CS 161 Computer Security
Fall 2005 Joseph/Tygar/Vazirani/Wagner Final

PRINT your name: ______________________________, ______________________________
(last) (first)

SIGN your name: ____

PRINT your Unix account name: __________________________

PRINT your TA's name: __________________________

You may consult any books, notes, or other paper-based inanimate objects available to you. Calculators and computers are not permitted. Please write your answers in the spaces provided in the test; in particular, we will not grade anything on the back of an exam page unless we are clearly told on the front of the page to look there.

Please be concise.

You have 3 hours. There are 10 questions, of varying credit (100 points total), not necessarily in order of difficulty. The questions are of varying difficulty, so avoid spending too long on any one question.

Do not turn this page until your proctor tells you to do so.

Problem 1	
Problem 2	
Problem 3	
Problem 4	
Problem 5	
Problem 6	

Problem 7	
Problem 8	
Problem 9	
Problem 10	
Total	

Problem 1. [Defaults] (9 points)

Short answer: At most one sentence of explanation.

(a) Which is generally safer (from a security point of view), a firewall with a "default deny" policy or a firewall with a "default allow" policy? Why?

(b) Many spam filters can be configured to use either a whitelist or a blacklist. Name one advantage of using a whitelist (instead of a blacklist) for your spam filter.

(c) Name one disadvantage of using a whitelist (compared to a blacklist) for your spam filter.

Problem 2. [Authentication] (8 points)

Describe two fundamentally different conceptual approaches that can be used for user authentication. Be concise: One sentence should suffice.

Scheme #1:

Scheme #2:

Problem 3. [Intrusion Response] (6 points)

The software company Snoracle (slogan: "Unwakeable") is selling a new defense against DDoS attacks. Their software looks at the source IP address on all incoming packets, and if it finds any IP address that accounts for more than 1% of traffic over the last hour, it installs an entry in the router that blocks all packets from that address for the next 24 hours. Their marketing folks are claiming that this will stop all DDoS attacks cold in the water. Is this a good solution to the problem? Give one reason why or why not.

Problem 4. [Hardware Support for Dual-Mode Operation] (6 points)

Early Intel processors (e.g., the 8086) did not provide hardware support for dual-mode operation (i.e., support for a separate user mode and kernel mode). As a result, most of the systems implemented on these processors did not support multi-user operation. List and explain one potential problem associated with supporting multi-user operation without hardware support for dual-mode operation. Be concise: one or two sentences should suffice.

Problem 5. [Shamir Secret Sharing] (10 points)

In this question, you have a chance to explain your understanding of the Shamir Secret Sharing system. Let s be a secret that is supposed to be shared. Let p be a large prime, let n be the number of share holders, and let q be a quorum of share holders (i.e., a threshold so that it will take at least q shares to recover the secret s). Assume that $1 < q < n < p$.

(a) Explain how Shamir creates a function $f(x)$ such that: $f(0) = s \pmod{p}$; and $f(1) \bmod p$ equals the first share; and $f(2) \bmod p$ equals the second share; etc. Be explicit.

(b) Explain briefly (maximum of 50 words!) why one can recover s when one has values of $f(x) \bmod p$ for at least q distinct values of x (where $0 < x < p$).

Problem 6. [Key Distribution with Mutual Authentication] (10 points)

Here is a version of an authentication protocol discussed in class. In this protocol Alice and Bob wish to authenticate. There is a trusted authority T which generates a fresh random session key K and distributes it to Alice and Bob. Alice has a symmetric key K_A that is shared with T. Bob shares symmetric key K_B with T.

In the notation below $x \to y : m$ means that x sends message m to y. $\{m\}_k$ means that message m is encrypted with symmetric key k. Messages in quotes are literals that are transmitted. For example, the first line means Alice sends the trusted authority T a message saying "I want to authenticate with Bob" and that message is encrypted with key K_A.

$$
\begin{aligned}
\text{Alice} \to \text{T}: &\quad \{\text{“I want to authenticate with Bob”}\}_{K_A} \\
\text{T} \to \text{Alice}: &\quad \{\text{“Use session key”}, K, \text{“and send Bob this message”}, \\
&\quad\quad \{\text{“This is Alice using session key”}, K\}_{K_B}\}_{K_A} \\
\text{Alice} \to \text{Bob}: &\quad \{\text{“This is Alice using session key”}, K\}_{K_B}
\end{aligned}
$$

Alice and Bob now share key K and can use K to secure all future messages between them.

(a) This authentication and key-exchange protocol is subject to a replay attack. Explain how the replay attack would work.

(b) Assume Alice, Bob, and T have synchronized clocks. Show how to modify the messages of the above protocol to defend against replay attacks. The only changes to the protocol permitted are to add additional values to the three messages in the protocol (but you may not delete any values or otherwise change the structure of the message flow). Make the minimum number of changes to the protocol necessary for security, and be precise about exactly where your new added values will go.

Problem 7. [Gesundheit] (12 points)

Kachoo!, Inc. has just released a new web service that allows people to sign their web pages. The service does this by appending, hidden inside a special HTML tag at the bottom of an otherwise normal web page, the author's name, the date, and a signature (which contains the author's name and date signed by the author's RSA private key). The web page itself is unencrypted, but the signature can be validated by downloading `http://www.kachoo.com/pubkeys.html` (which contains a list of all registered Kachoo! users and each user's public key) to retrieve the author's public key.

Explain why this gives a completely false sense of security, by outlining two different ways that you could make it appear that Linus Torvalds has posted a web page saying "Open source is for losers; I've decided to go work for SCO". The definition of "different" is that each attack has a unique fix. For each of the attacks you list, give a countermeasure that the author/viewer could take to protect themselves against that attack.

Attack #1:

Countermeasure #1:

Attack #2:

Countermeasure #2:

Problem 8. [One is the Loneliest Number] (10 points)

In this class, we have seen several different mechanisms for isolating untrusted programs, including virtual memory, system call interposition, and virtual machines.

(a) Name one threat that system call interposition protects against but virtual memory does not.

(b) The military runs a multi-user computer that all government employees can log into; programs that require access to top-secret data are run inside a virtual machine. Richard Stallman is given an account on this computer so that he can install emacs. Colonel Greene runs a copy of Stallman's emacs program inside a virtual machine and uses it to edit the top-secret list of UFOs stored in Area 51's warehouses. (Only Greene has an account on the guest OS running inside the virtual machine.) If Richard Stallman were malicious, could he arrange to learn the contents of this list? If yes, explain how; if no, say why not.

Problem 9. [And if you believe that, ...] (11 points)

Consider the zero-knowledge protocol presented in lecture that gives a proof of knowledge of a square root x of y mod N, where $N = PQ$ is the product of two large primes:

1. The prover sends random $s = r^2 \bmod N$.
2. The verifier sends either challenge I) $s \bmod N$ or II) $sy \bmod N$.
3. The prover answers the challenge with either I) $r \bmod N$ or II) $rx \bmod N$.

(a) Suppose that the verifier is later talking to Christina and wishes to convince her that the prover really does know a square root of y mod N. So he sends Christina the transcript of his conversation with the prover. Should Christina be convinced? Why or why not?

(b) Suppose that the verifier cannot directly communicate with the prover in the above protocol, but instead all the messages between the prover and verifier are relayed through Danielle. Assume that the prover and the verifier sign every message they send, and they know each other's public key. Should the verifier be convinced at the end of the protocol that the prover knows a square root of y mod N? Justify your answer.

(c) Under the same assumptions as part (b), should Danielle be convinced at the end of the protocol that the prover knows a square root of y mod N? Justify your answer.

Problem 10. [True/False, and Why?] (18 points)

Answer each question true or false, and then say why in at most one sentence. *Don't forget to provide a one-sentence justification for each part!*

(a) True or False: "Security through obscurity" refers to the practice of obscuring a user's password when the user types it in, so that no one else can see it on the screen.

Justification:

(b) True or False: Let E_k be a secure block cipher. Then the following encryption scheme is secure against chosen-plaintext attack: to send a message m, the sender picks a random r and sends the two strings r and $E_k(r) \oplus m$.

Justification:

(c) True or False: Suppose I generate a RSA public and private key pair, and I publish the public key. Then that's all I need to be able to send you a securely encrypted email.

Justification:

(d) True or False: If Jimmy Neutron tomorrow discovers an efficient algorithm for computing the greatest common divisor of two extremely large numbers, this will make it possible to break RSA.

Justification:

(e) True or False: Consider data that is stored over time in a mandatory access control based system. The contents of files containing highly classified ("top secret") information are necessarily more trustworthy than material stored in files marked unclassified.

Justification:

(f) True or False: Access control matrices can represent anything that is represented by access control lists.

Justification:

Survey. **[Tear off this page!]**

When you finish the exam, we'd appreciate if you would tear off this page, fill out the survey, and return it to us, so that we can learn how to improve the class the next time it is offered. This survey is anonymous and purely optional. Whether you fill it out or not, it will not affect your grade in any way. Please do not write your name on this page.

Finish your exam before filling out the survey—we don't want you to be short on time. You can fill this page out after you turn in your final exam, and there is no time limit.

Don't write the answer to any exam questions on either side of this page.

- What did you think of the projects?

- What did you think of the homework?

- What did you think of the textbooks?

- What topics did you find useful in the class?

- What topics do you wish were covered?

- What suggestions do you have for future years?

Do not write on this side of the page.