of confidentiality. (1p)
6. Indicate whether each characteristic in the left column is relevant for *non-repudiation* or *authentication* **of data origin**. Some characteristics are irrelevant, in that case select *'irrelevant'*. (3p)

	Authentication	Non-repudiation	Irrelevant
Implemented with MAC			
Proof to both recipient and to any 3rd party			
Proof only to recipient			
Always multi-factor			
Implemented with digital signature			
Always based on biometrics			

Answer

1. 2p for: Information security is the preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.
2. 1p for: Availability is the property of being accessible and usable upon demand by an authorized entity.
3. 1p for: DDoS attack
4. 2p for: i) Entity Authentication and iii) Data Authentication.
   (1p for each correct answer, 0p for wrong or no answer)
5. 1p for: Authorization is to specify access and usage permissions for entities, roles or processes.
6. 0.5p for each correct, -0.5p for each wrong, 0p for no answer, max 3p, min 0p

	Authentication	Non-repudiation	Irrelevant
Implemented with MAC	✓		
Proof to both recipient and to any 3rd party		✓	
Proof only to recipient	✓		
Always multi-factor			✓
Implemented with digital signature		✓	
Always based on biometrics			✓

Section 2: Information Security Management

7. State the meaning of the abbreviation ISMS (1p)
8. Select the relevant standard for each topic in the left column. (2p)

	ISO27000	ISO27001	ISO27002	X.800
ISMS				
Security Architecture				
Security Controls				
Security Vocabulary				

9. Briefly explain the term security control, and mention the three (3) general categories of security controls. Give one example security control of each category. (4p)
10. Mention the three (3) functional types of security controls. Give one example security control of each functional type. (3p)

Answer

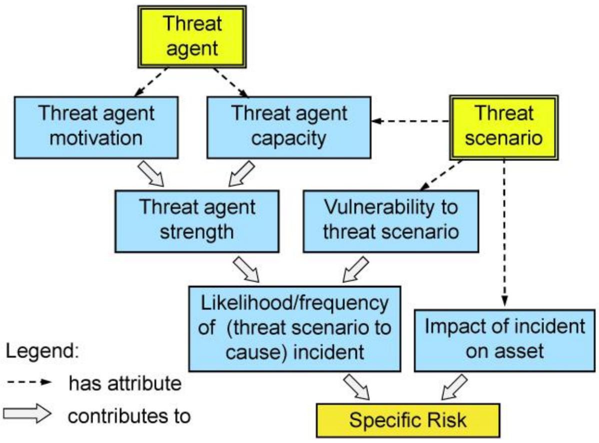
7. 1p for: ISMS: Information Security Management System.
8. 0.5p for each correct, 0p for each wrong or no answer, max 2p, min 0p

	ISO27000	ISO27001	ISO27002	X.800
ISMS		✓		
Security Architecture				✓
Security Controls			✓	
Security Vocabulary	✓			

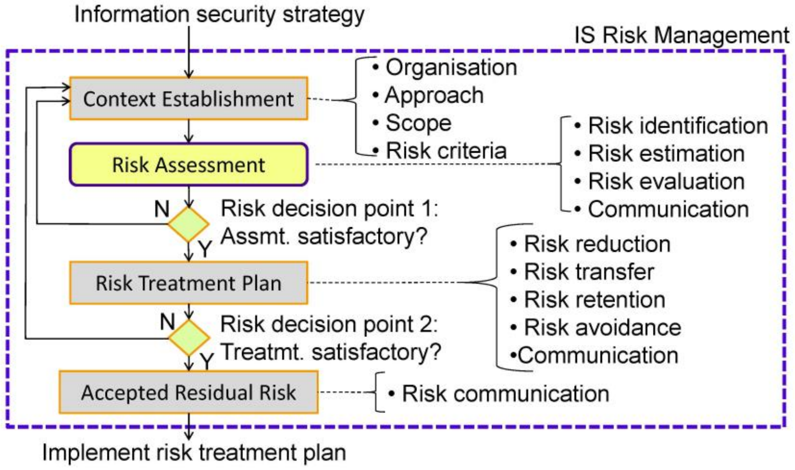
9. 1p for: Security controls are practical mechanisms, actions, tools or procedures that are used to provide security services.
   1p for: Physical controls, with relevant example
   1p for: Technical controls, with relevant example
   1p for: Administrative controls, with relevant example
10. Functional types of security controls
    1p for: Preventive controls, with relevant example
    1p for: Detective controls, with relevant example
    1p for: Corrective controls, with relevant example

Section 3: Risk Management

11. Select two (2) blue elements from the diagram below that must be specified in a typical practical method for qualitative assessment of risks. (2p)



12. Select the responsible entity for each of the risk decision points (RDP) in the diagram. (2p)



i) The risk analysis team is responsible for RDP 1.
ii) The company management is responsible for RDP 1
iii) The risk analysis team is responsible for RDP 2.
iv) The company management is responsible for RDP 2.

13. Risk Identification and Risk Estimation are different steps as part of Risk Assessment in the risk management process (see diagram of Q12).
i) Mention two (2) elements of Risk Identification. (2p)
ii) Mention two (2) elements of Risk Estimation. (2p)

14. Select two (2) relevant approaches for identifying/modelling threat scenarios. (2p)
i) Asset-centric threat modelling
ii) Attacker-centric threat modelling
iii) Impact-centric threat modelling
iv) Vulnerability-centric threat modelling

Answer

11. 1p for: Likelihood of incident
1p for: Impact of incident on assets
(0p for wrong or no selection)

12. 2p for: i) and iv)
(-1p for each wrong, 0p for no selection, max 2p, min 0p).

13. 1p each for any two of:
- Identification of assets
- Identification of threats
- Identification of existing controls
- Identification of vulnerabilities
- Identification of consequences

1p each for any two of:
- Assess asset values and impacts
- Assess incident likelihood/frequency
- Determine/compute risk levels

14. 2p for: i) Asset-centric threat modelling and ii) Attacker-centric threat modelling
(0p for a wrong or no selection).

Section 4: Cryptography.

15. Some well-known hash functions are MD5 (Message Digest 5), SHA-1 (Secure Hash Algorithm 1), SHA-2 and SHA-3. Indicate their current security status below. (2p)

	No attack exists	Attacks exist
MD5		
SHA-1		
SHA-2		
SHA-3		

16. The SHA-2 hash algorithm can have four (4) different output block sizes. Specify three of the four output block sizes (in bits) of the SHA-2 hash algorithm. (3p)
17. Alice wants to send a message *M* together with a message authentication code MAC(*M*) to Bob. Alice and Bob share a secret key *k*, and have agreed on using a specific MAC algorithm MACfunc that takes input parameters *M* and *k*, i.e. MAC(*M*) = MACfunc(*M*, *k*). Outline the steps that Alice must follow when creating MAC(*M*), and the steps that recipient Bob must follow for verifying MAC(*M*). (4p)
18. What is the purpose of sending a message with a MAC ? (1p)
    i) Any third party can authenticate the message origin.
    ii) It provides non-repudiation of message origin.
    iii) The recipient can authenticate the message origin.
    iv) It protects the message confidentiality.

Answer

15. (0.5p for each correct, 0p for each wrong or no answer, max 2p, min 0p)

	No attack exists	Attacks exist
MD5		✓
SHA-1		✓
SHA-2	✓	
SHA-3	✓	

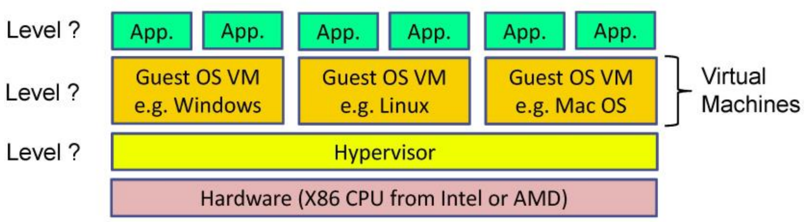
16. 1p each for any 3 of: 224, 256, 384 or 512 bits
17. 2p for: MAC generation by Alice:
    i. Alice prepares message *M*.
    ii. Alice applies the secure MAC algorithm MACfunc with input parameters *M* and *k* to produce MAC(*M*) = MACfunc(*M*,*k*).
    iii. Alice transmits message *M* and MAC(*M*) to Bob, together with her unique name and specification of the MAC algorithm she used.

    2p for: MAC validation by Bob:
    i. Bob receives message *M’* (denoted as *M’*, not *M*, because from Bob’s point of view the message origin is still uncertain), as well as MAC(*M*).
    ii. Bob applies MACfunc on *M’* to produce MAC(*M’*) = MACfunc(*M’*,*k*).
    iii. Bob checks whether MAC(*M*) =? MAC(*M’*). If TRUE, then MAC(*M*) is valid, meaning that *M’* = *M*. Bob therefore is convinced that Alice sent message *M*. If FALSE, then the signature MAC(*M*) is invalid, meaning that *M’* ≠ *M*. Bob therefore does not know who created the received message *M’*. He might then decide to reject the message, or use it knowing that its origin is uncertain.
18. 1p for: iii) The recipient can authenticate the message origin

Section 5: System Security.

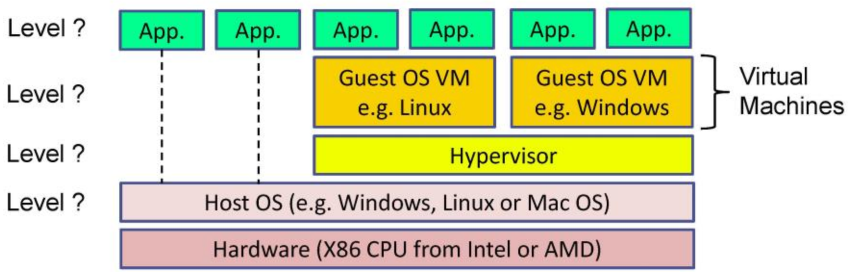
19. *“A trusted system or component is one that can break your security policy”*.
    Briefly explain the meaning of this proposition ? (2p)
20. TPM (Trusted Platform Module) is a hardware chip which supports three (3) main security services on computing platforms. List these three main TPM-supported services: (3p)
21. The X86 CPU architecture protects processes from each other based on privilege levels (protection rings). Indicate for each process type the corresponding privilege level in the Type 1 (native) virtualisation architecture. (3p)

Type 1 VM Architecture (native)



22. The X86 CPU architecture protects processes from each other based on privilege levels (protection rings). Indicate for each process type the corresponding privilege level in the Type 2 (hosted) virtualisation architecture. (2p)

Type 2 VM Architecture (hosted)



Answer

19. 2p for: If the system is trusted, then it is relied upon to enforce the security policy. So the security policy will be broken when the trusted system does not work as expected. A non-trusted system on the other hand is not relied upon to enforce the security policy, so when it breaks it does not lead to a breach of security policy.
20. 1p for: Authenticated/measured boot,
    1p for: Sealed Storage / Encryption
    1p for: Remote attestation,
21. Type 1 VM architecture (native)
    1p for: Applications, privilege level 3
    1p for: VMs, privilege level 0
    1p for: Hypervisor, privilege level -1
22. Type 2 VM architecture (hosted)
    0.5p for: Applications, privilege level 3
    0.5p for: VMs, privilege level 3
    0.5p for: Hypervisor, privilege level 3
    0.5p for: Host OS, privilege level 0

Section 6: Incident Response.

23. Specify four elements that are relevant to include in the IR (Incident Response) policy. (2p)
    i) List of potential threat agents.
    ii) Chain of escalation
    iii) Security awareness guidelines.
    iv) List of known security vulnerabilities
    v) Criteria for calling the police.
    vi) List of ranked security risks.
    vii) Who has the responsibility to make decisions.
    viii) List of systems that can be taken offline.
24. The type of IR (Incident Response) team depends on how it is manned (i.e. where its members come from). Mention the names and briefly describe the three (3) types of IR teams. (3p)
25. The activities of IR (Incident Response) can be divided into three (3) main phases. Mention the three phases, as well as one (1) specific procedure of each phase. (3p)
26. Select the relevant IDS (Intrusion Detection System) alarm for each case, or whether there is no relevance. A false positive alarm means that the IR team does not need to do anything about it. A true positive alarm means that the IR team must do something about it. (2p)

	False Positive Alarm	True Positive Alarm	Irrelevant
Detection of an attack exploiting a known vulnerability which has not been patched			
Detection of an attack exploiting a vulnerability that has been patched			
Detection of an attack exploiting an unknown vulnerability			
Detection of a new vulnerability			

Answer

23. 2p for selecting the following:
    - Chain of escalation
    - Criteria for calling the police.
    - Who has the responsibility to make decisions.
    - List of systems that can be taken offline.

    (0.5p for each correct, -0.5 for each wrong, 0p for no answer, max 2p and min 0p)
24. IR teams

    1p for: Permanent IR team, where the IR members’ principal job role is to handle security incidents

    1p for: Virtual IR team, where the IR team members have other main job roles, and are only called upon to handle security incidents whenever needed.

    1p for: Hybrid IR team, where some are permanent members, and some are virtual members.
25. IR activities:

    1p for: Detection phase, with one of: i) weed out false positive, ii) categorise event

    1p for: Respond phase, with one of: i) collect data, ii) mitigate damage, iii) isolate systems, iv) analyse and track adversary, v) report to police if necessary.

    1p for: Recovery phase, with one of: i) fix the problem, ii) improve the IR policy
    iii) disclosure.

26.(0.5p for each correct, -0.5 for each wrong, 0p for no answer, max 2p and min 0p)

	False Positive Alarm	True Positive Alarm	Irrelevant
Detection of an attack exploiting a known vulnerability which has not been patched		✓	
Detection of an attack exploiting a vulnerability that has been patched	✓		
Detection of an attack exploiting an unknown vulnerability		✓	
Detection of a new vulnerability			✓

Section 7: User Authentication.

27. Select the relevant password-protection method for implementing each requirement in the left column below for authentication to online services. (2p)

	Challenge-response	Limit attempts	Encryption	One-time passwords
Prevent guessing of passwords				
Prevent misuse of intercepted passwords				
Avoid transmission of passwords				
Prevent interception of passwords				

28. Select the relevant security method for implementing each requirement in the left column in password databases. (2p)

	Hashing	Salting	Complex password	Access control
Only authorized enties can read the password database				
Passwords are not readable in the database				
Attackers can not crack a salted and hashed password in the database				
Pre-computed hash tables can not be used to crack passwords				

29. Mention and briefly describe the two types of synchronised authentication tokens, as well as one type of authentication tokens not based on synchronisation. (3p)

30. Requirements for different AALs (Authentication Assurance Levels) are e.g. specified by the internationl standard ISO 29115 'Entity authentication assurance framework' and by the Norwegian Framework for Authentication and Non-Repudiation (Rammeverk for autentisering og uavviselighet).
How many AALs do the ISO framework and the Norwegian framework specify ? (1p)
How many authentication factors are at least required for the highest AAL ? (1p)
How many authentication factors are at least required for the lowest AAL ? (1p)

Answer

27.(0.5p for each correct, -0.5 for wrong, 0p for no answer, max 2p and min 0p)

	Challenge-response	Limit attempts	Encryption	One-time passwords
Prevent guessing of passwords		✓		
Prevent misuse of intercepted passwords				✓
Avoid transmission of passwords	✓			
Prevent interception of passwords			✓	

28.(0.5p for each correct, -0.5 for wrong, 0p for no answer, max 2p and min 0p).

	Hashing	Salting	Complex password	Access control
Only authorized entities can read the password database				✓
Passwords are not readable in the database	✓			
Attackers can not crack a salted and hashed password in the database			✓	
Pre-computed hash tables can not be used to crack passwords		✓		

29.Authentication tokens

1p for: Clock-synchronised tokens, where the token and server generate equal OTPs based on time from synchronised clocks as input, together with other data such as a secret key and user Id.

1p for: Counter-synchronised tokens, where the token and server generate equal OTPs based on counter values from synchronised counters as input, together with other data such as a secret key and user Id.

1p for: Challenge-response tokens, where the server sends a challenge (random number) to the token which returns the response computed as a function of the challenge in addition to e.g. a secret key and the user identity.

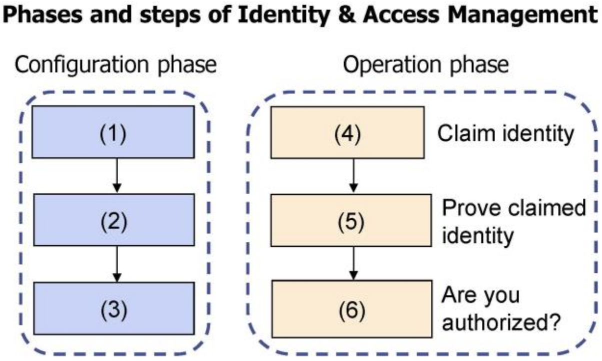
30.1p for: 4 AALs specified in the ISO framework and the Norwegian framework

1p for: The highest (AAL 4) requires at least two (2) authentication factors

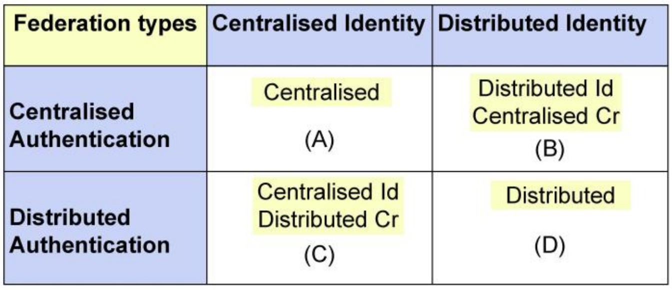
1p for: The lowest (AAL 1) requires at least one (1) authentication factor

Section 8: Identity and Access Management.

31. The diagram shows that the configuration phase and the operation phase of IAM (Identity & Access Management) consist of steps which represent specific activities. Name the steps 1-6 in the diagram: (3p)



32. Identity federation architectures can have centralized or distributed authentication, and centralized or distributed management of identities, which gives four different types. Select the correct federation type (A. B, C or D) to the specific Id federations under the table. (4p)



Federation types	Centralised Identity	Distributed Identity
Centralised Authentication	Centralised (A)	Distributed Id Centralised Cr (B)
Distributed Authentication	Centralised Id Distributed Cr (C)	Distributed (D)

33. AC (Access Control) models can have varying degrees of flexibility. Rank the AC models in the left column below according to flexibility. (3p)

	Least flexible	Intermediate	Most flexible
ABAC			
DAC			
RBAC			

Answer

31. 1.5p for: (1) Registration, (2) Provisioning, (3) Autorization
    1.5p for: (4) Identification, (5) Authentication, (6) Access control

32. 1p for: facebook B
    1p for: FEIDE D
    1p for: google+ A
    1p for: ID-porten C

33. (1p for each correct, -1p for each wrong, 0p for no answer, max 3p and min 0p)

	Least flexible	Intermediate	Most flexible
ABAC			✓
DAC	✓		
RBAC		✓	

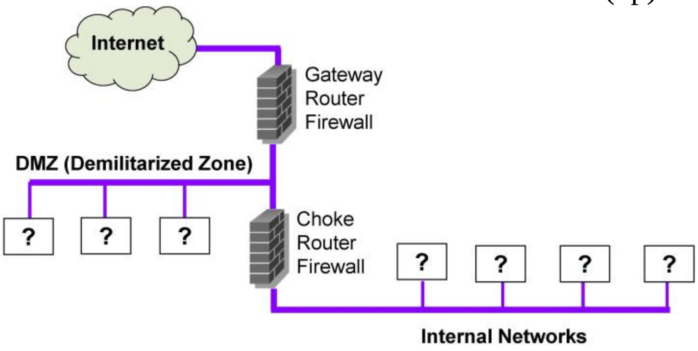
Section 9: Network Perimeter Security.

34. NGFW (Next Generation Firewalls) are advanced 3rd generation firewalls that support multiple functions. Select the functions that are typically supported by NGFWs. (2p)

- Deep packet inspection
- Email spam filtering
- Inspection of TLS/SSL encrypted traffic
- Intrusion detection and prevention
- Penetration testing
- Software fuzzing
- Vulnerability scanning
- X.509 certificate generation

35. In the case of two firewalls with a so-called DMZ (Demilitarized Zone) between them, servers/systems can be connected to either the DMZ or to internal networks. Select the typical location (DMZ or Internal Networks)) for connecting the servers/systems in the left column below. (3p)

i) Database Server
ii) DNS Server
iii) Email server
iv) Production Server
v) Web Server
vi) Workstation



36. The two main techniques used in IDS (Intrusion Detection Systems) are Signature-Based Detection and Anomaly-Based Detection respectively. Select the relevant IDS technique for each property in the left column below. (3p)

	Signature detection	Anomaly detection
Can detect unknown attacks		
Generates relatively many false intrusion alarms		
Can only detect known attacks		
Based on known attacks		
Generates relatively few false intrusion alarms		
Based on learning normal behavior		

37. Briefly explain how a user can know whether the TLS-encrypted traffic from a workstation in a company to a remote server on the Internet is being inspected in the company gateway firewall. (2p)

Answer

34. 2p for selecting

- Deep packet inspection
- Inspection of TLS/SSL encrypted traffic
- Intrusion detection and prevention
- X.509 certificate generation

(0.5p for each correct, -0.5p for wrong, 0p for unanswered, max 2p and min 0p)

35. 0.5p for each correct network location, max 3p.

i) Database Server	Internal Net
ii) DNS Server	DMZ
iii) Email server	DMZ
iv) Production Servers	Internal Net
v) Web Server	DMZ
vi) Workstations	Internal Net

36. (0.5p for each correct, -0.5 for wrong, 0p for unanswered, max 3p and min 0p)

	Signature detection	Anomaly detection
Can detect unknown attacks		✓
Generates relatively many false intrusion alarms		✓
Can only detect known attacks	✓	
Based on known attacks	✓	
Generates relatively few false intrusion alarms	✓	
Based on learning normal behavior		✓

37. 2p for: The user must view the certification path of the received server certificate, and know the difference between a Browser PKI root certificate and the internal proxy root certificate used for validation. If the certification path leads to an authentic root certificate of the Browser PKI, then there is no TLS inspection. If the certification path leads to the internal proxy root CA, then there is TLS inspection.

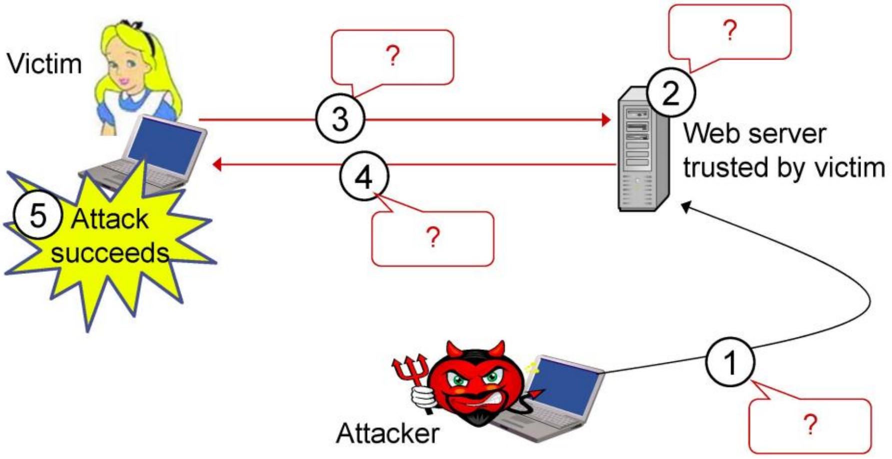
Section: Application Security.

38. Select the relevant type of malware according to each description in the left colum below (4p)

	Virux	Exploit	Worm	Trojan
Malicious software or data that exploits a software/hardware vulnerability in systems				
A self-replicating independent malicious program				
Self-replicating malicious code which is injected into other programs				
A user-installed program with hidden malicious functionality				

39. Mention the meaning of the acronym OWASP, and describe what *'OWASP Top 10'* is. (2p)

40. Stored XSS (Cross-Site Scripting) attacks can be described in terms of messages/actions between the involved entities as indicated in the diagram above. List and briefly describe the four (4) messages/actions that are shown with '?' as place-holders. (4p)



Answer

38. (1p for each correct, -1p for wrong, 0p for unanswered, max 4p and min 0p)

	Virux	Exploit	Worm	Trojan
Malicious software or data that exploits a software/hardware vulnerability in systems		✓		
A self-replicating independent malicious program			✓	
Self-replicating malicious code which is injected into other programs	✓			
A user-installed program with hidden malicious functionality				✓

39. 1p for: OWASP: Open Web Application Security Project
    1p for: The OWASP Top 10 describes the most critical and common web application security flaws currently found in online applications.
40. 1p for: 1: Input to website in the form of attack script disguised as user content
    1p for: 2: Store and display attack script on web page
    1p for: 3: Access web page
    1p for: 4: Attack script sent in web page to client