Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

EIGHTH SEMESTER B.TECH DEGREE EXAMINATION, MAY 2019

Course Code: CS472

Course Name: PRINCIPLES OF INFORMATION SECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks. Marks

1		What is brute force attack?	(4)
2		Discuss different types of attacks that can occur in an organization.	(4)
3		Describe discretionary policies for Biba model.	(4)
4		What is phishing? Give an example.	(4)
5		Differentiate between polymorphic and metamorphic worm.	(4)
6		How do you reduce the impact of XSS vulnerabilities?	(4)
7		Describe frame spoofing with a neat diagram.	(4)
8		Describe the security enhancements present in UMTS.	(4)
9		What is SOAP binding? Explain with the help of a HTTP message.	(4)
10		List the security threats in RFID based identification and tracking systems.	(4)

PART B

Answer any two full questions, each carries 9 marks.

11	a)	What is role based access control. Illustrate with suitable example the concept of role inheritance.	(4)
	b)	Differentiate between Discretionary and Role based access control.	(2)
	c)	Briefly discuss Mandatory access control implemented in a typical secure operating system.	(3)
12	a)	Demonstrate Chinese wall security model with neat diagram.	(5)
	b)	Classify each of the following as a violation of confidentiality, integrity, availability or some combination thereof. Also justify your answer. i. John copies Mary's homework. ii. Paul crashes Linda's system iii. Carol changes the amount of Angelo's check from 100 to 1000 iv. Gina forges Roger's signature on a deed.	(4)

13	a)	Interpret about the star property in Bell -LaPadula model.	(4)
	b)	Write Windows access control algorithm.	(5)

PART C

Answer any two full questions, each carries 9 marks.

14	a)	How Buffer OverFlow (BOF) vulnerability makes software insecure. Explain different ways in which BOF exploitations occur.	(5)
	b)	Explain XSS vulnerabilities.	(4)
15	a)	Describe Kermack-McKendrick Model of worm propagation.	(5)
	b)	Explain any two categories of topological worms.	(4)
16	a)	Explain how can you detect and prevent SQL Injection vulnerabilities.	(5)
	b)	Name any worm that exploited buffer overflow vulnerability. Explain its characteristics.	(4)

PART D

Answer any two full questions, each carries 12 marks.

17	a)	Explain link level security provided by Bluetooth.	(6)
	b)	Describe entity authentication and key agreement in GSM Networks.	(6)
18	a)	How security is implemented in online credit card payment systems?	(8)
	b)	What are the main concerns involved in online credit card payment systems?	(4)
19	a)	Explain MAC generation and encryption in CCMP.	(6)
	b)	Explain any two technologies for web services.	(6)

****

Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

EIGHTH SEMESTER B.TECH DEGREE EXAMINATION(S), OCTOBER 2019

Course Code: CS472

Course Name: PRINCIPLES OF INFORMATION SECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks. Marks

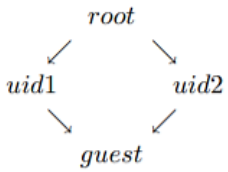
1		Explain the need of information security.	(4)
2		Distinguish between vulnerability and threat. Give example.	(4)
3		Explain Clark-Wilson Model with a neat diagram.	(4)
4		Illustrate SQL injection with an example.	(4)
5		Briefly explain the life cycle of a computer virus.	(4)
6		Explain XSS or Cross Site Scripting.	(4)
7		What is a poll control frame? How does an attacker exploit a poll control frame?	(4)
8		List out any 4 lacunae/pitfalls in GSM Security. Give a brief explanation.	(4)
9		Discuss the strength and weakness of Secure Electronic Transactions.	(4)
10		Explain the entities involved in a web service.	(4)

PART B

Answer any two full questions, each carries 9 marks.

11	a)	Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file alicerc, and Bob and Cyndy can read it. Cyndy can read and write the file bobrc, which Bob owns, but Alice can only read it.Only Cyndy can read and write the file cyndyrc, which she owns. Assume that the owner of each of these files can execute it. Create the corresponding access control matrix.	(6)
	b)	What is a CIA Triad? Explain.	(3)
12	a)	State the *-property for the Chinese Wall model	(4)
	b)	Explain Biba Model.	(5)
13	a)	Differentiate between Discretionary and Mandatory Access Control	(4)
	b)	You are given a security policy stating that a subject has access to an object if and only if the security level of the subject dominates the security level of the	(5)

object. What is the effect of using the following lattice with this policy?



PART C

Answer any two full questions, each carries 9 marks.

14 a) How does buffer overflow vulnerability occur? How does a canary variable detect buffer overflow attack? (5)

b) What is software vulnerability? What are the common types of software flaws that lead to vulnerability? (4)

15 a) Explain various Internet propagation models for worms. (6)

b) Explain about code red worms. (3)

16 a) What are topological worms? Explain any 2 Topological worms. (5)

b) Differentiate between stored and reflected XSS. (4)

PART D

Answer any two full questions, each carries 12 marks.

17 a) How is security enhanced in UMTS when compared to GSM? (8)

b) How is encryption of messages between cell phone and base station achieved in GSM? (4)

18 a) Explain various security threats associated with RFID systems. (6)

b) What are the various elements in XML Encryption? Explain. (6)

19 a) How is data protection achieved in WEP? What are its drawbacks. (6)

b) Explain dual signature with respect to SET. (3)

c) With an example, explain SAML assertion. (3)

****

Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Eighth semester B.Tech degree examinations, September 2020

Course Code: CS472

Course Name: PRINCIPLES OF INFORMATION SECURITY

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks. Marks

1		What access control mechanism provides enhanced security in SELinux? How is the security provided?	(4)
2		Illustrate with an example how access is granted by an access control matrix.	(4)
3		Describe Biba integrity model.	(4)
4		How can buffer overflow vulnerability be prevented?	(4)
5		What is timing attack?	(4)
6		How did Code Red propagate?	(4)
7		With the help of a diagram explain the key hierarchy in 802.11i.	(4)
8		What is the need for Link Level Authentication in Bluetooth?	(4)
9		Describe the strength and weakness of secure electronic transaction	(4)
10		Describe SAML assertion with an example.	(4)

PART B

Answer any two full questions, each carries 9 marks.

11	a)		Distinguish between discretionary and mandatory access control	(3)
	b)		Let L and C be the set of sensitivity/clearance levels and set of categories respectively. L= {UNCLASSIFIED, CONFIDENTIAL,TOP SECRET} and C={Sales, NewProducts, BusinessPartners}. Here TOP SECRET is at the highest clearance level and UNCLASSIFIED the lowest.	
		(i)	How can two documents with security labels <TOP SECRET,{Sales}> and <UNCLASSIFIED,{Sales,NewProducts}> be compared?	(3)
		(ii)	What is the minimum clearance that a subject should have to access the two documents?	(3)
12	a)		Explain waterfall model for providing security.	(5)
	b)		Explain Star property of Bell- LaPadula Model.	(4)

13	a)	Rima, shankar and david are three users of a computer system. They own the files A, B and C respectively Rima is able to write the files B and C shankar can read and write files A & C David can read file A and write file B. The owner of each of these files can execute it. Create the corresponding access control matrix	(4)
	b)	Demonstrate Chinese wall Security model with a neat diagram.	(5)

PART C

Answer any two full questions, each carries 9 marks.

14	a)	What are topological worms? Illustarte email and P2P worms.	(5)
	b)	Explain Kermack-McKendrick Model of worm propagation.	(4)
15	a)	Describe SQL injection vulnerability.	(5)
	b)	How can a shell code be used for exploiting stack overflow?	(4)
16	a)	Discuss cross site scripting vulnerabilities.	(4)
	b)	Explain different worm characteristics.	(5)

PART D

Answer any two full questions, each carries 12 marks.

17	a)	Explain Integrity protection and encryption in UMTS.	(6)
	b)	Illustrate the need for frame spoofing.	(6)
18	a)	What are the various elements in XML signatures?	(6)
	b)	Describe Secure Electronic Transaction.	(6)
19	a)	Explain Authentication and Key Agreement in 802.11i.	(6)
	b)	Explain any one mechanism used in RFID for ensuring the security. Mention any one attack that can occur in RFID system.	(6)

****