
Unit Test 1

Student ID Number

*** SOLUTIONS ***

DIRECTIONS: Please make sure that your student ID number and answers are written clearly. You have 30 minutes for this test. You are permitted to use handwritten notes during this test.

Question 1A. Place an "x" in the box next to all terms that are related to identification factors used for authentication. [5 marks]

<input checked="" type="checkbox"/>	possession
<input checked="" type="checkbox"/>	knowledge
<input type="checkbox"/>	salt
<input type="checkbox"/>	architecture
<input type="checkbox"/>	prime factor

<input checked="" type="checkbox"/>	attribute
<input type="checkbox"/>	seed value
<input checked="" type="checkbox"/>	secret
<input checked="" type="checkbox"/>	profile
<input type="checkbox"/>	hash

Question 1B. Briefly describe examples of authentication procedures using all the terms that you selected in question 1A. [5 marks]

possession, e.g. token
knowledge, e.g. password
attribute, e.g. biometric
secret, e.g. birthday
profile, e.g. engineering student

Unit Test 1

Question 2A. Place an “x” in the box next to all terms that are related to symmetric ciphers. [5 marks]

<input type="checkbox"/>	cipher block multiplexing
<input type="checkbox"/>	prime number
<input checked="" type="checkbox"/>	key exchange
<input type="checkbox"/>	one way function
<input checked="" type="checkbox"/>	padding

<input type="checkbox"/>	digital signature
<input checked="" type="checkbox"/>	cipher mode
<input checked="" type="checkbox"/>	algorithm
<input checked="" type="checkbox"/>	cipher block chaining
<input type="checkbox"/>	public key

Question 2B. Briefly describe a typical symmetric enciphering process using all the terms that you selected in question 2A. [5 marks]

- 1) Establish **key exchange** protocol and channel.
- 2) Select key size and block size.
- 3) Select a **cipher mode**, such as **cipher block chaining**.
- 4) Divide plaintext into necessary blocks of selected block size.
- 5) Apply **padding** to blocks if necessary.
- 6) Apply cipher **algorithm** to generate ciphertext.

Unit Test 2

Student ID Number

*** SOLUTIONS ***

DIRECTIONS: Please make sure that your student ID number and answers are written clearly. You have 30 minutes for this test. You are permitted to use handwritten notes during this test.

Question 1A. Place an "x" in the box next to **5 terms** that are **most directly related** to the steganographic technique of **cover generation**.

x	semagram
---	----------

	injection
--	-----------

	watermark
--	-----------

x	stego-object
---	--------------

x	message
---	---------

x	stego-key
---	-----------

	distortion
--	------------

	substitution
--	--------------

	fingerprint
--	-------------

x	cover object
---	--------------

Question 1B. Briefly describe an **example of a cover generation steganographic method or tool** using all the terms that you selected in question 1A. [5 marks]

Spam Mimic is an example where:

* **message** may be text or visual **semagram**

* **stego-key** is the spam generation algorithm

* **cover object** is spam text

* **stego-object** is the spam text generated for a particular message or semagram

Unit Test 2

Question 2A. Place an "x" in the box next to **5 terms** that are **most directly related** to a **stack overflow attack**. [5 marks]

<input type="checkbox"/>	text segment	<input checked="" type="checkbox"/>	EIP register
<input checked="" type="checkbox"/>	return address	<input checked="" type="checkbox"/>	heap segment
<input type="checkbox"/>	EXE instruction	<input type="checkbox"/>	CS register
<input checked="" type="checkbox"/>	shellcode	<input type="checkbox"/>	bss segment
<input type="checkbox"/>	ECX register	<input checked="" type="checkbox"/>	NOP instruction

Question 2B. Briefly describe **typical steps for creating a stack overflow** using all the terms that you selected in question 2A. [5 marks]

- * identify software with buffer overflow vulnerability
- * store **shellcode** in **heap segment** or environment variables
- * cause buffer overflow that overwrites **return address** on stack
- * use **NOP instructions** to improve chances of return address alignment
- * allow **EIP register** to execute instructions at the new return address

Unit Test 3

Student ID Number

*** SOLUTIONS ***

DIRECTIONS: Please make sure that your student ID number and answers are written clearly. You have 30 minutes for this test. You are permitted to use handwritten notes during this test.

Question 1A. Place an "x" in the box next to **5 terms** that are **most directly related** to the **primary components** of worm software. [5 marks]

<input type="checkbox"/>	copy files	<input checked="" type="checkbox"/>	list of infected nodes
<input checked="" type="checkbox"/>	find targets	<input type="checkbox"/>	respond to firewalls
<input type="checkbox"/>	delete files	<input checked="" type="checkbox"/>	send data to infected nodes
<input checked="" type="checkbox"/>	launch attacks	<input checked="" type="checkbox"/>	respond to commands
<input type="checkbox"/>	find bugs	<input type="checkbox"/>	send data to infected programs

Question 1B. Briefly describe a **specific sample activity for each component** of worm software using all the terms that you selected in question 1A. [5 marks]

Find targets by scanning ports.

Launch attacks by causing stack overflows.

Maintain **list of infected nodes** by using a private chat channel.

Send data to infected nodes by using email.

Respond to commands by opening a back door on the infected node.

Unit Test 3

Question 2A. Place an “x” in the box next to **5 terms** that are **most directly related** to the **commercial roles of authentication technology**. [5 marks]

<input type="checkbox"/>	formats	<input checked="" type="checkbox"/>	communications
<input type="checkbox"/>	opt-in	<input type="checkbox"/>	outsourcing
<input checked="" type="checkbox"/>	loyalty	<input type="checkbox"/>	utility patents
<input checked="" type="checkbox"/>	privileges	<input type="checkbox"/>	copyright
<input checked="" type="checkbox"/>	payments	<input checked="" type="checkbox"/>	transactions

Question 2B. Briefly describe **specific examples of commercial products or vendors and how they use authentication technology**. Use all the terms that you selected in question 2A. [5 marks]

Authentication protects **loyalty** and brand value of companies and/or products, eg RFID tags to identify authentic Viagra capsules.

Authentication is required for communities to provide **privileges** to their members, eg merchant ratings in Amazon or Ebay communities.

Authentication is required to setup electronic **payments**, eg banking account verification to setup PayPal accounts.

Authentication is required in order to protect the privacy of electronic **communications**, eg Verisign certificates to encrypt email messages.

Authentication increases trust between participants in a **transaction**, eg certificate signing to permit ActiveX components or Java applets more application access.