Net ID:

Information Assurance: Final Exam - Key

Multiple Choice – 3 points each

1. The SYN Flood attack targets which security element?
   A) Confidentiality
   B) Integrity
   C) Availability
   D) All of the above

2. Which of the following is a technique that makes information more readily available via emanations analysis, but is not obvious to someone looking at the computer?
   A) Manipulating the screen to generate an AM radio signal
   B) Using dither when creating the screen display
   C) Using stegonoraphic techniques when creating the display image
   D) Using storage covert channels

3. When performing a stack smashing attack, what is the key piece of information that must be overwritten to enable the redirection of execution to the attack code?
   A) The function's return address
   B) The function's frame pointer
   C) The stack pointer
   D) The calling function's arguments

4. Which of the following directly contributes to assurance during the development or implementation phase of a product's life cycle?
   A) Implementation of a mandatory access control model like Bell-LaPadula
   B) Trusted distribution chain
   C) Addition of multi-factor authentication in the product
   D) Use of a source control or configuration management system

5. Assuming that passwords are selected with uniform probability over an alphabet of 100 characters, how long should the passwords be to ensure that they have at most a 10% probability of being cracked over a month (30 days) by an attacker capable of 1,000 password guesses a second.
   A) 11
   B) 3
   C) 6
   D) 8

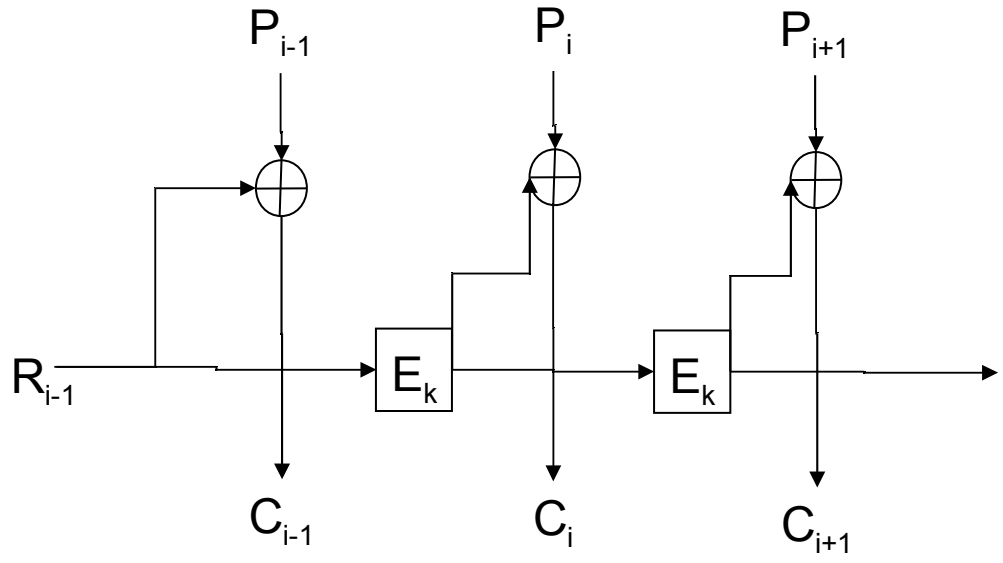
6. You are shopping for a network security appliance for use in a high assurance environment. Based on the following evaluation information, which product would be the best for your situation?
   A) Product A evaluated under the Common Criteria in Canada with a security target based on the Labeled Security Protection Profile at EAL 3
   B) Product B evaluated under the Common Criteria under a security target not based on a protection profile at EAL 2 in the United States.
   C) Product C evaluated under TCSEC at C2 in the United States
   D) Product D evaluated under the Common Critera with a security target based on the "Network Intrusion Prevention System Protection Profile" at EAL5 in Germany.

7. Which of the following laws affects network and telephone service providers? It states that such service providers must have networks that enable them to comply with legal wiretap requests.
   A) Electronic Communication Privacy Act (ECPA)
   B) Foreign Intelligence Surveillance Act (FISA)
   C) USA PATRIOT Act
   D) Communications Assurance For Law Enforcement Act (CALEA)

8. Which of the following statements is **not** true about partial and total orderings?
   A) The "is less than or equal to" relation on the set of integer values form a total order.
   B) The "is subset of" relation on the set of subsets of {1,2,3} form a total order.
   C) A total order has the anti-symmetry property.
   D) In the Bell-LaPadula model, the security levels plus the "dominates" relation form a partial order.

9. What does the two-phase commit in databases protect?
   A) Confidentiality
   B) Integrity
   C) Availability
   D) All the above

10. Identify the common mode that can be used with block encryption algorithms such as AES and DES that is illustrated in the diagram below. P_i is a unit of plaintext. C_i is a unit of cipher text. E_k is the block encryption algorithm operating with key k. R_i is a register value.



A) Output Feedback mode (OFB)
B) Cipher Block Chain mode (CBC)
C) Counter mode
D) Electronic Codebook mode (ECB)

11. Which of the following is an amplification attack?
A) Smurf attack
B) SYN flood attack
C) Chop chop attack
D) Teardrop attack

12. How would an investigator use slack space?
A) Use an electron microscope to detect the magnetic remnance from past writes.
B) Look for data remaining from previous times the operating system allocated the block to a file.
C) Look for alternate data encodings.
D) Search for unusual filename suffixes

Net ID:

Short answer

13. The following questions work with the rail cipher (6 points)
    A) Decrypt the following message that was encrypted with the rail cipher.

TEUETRECISNIHUYNSRAEOFIHEHA
HQENUNDRMOWTFRADCEMDFWTHRED

THE QUEEN TURNED CRIMSON WITH FURY AND SCREAMED OFF WITH HER HEAD

B) For sufficiently long English messages, how should the character frequency of the message be related to the average character frequency of English text?

The character frequency should be very close the the character frequency of average English text.

14. Bob is buying a new cell phone. Use quantitative risk analysis to determine whether he should buy the loss protection plan. (12 points)
    A) The replacement cost for the phone is $200. Bob is absent-minded. He expects that he has a 30% probability of losing the phone in the course of a year. What is the annual loss expectancy for the phone?

*.30 * 200 = $60*

    B) The mobile phone company offers loss insurance at the cost of $5 per month. If he loses the phone, the phone company will give him a new phone at no additional cost. What is the risk leverage calculation for this control?

New ALE is $0
*Cost of control for a year is $5*12 = $60*
Risk leverage is (60 – 0)/60 = 1

    C) In Extreme Geek, Bob found a two piece electronic gadget. You stick one half on the phone and keep the other half on yourself. When looking for your phone, you press a button on one half, and the half on the phone beeps. The gadget costs $15, and Bob figures this will reduce his probability of loss by one half to 15% probability of loss per year. What is the risk leverage calculation for this control?

*New ALE is .15*200 = $30*
Cost of control for a year is $15
Risk leverage is (60 – 30)/15 = 2

    D) Based on these calculations, how would you advise Bob? Should he pay for the loss insurance? The Extreme Geek gadget? Or nothing? Why?

You could argue for each of the options. Based on the risk leverage, the electronic gadget is probably the best bet. It is also a single fixed cost. You don't have to pay for the gadget again next year.

You might argue that the cost of replacing a phone is not worth the cost of either control. The phone package probably gives you the option to cheaply upgrade every year or two in any case.

As long as the argument is well supported, give credit.

15. Identify the following statements as policy or mechanism. If you identify the statement as policy, list a possible enforcing mechanism, or if you identify the statement as mechanism, list a policy that the mechanism might be enforcing. (12 points)
    A) All customers must show photo ID when purchasing alcohol if they appear 40 or younger.

Mechanism. Could be enforcing the policy that the store will not sell alcohol to minors even if they look older. Could be enforcing the policy of flattering older customers by making them feel younger by asking for ID.

    B) Patient information may only be accessed by the attending physician and nurse.

Policy. Could be enforced by authentication and access controls over electronic media.

    C) Clients must select a password with at least 10 characters with at least one lower case, one upper case, one numeric, and one special character.

Mechanism. Could be implementing policy that entities may only access the system via strong authentication.

    D) Only city residents may enroll their children in Urbana schools.

Policy. Could be implemented by showing proof of residency when enrolling children in the school.

16. A certificate C is signed by the certificate authority (CA) with its RSA key. The CA RSA key is, e_{CA}, d_{CA}, N_{CA} (12 points)
    A) What are the public portions of the CA's key?

e_{CA} and N_{CA} are the public key components.

    B) What is the equation for computing the signature of CA's signature over the hash of the certificate, h(C)?

$h(C)^{dCA}$ mod N_{CA} = signature

    C) When someone receives the certificate C, how should they verify the signature?

They should compute the hash over the contents of the certificate, h(C).

Then they should undo the signature as X = $signature^{eCA}$ mod $N_{CA.}$

X and h(C) should be equal.

    D) On what hard problem is the security of the RSA algorithm based? Assuming this problem was solved, how would you break the RSA key pair?

Factoring composites of large primes.

If we could do this, we could compute the primes p and q that make up N_{CA}

Knowing that we could compute d from e

*e*d mod totient(N) = 1*
*e*d mod (p-1)*(q-1) = 1*

There are a number of algorithms that can solve for d efficiently. This is how the key pair is originally computed.

17. The following questions address mandatory access control under the Bell-LaPadula model. (9 points total)
    A) Define the dominates operator between SL1=(L1, C1) and SL2 = (L2, C2) where the sensitivity labels are defined as pairs of levels and category or compartment sets. (3 points)

SL1 dominates SL2 if L1 >= L2 and C1 is a superset or equal to C2.

    B) Consider the following access control matrix. You have a set of levels: low < medium < high, and a set of categories c1, c2, ... cn. Define and assign a set of sensitivity labels to the subjects and objects in the access control matrix that would match the protection state defined by the access control matrix. (6 points)

	X	**Y**	**Z**
Alice	Append	Append	Append
Bob	Read	Read	Read
Carol			Append,Read

There are a number of options here too. One that works is:

B = low:{c1}

A = high:{c1,c2}

Z = C = medium:{c1,c2}

X = Y = medium:{c1}

18. A worm uses a simple random selection to find addresses of systems to test for the presence of vulnerable services. There are approximately 2^30 infected systems across the Internet. (7 points)
    A) In IPv4, what is the probability of selecting an address of a vulnerable machine? (2 points)

2^30/2^32 = 1/4

    B) In IPv6, what is the probability of selecting an address of a vulnerable machine? (2 points)

2^30/2^128 = 1/2^98

    C) What is one technique the worm writer can use to improve his odds of finding a vulnerable machine? (3 points)

The worm writer can look for active machine addresses in logs, or by sniffing traffic.
The worm writer can look for addresses registered in DNS.

19. A client machine communicates with a server machine. (9 points)
    A) What technique could an attacker use to place himself in the middle to attack the confidentiality or integrity of the conversation?

The attacker could use ARP cache poisoning. He could implement a rouge DHCP server to insert his machine as a default gateway router. He could poison the DNS cache to insert himself between the client and the real domain named server.

    B) The client and server tunnel their conversation through SSL. How does the SSL handshake protocol enable the client to detect that an third party is trying to insert itself into the conversation?

In the certificate authentication, the attacker could give his certificate to the client. However, the attacker should not get a legitimate CA to sign a certificate that is associated with someone else's domain name.

    C) Provide one technique that you as an attacker could use to subvert the SSL handshake detection you described in part B.

Attacker could cause another CA root to be installed in the client's browser. Then the attacker could create a duplicate certificate and get it signed by a bogus "root" server.

The attacker to "crack" the crypto hash and create a bogus certificate that has the same hash value as a legitimately signed certificate. This has been done, but not with currently approved crypto hash protocols.

The attacker could try to use javascript or other techniques to change the client's browser.

20. Consider the Wired Equivalence Protocol (WEP). (9 points)

A) Why is it never a good idea to reuse a key stream in stream cipher?

If you know that two cipher text streams are encrypted with the same key stream, you can xor the cipher text streams. The result is the xor of two plaintext streams. This has more pattern than the original cipher text streams. And is more vulnerable to analysis.

B) Why is RC4 insecure when used in WEP but secure when used in SSL?

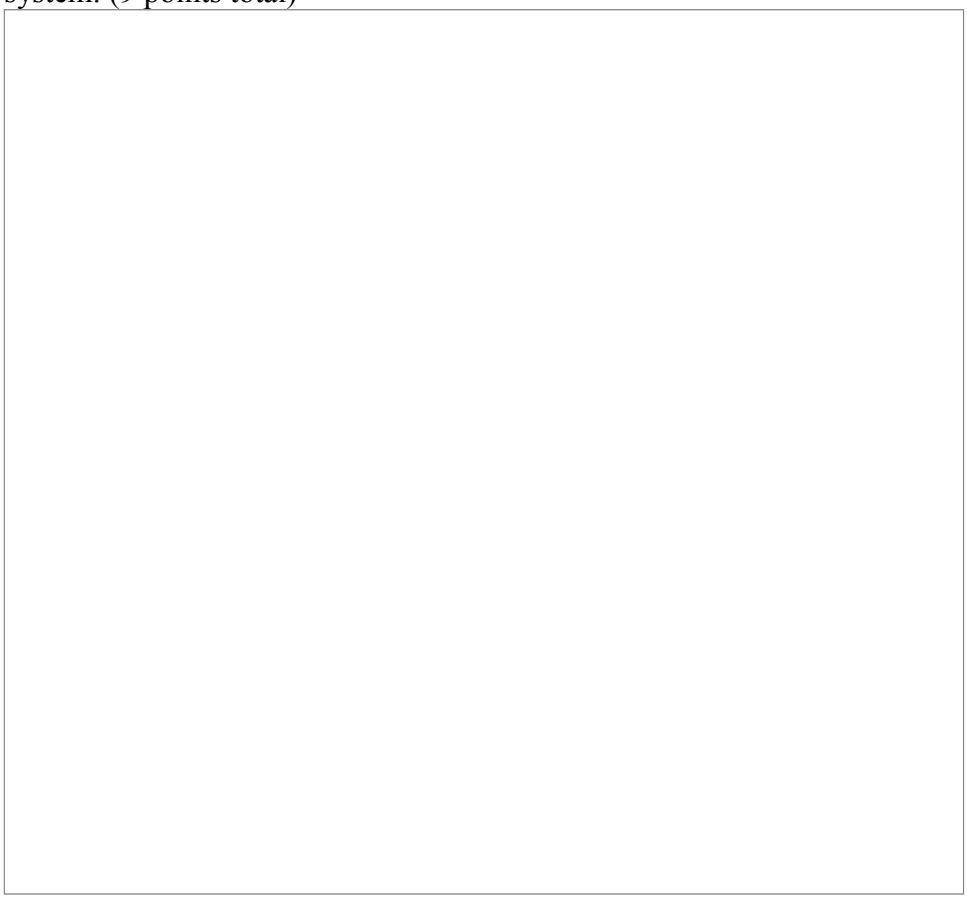
SSL is built over TCP, which is a reliable transport. Therefore, the RC4 key stream does not need to be restarted on pack packet. Rather it only needs to be restarted on each connection.

C) Why is AES in counter mode, used in WPA2, a superior choice for encrypting wireless packets?

AES in counter mode generates a key stream too. But the key stream is generated by successive AES encryptions over a running counter. The AES key is unchanged between packets. And the AES key is not passed with the packet.

In WEP, the "name" of the keystream is passed with the packet.

21. The following Data Flow Diagram provides a high level view of the Fabrikam Phone 1.0 system. (9 points total)



A) What is an entry point into the system? (2 points)

The user entering the system via the Public Switched Telephone Network.

(more parts next page)

B) Consider the following threat. "An adversary gains access to the remote administration interface, resulting in access to the phone configuration." Sketch an attack tree that specifies some possible details of attacks that result from this threat. (4 points)

See comments on exam 2.

C) Identify one threat path in your attack tree, and specify one control that would mitigate that path. (3 points)

See comments on exam 2.

22. (3 pts) Use the key "snow" to decrypt the following message encrypted using Vigenere's algorithm.

ZNDLQUCHAQOUK
SNOWSNOWSNOWS
HAPPYHOLIDAYS

Net ID:

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y