CS 161 Computer Security
Fall 2006 Joseph/Tygar
Midterm 1

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

SIGN your name: _____

PRINT your Unix account name: _____

PRINT your TA's name: _____

READ ALL INSTRUCTIONS CAREFULLY.

You are allowed to bring one 8.5"×11" page of handwritten notes with you, but no books, printouts, or other study aids. Calculators, computers, and other electronic devices are not permitted. Please turn off cell phones and music players and keep them off your desk, and remove headphones.

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 explain all work, but be concise.

If you think there is an error or a significant ambiguity in the exam, please bring it to the attention of the exam proctor.

You have 80 minutes. There are 4 questions, of varying credit (100 points total). 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	
Total	

Problem 1. [Definitions] (16 points)

Please give a *short* (one sentence) definition for each of the following terms. (2 points apiece)

(a) (Cryptanalysis) Brute-force attack

(b) (Cryptanalysis) Known-plaintext attack

(c) (Cryptanalysis) Chosen-plaintext attack

(d) (Access control) Authorization

(e) (Access control) Authentication

(f) (Message protocols) Nonce

(g) (Firewalls) Security policy

(h) (Firewalls) Reference monitor

Problem 2. [Cryptography] (28 points)

(a) (4 points) What are revocation lists for public-key certificates?

(b) (8 points) One way to handle revocation is to put an expiration date in a public key certificate. When the expiration date is reached, the certificate is no longer valid and will not be renewed. What are the disadvantages of this approach?

(c) (8 points) A second way to handle revocation is to maintain a list of "bad public-key certificates" at a central repository that is heavily protected from attack. Assuming that it is possible to protect the repository from attack, what are the disadvantages of this approach?

(d) (8 points) A third way to handle revocation is to broadcast a secure message to all parties alerting them that a particular public key certificate has been compromised. What are the disadvantages of this approach?

Problem 3. [Shamir Secret Sharing] (28 points)

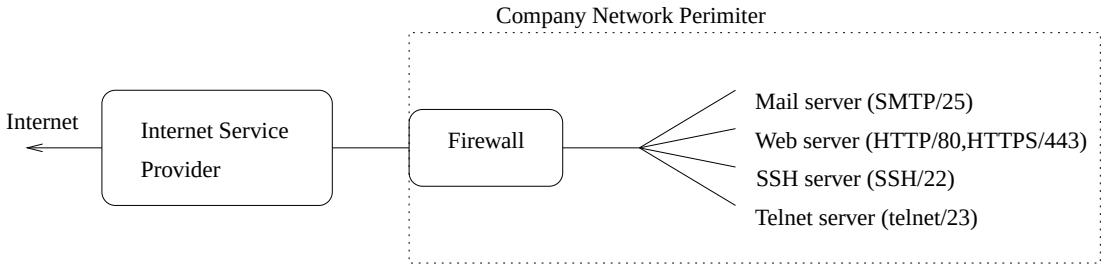
(a) (14 points) Let us review how the Shamir secret sharing system works. The creator of a secret uses a function $f(x) = x^n + a_{q-1}x^{n-1} + \ldots + a_1 x + a_0 \mod p$. What is the secret? What are the secret shares? The modulus p must be larger than the secret; what other restrictions are there on p? How are the shares created? How is the secret reconstructed?

(b) (7 points) One problem with the Shamir secret sharing scheme is that if one of the secret holders is compromised, s/he may provide a bad secret share during reconstruction. In other words, if s/he holds secret s_i, s/he may provide a value different from s_i. Why does this cause a problem for secret sharing?

(c) (7 points) To solve this problem with secret sharing, we may try adding a digital signature. There are two approaches we could use: (i) the secret-share generator could add the digital signature to the secret originally and then generate the secret shares from the signed secret. (ii) the secret-share generator could take the secret and break it into shares, but before distributing the shares, add a digital signature to each share. Compare the advantages and disadvantages of each approach.

Problem 4. [Firewalls] (28 points)

The following diagram shows the architecture for your company's network and connection to the internet.



IP addresses:

ISP router	2.2.2.1
Mail server	1.2.3.5
Web server	1.2.3.4
SSH server	1.2.3.3
Telnet server	1.2.3.2

Example rules:

```
allow * *:*/in -> *:*/out
drop * *:* -> *:*
```

Your company is installing a packet filter firewall. Here is the proposed security policy for the firewall:

1. By default, block all inbound connections.
2. Allow all inbound TCP connections to SMTP on mail server.
3. Allow all inbound TCP connections to HTTP and HTTPS on web server.
4. Allow all inbound TCP connections to SSH on SSH server.
5. Allow all outbound connections.
6. Telnet access should not be allowed (because it sends passwords in cleartext).

(a) (12 points) Using the syntax from lecture (examples above), write the firewall ruleset for your company's firewall. For each rule, give a brief description of its purpose.

(b) (8 points) Hackers target your company's network with repeated requests for large images on your company's webserver. The hackers machines are on the `20.1.21.x` subnet. How could you change your firewall ruleset to block these attacks?

(c) (8 points) Employees start downloading lots of movie trailers from the new Pear SlowTime website at `4.3.2.1:80`. How could you change your firewall rules to stop employees from accessing the website?