Song
Spring 2015

CS 161
Computer Security

Midterm 2

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

I am aware of the Berkeley Campus Code of Student Conduct and acknowledge that any academic misconduct will be reported to the Center for Student Conduct, and may result in partial or complete loss of credit.

SIGN your name: _____

PRINT your class account login: `cs161-`_____ and SID: _____

Your TA's name: _____

Your section time: _____

Exam # for person sitting to your left: _____

Exam # for person sitting to your right: _____

You may consult one sheet of paper (double-sided) of notes. You may not consult other notes, textbooks, etc. Calculators, computers, and other electronic devices are not permitted.

You have 80 minutes. There are 6 questions, of varying credit (270 points total). The questions are of varying difficulty, so avoid spending too long on any one question. Parts of the exam will be graded automatically by scanning the **bubbles you fill in**, so please do your best to fill them in somewhat completely. Don't worry—if something goes wrong with the scanning, you'll have a chance to correct it during the regrade period.

If you have a question, raise your hand, and when an instructor motions to you, come to them to ask the question.

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

Question:	1	2	3	4	5	6	Total
Points:	55	40	45	30	40	60	270
Score:							

Problem 1 ***True or False*** **(55 points)**

Circle TRUE or FALSE, **and use one sentence to justify your answer if your answer is False.**

(a) TRUE or FALSE: A polymorphic virus encrypts the virus body to avoid detection. This means that all copies of the virus have the same encrypted body.

(b) TRUE or FALSE: Malicious software can be installed as a drive-by download automatically, without the user clicking on anything on the infectious site.

(c) TRUE or FALSE: In a CSRF (Cross Site Request Forgery) attack, the attacker needs to steal a victim's cookie.

(d) TRUE or FALSE: The Same Origin Policy (SOP) prevents stored XSS (cross-site scripting) attacks, but not reflected XSS attacks.

(e) TRUE or FALSE: Diffie-Hellman is secure against both passive eavesdroppers and man-in-the-middle attacks. (Note: passive eavesdroppers are attackers who cannot modify packets or send forged packets).

(f) TRUE or FALSE: Suppose Alice wants to share a secret among 10 persons using Shamir Secret Sharing, and Alice chooses a polynomial $f(x) \equiv \sum_{i=0}^{5} a_i x^i \pmod{17}$. Then if 5 persons get together, they can calculate the secret.

(g) TRUE or FALSE: A RSA encryption system has a private key (d, n) and a public key (e, n). If Alice possesses the private key and Bob gets the public key, then Alice can prove to Bob that she possesses the private key without revealing the private key to Bob.

(h) TRUE or FALSE: Private-key cryptography systems relying on a secret private key are a violation of the principle that you shouldn't rely on security through obscurity.

(i) TRUE or FALSE: A firewall that forwards ports by default for those without explicitly specified rules follows the principle of fail-safe defaults.

(j) The Java Language Specification requires that all local variables must be explicitly initialized. TRUE or FALSE: This can be checked via syntactic static analysis.

(k) TRUE or FALSE: Type checking in C compilers is a syntactic static analysis.

Problem 2 ***Modes of Operation*** **(40 points)**

Alice and Bob are communicating over an encrypted channel using AES with key K. Mallory does not know K but Mallory knows one plaintext block P_i and can intercept and modify all the ciphertext blocks sent from Alice to Bob. Mallory's goal is to change the plaintext block P_i to a different plaintext block m. To achieve this, Mallory computes $(P_i \; xor \; m \; xor \; C_{i-1})$ and forwards this ciphertext block to Bob in place of C_{i-1}. In the questions below, an attack is "successful" if Bob decrypts Mallory's changed ciphertext to get m instead of P_i. A block is "not decrypted correctly by Bob" if the decrypted plaintext block does not match the corresponding original plaintext block that Alice wants to send to Bob.

(a) Will this attack succeed if Alice and Bob are using ECB? Which blocks cannot be decrypted correctly by Bob? Explain the reasons.

(b) Will this attack succeed if Alice and Bob are using CBC? Which blocks cannot be decrypted correctly by Bob? Explain the reasons.

(c) This attack will fail if Alice and Bob are using CTR. Can Mallory modify his attack to obtain his goal? Which blocks cannot be decrypted correctly by Bob? Explain the reasons.

Problem 3 ***Web Security*** **(45 points)**

In this question, you will assess the security of a website designed to answer the question that once plagued the internet: is the dress white and gold or blue and black? The website in question is `http://dresscolor.com`. Some important components of this website:

- `http://dresscolor.com/guess.html` is a form where a user can submit their guess as to the color of the dress.
- Users can search the website at `http://dresscolor.com/search.html` for other users based on their color guess.

(a) Suppose `http://dresscolor.com/guess.html` accepts only HTTP POST requests with two parameters: `name` and `color`, and does not use any form of CSRF defense. If an attacker convinces a victim to click on the link `http://dresscolor.com/guess.html?name=victim&color=whitegold`, would the server successfully process the request on behalf of the victim? If so, explain why. If not, explain what the attacker needs to change for the attack to work. Your explanations should be no more than 2-3 sentences.

(b) You note that visiting the following URL does **not** result in an alert being spawned!

```
dresscolor.com/guess.html? name=bob&color=<script>alert('pwnd!');</script>
```

Is `http://dresscolor.com/guess.html` necessarily safe from reflected XSS attacks? Why or why not?

(c) Provided below is the server-side Java code behind `http://dresscolor.com/search.html` that is running a SQL query, which is specified by the user in `user_input`. Supply the user input that would cause the SQL command `DROP TABLES;` to be injected and run successfully. **Hint:** In SQL, specified-length comments are done using `/*` and `*/`. For example, `/* this is a comment */`

```
1  // Assume that user_input is a String that contains
       the user-supplied input, taken as is.
2  for(int i=0; i < user_input.length(); i++){
3      if (user_input.charAt(i) == '\''){
4          user_input = user_input.substring(0,i) + "\\
               " + user_input.substring(i, user_input.
               length());
5          i++;
6      }
7  }
8  // toLowerCase() returns the string in lowercase
       characters only. Ex. "Cs16oNE" => "cs16one"
9  // contains("abc") returns true if the substring "
       abc" exists in the input string, false otherwise
10
11 if (user_input.toLowerCase().contains("drop tables")
       ){
12     user_input = "blueblack";
13 }
14 String sql_query = "SELECT user FROM dressdata WHERE
       color='" + user_input + "';";
15
16 // Run sql_query as a SQL command on the database
```

user_input =

Problem 4 ***Network Security*** **(30 points)**

Circle all that apply.

(a) Which of the following capabilities does an attacker necessarily need to steal a plaintext password that a client sends to `http://facespace.com/`:

A: Drop packets sent by others

B: Modify the payload of IP packets sent by others

C: Inject packets with a forged source IP address

D: Inject packets with a forged destination IP address

E: Eavesdrop on packets whose destination IP address is not the attacker's IP address

F: None of the above

(b) Which of the following capabilities does an attacker necessarily need to perform a DNS amplification denial-of-service attack against a web server:

A: Drop packets sent by others

B: Modify the payload of IP packets sent by others

C: Inject packets with a forged source IP address

D: Inject packets with a forged destination IP address

E: Eavesdrop on packets whose destination IP address is not the attacker's IP address

F: None of the above

(c) Suppose an attacker's IP address is on a blacklist. Which of the following capabilities does the attacker necessarily need to bypass a firewall that filters IP packets whose source IP address is on this blacklist (bypassing a firewall means that the attacker's IP packets are not filtered):

A: Drop packets sent by others

B: Modify the payload of IP packets sent by others

C: Inject packets with a forged source IP address

D: Inject packets with a forged destination IP address

E: Eavesdrop on packets whose destination IP address is not the attacker's IP address

F: None of the above

(d) Which of the following capabilities does an attacker necessarily need to perform DNS blind spoofing (i.e., Kaminsky spoofing):

A: Drop packets sent by others

B: Modify the payload of IP packets sent by others

C: Inject packets with a forged source IP address

D: Inject packets with a forged destination IP address

E: Eavesdrop on packets whose destination IP address is not the attacker's IP address

F: None of the above

(e) In a modern DNS implementation, the ID of a DNS transaction consists of both the Identification and source port (i.e., SRC) fields, which makes DNS blind spoofing orders of magnitude harder. Which of the following capabilities does an attacker necessarily need to perform DNS spoofing against a modern DNS implementation:

A: Drop packets sent by others

B: Modify the payload of IP packets sent by others

C: Inject packets with a forged source IP address

D: Inject packets with a forged destination IP address

E: Eavesdrop on packets whose destination IP address is not the attacker's IP address

F: None of the above

Problem 5 ***Use RSA to share secrets*** **(40 points)**

Suppose Alice wants to share a secret among k ($k \geq 2$) persons such that 1) no single person can recover the secret, and 2) any **two** persons can recover the secret. Instead of using Shamir Secret Sharing, Alice decides to design a new secret sharing system based on RSA. In a RSA encryption system, we have a public key (e, n) and a private key (d, n). The encryption and decryption algorithms are:

$$\textbf{Encryption: } c \equiv m^e \pmod{n}$$
$$\textbf{Decryption: } m \equiv c^d \pmod{n},$$

where m is a plaintext message and c is the ciphertext of m.

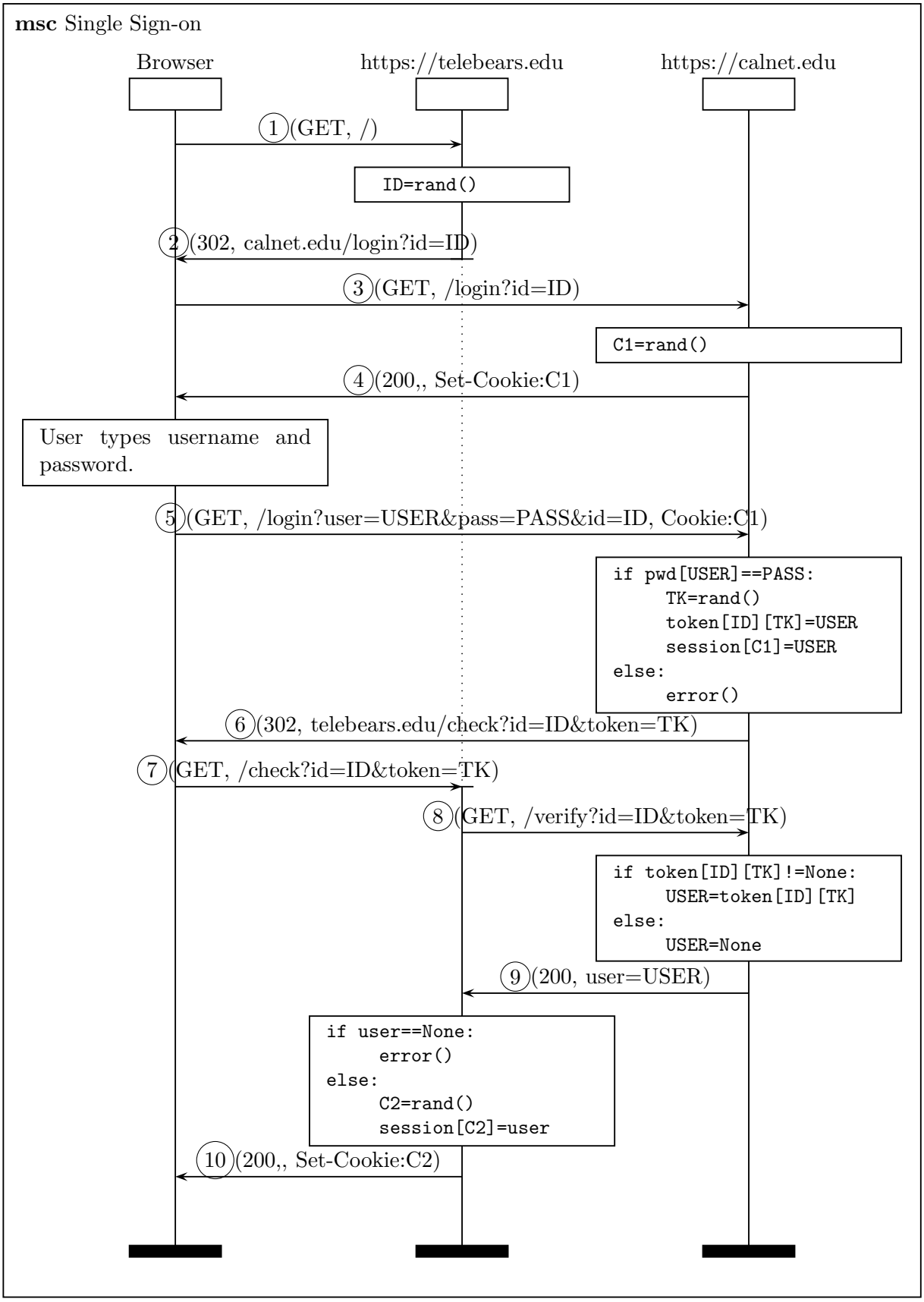
Alice designs a secret sharing system based on RSA as follows:

- Alice generates a single n, and k pairs $(e_1, d_1), (e_2, d_2), \cdots, (e_k, d_k)$, which satisfy that e_i and e_j are relatively prime for any $i, j \in \{1, 2, \cdots, k\}$ and $i \neq j$.
- Suppose m is the secret. Alice computes $c_i \equiv m^{e_i} \pmod{n}$ for each $i \in \{1, 2, \cdots, k\}$.
- Alice sends the tuple (c_i, e_i, n) to the ith person, where $i = 1, 2, \cdots, k$.

Show that this secret sharing system achieves Alice's goal, i.e., 1) no single person can recover the secret, and 2) any two persons can recover the secret.

Problem 6 ***Single Sign-on*** **(60 points)**

Single sign-on (SSO) is a popular way for web applications to allow users to log in using a third-party authetication service, such as Facebook Connect or CalNet ID. The following message sequence chart illustrates a single sign-on protocol similar to the CalNet ID. There are three parties involved in this protocol, the client(`Browser`), the class registration service(`telebears.edu`), and the login service(`calnet.edu`). In order to register for classes on `telebears.edu`, the client needs to be autheticated through `calnet.edu`. (1)-(10) are HTTP requests and responses. An HTTP GET request is represented as `(GET, url, [cookie])`, and an HTTP response is represented as `(200, [data], [setcookie])` or `(302, redirection-url)` where the `redirection-url` is the URL that the browser will be redirected to. The pseudocode in the boxes represent the operations from the three parties. The `rand` function returns a large random number. The `error` fuction terminates the protocol with an error. This chart only shows the flow of a successful login. All communications are using `https`.


msc Single Sign-on
Browser
https://telebears.edu
https://calnet.edu
1 (GET, /)
ID=rand()
2 (302, calnet.edu/login?id=ID)
3 (GET, /login?id=ID)
C1=rand()
4 (200,, Set-Cookie:C1)
User types username and password.
5 (GET, /login?user=USER&pass=PASS&id=ID, Cookie:C1)
if pwd[USER]==PASS:
TK=rand()
token[ID][TK]=USER
session[C1]=USER
else:
error()
6 (302, telebears.edu/check?id=ID&token=TK)
7 (GET, /check?id=ID&token=TK)
8 (GET, /verify?id=ID&token=TK)
if token[ID][TK]!=None:
USER=token[ID][TK]
else:
USER=None
9 (200, user=USER)
if user==None:
error()
else:
C2=rand()
session[C2]=user
10 (200,, Set-Cookie:C2)

(a) Messages (3)-(6) illustrates a typical login process in a web application. However, it is vulnerable to CSRF attacks. A successful attack will cause the victim to log in as the attacker when browsing `calnet.edu` and all websites that integrate `calnet.edu`'s SSO service. Explain how the attack can be performed. In your answer, you should include the URL(s) used in the CSRF attack.

(b) Propose a solution to fix the aforementioned CSRF vulnerability. In your solution, you should list the message number(s) and the fix on each messsage, as well as the addtional checks needed on the server-side.

(c) Assuming the CSRF vulnerability in messages (3)-(6) is fixed, there is another CSRF vulnerability in the overall flow of the single sign-on protocol. A successful attack will cause the victim to log in as the attacker when browsing `telebears.edu`. Explain how the attack can be performed. In your answer, you should list each step of the attack as well as the URL(s) used.

(d) Propose a solution to fix the aforementioned CSRF vulnerability. In your solution, you should list the message number(s) and the fix on each messsage, as well as any addtional checks needed on the server-side.

[Doodle page! Draw us something if you want or give us suggestions or complaints. You can also use this page to report anything suspicious that you might have noticed during the exam.]

Extra page.

1. Do not tear off this page.
2. We will not grade anything on this page unless we are clearly told in the original problem to look here.

Extra page.

1. Do not tear off this page.
2. We will not grade anything on this page unless we are clearly told in the original problem to look here.