CS 361S - Network Security and Privacy
Spring 2017

MIDTERM

March 6, 2017

DO NOT OPEN UNTIL INSTRUCTED

YOUR NAME: ________________________________

Collaboration policy

No collaboration is permitted on this midterm. Any cheating (*e.g.*, submitting another person's work as your own, or permitting your work to be copied) will automatically result in a failing grade. The UTCS code of conduct can be found at `https://www.cs.utexas.edu/academics/conduct`

Midterm (100 points)

Problem 1 (24 points)

Circle only one of the choices **(4 points each)**.

1. **TRUE** **FALSE** The Same Origin Policy ensures that a script in one origin cannot send data to another origin without user intervention.
2. **TRUE** **FALSE** The Same Origin Policy in Web browsers prevents a network attacker from injecting scripts into content received over HTTP from trusted websites.
3. **TRUE** **FALSE** "Perfect message secrecy" means that even with infinite computational power and infinite time, an attacker without prior knowledge of the key cannot recover the plaintext.
4. **TRUE** **FALSE** If the key is truly random, as long as the plaintext, and never re-used, the one-time pad provides perfect message secrecy.
5. **TRUE** **FALSE** If the key is truly random, as long as the plaintext, and never re-used, a block cipher like AES provides perfect message secrecy.
6. **TRUE** **FALSE** If the encryption scheme is secure against chosen-plaintext attacks, an eavesdropper cannot learn anything about the plaintext by looking at the ciphertext, but can still tell if two ciphertexts encrypt the same message by comparing them for equality.

Problem 2

Recall that the definition of a hash function is a function which takes an arbitrary length input and returns a fixed-length output.

Problem 2a (2 points)

If a hash function is collision resistant, does that imply that it is weakly collision resistant? If so, demonstrate why. If not, give an example of a hash function function which is collision resitant but not weakly collision resistant.

Problem 2b (6 points)

If a hash function is one-way, does that imply that it is collision resistant? If so, demonstrate why. If not, give an example of a hash function function which is one-way but not collision resistant.

Problem 3

Problem 3a (6 points)

What are:

- HTTP-only cookies
- Secure cookies

For each flag, describe the differences in how the browser treats a cookie with or without that flag.

Problem 3b (6 points)

Describe an attack which is prevented by HTTP-only cookies.

Problem 3c (6 points)

Describe an attack which is prevented by Secure cookies.

Problem 4

Problem 4a (4 points)

What is a third-party cookie?

Problem 4b (8 points)

You are at home, browsing various flavors of ramen noodles on Amazon (your favorite is chilli-lime with shrimp). Later, you visit your favorite Justin Bieber fansite, and find that many of the advertisements are for instant noodles. How could the advertising network use third-party cookies to learn that you had been looking at ramen noodles on Amazon without violating the same origin policy?

Problem 5 (6 points)

Explain how Facebook "like" buttons enable Facebook to track any of its users across any website implementing the Like button. Does this still apply even if the user is careful never to interact with the button in any way? If so, why does this not violate the Same Origin Policy?

Problem 6 (8 points)

Alice and Bob want to exchange secret messages using a key known only to the two of them. Messages that they send each other are composed of:
`[Encrypt(key, plaintext), HMAC(key, plaintext)]`.

For each of *Confidentiality*, *Integrity* and *Authentication*, indicate whether the scheme upholds the property and why.

Problem 7 (8 points)

Intuitively it seems like an encryption scheme is secure if an adversary can't decrypt the ciphertext without knowledge of the key. Why do we bother with the "encryption game" instead of simply defining security in terms of this property?

Problem 8

You are eavesdropping on encrypted messages between Alice and Bob. You notice that many ciphertexts have the same prefix. When two ciphertexts have the same prefix, it consists of several hundred bytes, and the number of common bytes is always a multiple of 16. The parts of the ciphertexts that follow the common prefix never seem to have any common byte sequences of any significant length.

Problem 8a (8 points)

What kind of cipher is likely being used? In what mode of operation? Explain your reasoning.

Problem 8b (8 points)

What are Alice and Bob doing wrong?

This page intentionally left blank.

This page intentionally left blank.