Net ID:

University of Illinois at Urbana-Champaign
Department of Computer Science

Midterm 1
CS461/ECE422 – Computer Security I
Fall 2008
Wednesday, October 8, 2008
Time Limit: 50 minutes

Instructions for the Student

Print your name and NetID in the space provided below**; print your NetID in the upper right hand corner of every page.**

Name: _____

NetID: _____

1. A single page of supplementary notes is allowed
2. Closed book
3. A calculator is allowed.
4. Students should show work on the exam. They can use supplementary sheets of paper if they run out of room.
5. Students can use scratch paper if desired.

Number of pages of the exam: 8

Number of questions on the exam: 12

Maximum grade on this exam is: 74 pts

Problem	Points	Score	Grader
1	2		
2	2		
3	2		
4	2		
5	2		
6	2		
7	12		
8	14		
9	6		
10	10		
11	8		
12	12		

Net ID:

Information Assurance: Midterm 1

Multiple Choice – 2 points each

1. The key generation technique used by Schneier's Solitaire encryption scheme that we studied in class is an example of what style of key generation.
    a. Electronic Codebook (ECB) mode
    b. Cipher Feedback (CFB) mode
    c. Book cipher
    d. Output Feedback (OFB) mode

2. Which asymmetric key algorithm is used for securely generating common secrets in commonly used network security protocols?
    a. RSA
    b. AES
    c. Bin packing
    d. Diffie-Hellman

3. What style of risk analysis uses exact values for probabilities of a risk and values of assets?
    a. Qualitative risk analysis
    b. Coordinated risk analysis
    c. Quantitative risk analysis
    d. Cooperative risk analysis

4. Which algorithm would be most appropriate for storing a message integrity code or message authentication code with a network packet?
    a. CRC
    b. SHA-256
    c. MD5
    d. HMAC-SHA1

5. Which of the following measures can aid in discovering the period of a Vigenere's cipher?
    a. Index of coincidence
    b. Avalanche effect
    c. Birthday paradox
    d. Totient function

6. What technique is effective in deterring an online (type 2) password attack?
    a. Adding salt to the complementation information.
    b. Backoff or increasing delay between failed password attempts
    c. Eliminating access to the L function.
    d. Adding a trusted path.

Short answer

7. (12 pts) Below is a list of policies and mechanisms.
    a. Mark each element as a policy or a mechanism.
    b. Create pairs of policies and the mechanism that could implement that policy. There are an odd number of items in the list, so there will be one spare.

Index	Type	Matching Pol or Mech Index	Value
1			The company login page must store unique images for each customer and present that image upon login.
2			Only members of the executive council (and their direct representatives) should have access to sensitive business plans.
3			At registration, all parents must show a deed or bill showing their name and current address.
4			When purchasing a book online, the customer must provide their residential zip code.
5			All network communication to and from the critical access servers must be encrypted using at least AES 256 encryption.
6			Access to any educational computing resources must be authenticated by a University netid and a bluestem password.
7			Online and mail order vendors are responsible for collecting the sales taxes levied by the locality of the purchaser.
8			Only University of Illinois students may use the student computing labs.
9			All communication on the network must include message authentication codes constructed from HMAC-SHA.
10			All customers must be able to distinguish the company's true login web page from similar pages not hosted by the company.
11			Only residents of Urbana may enroll their children in Unit 116 schools.

8. (14 pts) You have received a X.509 certificate C2<<Bob>> (Bob's certificate signed by C2). Your certificate authority is C1. The certificate infrastructure uses RSA keying information.
    a. What certificate should you already have to protect yourself against a man-in-the-middle attack?

    b. What certificate do you need to fetch to verify the certificate you just received?

    c. What do you need to verify? What information will you use to complete this verification?

    d. Show the equations you would use the verify one certificate.

    e. If you (or your system) do not perform this verification, what attack are you opening yourself to?

9. (6 pts) Use the text from question 10 and the Vigenere's tableau at the end of the exam (if needed) to decipher the following phrase using the book cipher technique.

    BLRBH YPLPY HLVVD

10. (10 pts) The standard Unix access control encoding of permissions in the user/group/other triplet approximates the expressibility of the full access control list model.
    a. Give an example of a scenario that could be expressed in a full access control list that cannot be expressed by the Unix user/group/other model.

    b. Show the protection state of your example from part a in an access control matrix.

11. (8 pts) You have discovered an efficient algorithm to factor large numbers. How does this affect the effectiveness of RSA? Given Bob's public key **(e,n)**, private key **d**, and an encrypted message **{m}(e,n)** from Alice to Bob, show specific equations to illustrate how your algorithm could be used to discover **m**.

12. (12 pts) Your boss wants you to compute how long a password would need to be to ensure that an adversary capable of testing 18,000 passwords per second will only have a 40% probability of breaking any randomly selected password in 9 months.
    a. Over the basic latin alphabet (a-z).

    b. Over the set of phonemes (440 phonemes). Each phoneme is represented by approximately 3 characters.

    c. Which alphabet would you suggest using for randomly generated passwords and why?

    d. How accurately do you feel that your computations model how quickly a real attacker will take to break passwords? Why is this a good model? Or what are the weaknesses?

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