Homework 2: More Crypto and Web Intro

Due: Thursday, February 13 @ 11:59 pm

Do not include any identifying information (name, login, Banner ID, etc.) on your handin. When you’re done, please submit a PDF file to Gradescope where your answer to each problem is on a separate page.

Reminder: While we encourage everyone to discuss and work through the problems on the homeworks, please remember that you are not permitted to take away notes (hand-written or electronic) from any collaboration sessions—your final solution must be written up independently without relying on shared answers or notes from discussions. Additionally, you are permitted to consult online resources, but you must cite the resources you consulted during your problem-solving process.

Cryptography

Problem 1: Dating with Public Keys

Alice and Bob, both Brown CS students, are secretly dating. In order to set up a meeting, they exchange encrypted messages using a deterministic public key encryption scheme (deterministic meaning that multiple encryptions of a given plaintext always produce the same ciphertext).

Alice and Bob both have their own public-private key pair, \( (PK_A, SK_A) \) and \( (PK_B, SK_B) \) respectively. When Alice wants to send a message, \( m \), to Bob, she encrypts it using his public key and sends the resulting ciphertext, \( c = \text{Enc}(m, PK_B) \), to him. Similarly, Bob’s messages to Alice are computed from \( \text{Enc}(m, PK_A) \).

In plaintext, the messages Alice and Bob exchange are always of the following form:

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIT, 7:00pm</td>
<td>NO</td>
</tr>
<tr>
<td>GCB, 8:30pm</td>
<td>YES</td>
</tr>
</tbody>
</table>

Assume that they always plan to meet at a Brown building, and when referring to a specific Brown building, the name they use is consistent (i.e. they won’t alternate between “SciLi” and “Sciences Library”).

Question a) Trudy is Alice’s curious roommate who wants to find out about the secret dates between Alice and Bob. She knows both of their public keys, the form of their messages, and she can eavesdrop on the ciphertexts being exchanged. Describe how Trudy can find out when and where the next meeting is going to be, even though she is unable to learn the secret keys. (You can assume Trudy knows all possible Brown buildings.)

Question b) Alice and Bob found out that Trudy can learn about their meetings. Propose a simple modification to the protocol that prevents the attack from part (a) and explain why the protocol will prevent the attack. (Your new protocol cannot rely on sending additional messages.)

Problem 2: Commitment Schemes

After Bob didn’t show up at the Graduate Center Bar at 8:30pm (even though he previously agreed to go there in Problem 1), Alice decided that it was time for them to break up. They no longer trust each other, so much in fact that they refuse to be together in the same room. As part of the break up, Bob wants to take one of the \( n \) houseplants he and Alice previously shared. Alice agrees, but she likes some houseplants more than others, and so she doesn’t want Bob to just be able to pick any particular one.
To settle this, they send texts to each other and assign unique numbers \( \{0, 1, \ldots, n-1\} \) to each plant. Then, they agree that Bob should roll an \( n \)-sided die, and Bob will receive the plant that corresponds to the number Bob rolled. However, suppose Bob really wants a particular houseplant with associated number \( b \). All Bob needs to do is simply notify Alice that he rolled \( b \), regardless of what his \( n \)-sided die actually rolled.

**Question a)** Using cryptography, design a protocol between Alice and Bob that emulates the rolling of an unbiased \( n \)-sided die (that is, the outcome is uniformly distributed in \( \{0, 1, \ldots, n-1\} \)), and does it in such a way that neither Alice nor Bob can “cheat” during the protocol; that is, neither Alice nor Bob can affect the outcome of the die roll without the other person knowing. (Recall that Alice and Bob don’t want to meet in person and communicate only via text messages. Your solution should not involve the use of a third-party.)

**Question b)** Explain why your protocol from part (a) prevents Alice and Bob from cheating. You should refer to relevant properties of the cryptographic methods you have employed in the protocol.

**Question c)** In your protocol from part (a), is it possible for Alice or Bob to discover the outcome of the die roll before their ex? If so, what could they do to prevent their ex from knowing the outcome?

**Question d)** Kris is a trustworthy friend of Alice and Bob. Kris is known for keeping their friends’ secrets safe and would never be bribed. Also, Kris can communicate via messages with Alice and Bob and keep track of messages previously exchanged. However, Kris cannot perform any computations. In particular, Kris cannot execute arithmetic operations, run programs, or apply cryptographic methods to the content of the messages transmitted by Alice and Bob. Can Kris help Alice and Bob with their protocol such that they learn the outcome of the die roll at the same time (if at all)? If yes, explain how and why your proposed protocol ensures both Alice and Bob receive the outcome at the same time; if no, explain what parts of the protocol prevent such a system from existing.

**Problem 3: Digital Lockpicking**

While physical locks can usually be broken open with enough time and effort (e.g., lockpicking and bolt cutters), digital locks are not so easy to crack, thanks to encryption. However, there are instances in which it may be beneficial or even necessary for certain parties, such as law enforcement officials, to be able to access an individual’s files behind a digital lock.

We discussed in class the aftermath of a December 2015 mass shooting in San Bernardino, California, in which the FBI and Apple were embroiled in a public debate over implementing a “backdoor” on the iPhone operating system. A similar debate came up recently over the December 2019 shooting at a naval base in Pensacola, Florida.

Please read the following documents:


- This speech by James Comey to the American Bar Association expresses his and the FBI’s view ([https://www.fbi.gov/news/speeches/finding-the-balance-we-need-in-law-and-life](https://www.fbi.gov/news/speeches/finding-the-balance-we-need-in-law-and-life)). Please read from “This is a shadow that’s falling across our work” through the paragraph starting with “Litigation is not the place to solve this problem.”

**Question a)** How might a digital lockpick (like the software Apple refused to develop) be used for good? How might it (or the precedent it sets) be used for evil?

**Question b)** Should Apple have complied with the FBI’s request to bypass personal security mechanisms in the interest of national security, or were they justified in denying their request?

**Question c)** The FBI was eventually able to get into the San Bernardino shooter’s iPhone without Apple’s help. Should the FBI have been required to disclose how they accessed the phone’s contents?
Question d) How much influence should tech industry leaders have in the decisions made by policymakers and national security advisors?

These are open questions and will be graded for thought and justification. Please reference and/or quote specific arguments from the readings in your answers.

Airport Security

Problem 4: Biometric Checkpoints

Prior to the world of securely connected networks and databases, a variation of the following biometric authentication protocol was tested decades ago at the border checkpoints in major U.S. airports.

- Before travelling, a user can “pre-verify” themselves by registering in-person with a registration authority. They present their credentials (e.g., passport, visa) to the registration authority as well as their palmprint. The authority then generates and issues to the user an electronic smartcard that (1) stores data about the user and their palmprint as well as code for a particular palmprint matching algorithm and (2) incorporates a processor to execute the code stored in the card taking as input data on the card and data supplied by the card reader.

- The checkpoint itself has an admission device that contains a palmprint scanner and a smartcard reader. The user inserts their smartcard and provides their palmprint to the scanner. Then, the smartcard internally executes the matching algorithm on the palmprint retrieved by the scanner and the palmprint stored on the card. The algorithm outputs ACCEPT if the two palmprints match; otherwise, REJECT.

There’s an issue with this protocol stemming from the fact that the smartcard stores the palmprint and matching algorithm internally. For example, an attacker could modify the palmprint data in the smartcard so that it matches their own palmprint. Alternatively, the attacker could modify the matching algorithm on the card with one that always outputs ACCEPT.

Given this setup, propose a modification to the protocol that allows the admission device to detect if an attacker has modified their smartcard in any way, and explain why it works. In designing your protocol, you should take into account the following assumptions.

- The processor within the smartcard is tamperproof and cannot be modified without destroying it.
- The admission device is offline. Thus, it cannot send or receive data over a network.
- The admission device has a small amount of storage. Thus, it not have enough storage for a database of biometric data about multiple users.

Web Security

Problem 5: Hotel Cookies

As part of their training, the staff of THE HOTEL CIT are required to take a professional development course called cs666: “Secure Computer Systems”. The TAs of cs666 have implemented an assignment submission system on the course website at http://hotelcit.com/courses/cs666/submissions.

Hotel staff members taking the course provide an email and password to log in to the submission site. The website then issues authenticated users a cookie which contains a session ID that allows the user to authenticate themselves without having to type in their password again for twenty-four hours:

1 In other words, your protocol should not rely on the availability of internet connectivity to the device or a server ready to communicate with the device. Also, note that some United States border checkpoints are not actually in the United States (https://www.cbp.gov/border-security/ports-entry/operations/preclearance), and so the government may not want to rely on a network transfer overseas.
Name: sessionid
Value: [random session ID...]
Domain: hotelcit.com
SameSite: Strict

Authenticated users can then upload their assignments (or download assignment handins that they’ve previously uploaded). There’s two other things worth mentioning about the The Hotel CIT website—first, each hotel staff member has full control over their personal web page on the hotelcit.com domain (i.e. http://hotelcit.com/staff/zespirit/); second, the The Hotel CIT website allows for access via both http and https (similar to the Brown CS website).

**Question a)** Consider Abby, a staff member taking the cs666 course, and Eve, an attacker who eavesdrops on Abby’s network connection while Abby visits the site at http://hotelcit.com/courses/cs666/submissions. Can Eve acquire Abby’s sessionid cookie for the submission system? If so, outline an attack to steal the cookie; if not, explain why.

**Question b)** Consider Zachary, who controls the webpage at http://hotelcit.com/staff/zespirit/. Can Zachary acquire Abby’s sessionid cookie for the submission system? If so, outline an attack to steal the cookie; if not, explain why.

**Question c)** The Hotel CIT now considers various modifications to the cookie scheme.

(i) Suppose the management adds the Secure:TRUE property to the cookie. First, identify what Abby has to change in the way she visits the submission site. Then, answer: does this change any of your answers to part (a) or part (b)? Explain.

(ii) Suppose the management adds the HttpOnly:TRUE property to the cookie instead of the Secure property. Does this change any of your answers to sub-part (i)? Explain.

**Question d)** For this part, only consider Zachary, the attacker from part (b), and ignore the modifications made to the cookie scheme in part (c).

(i) Suppose the management changes the URL of the submission system to cs666.hotelcit.com/handin and changes the Domain property of the cookie to cs666.hotelcit.com. Does this change your answer to part (b)? Explain.

(ii) Suppose the management decides to keep the domain of the submission system as hotelcit.com (and keeps the Domain:hotelcit.com property) and instead decides to put each staff page on its own subdomain, e.g., Zachary’s staff page is now located at zespirit.hotelcit.com. Does this change your answer to part (b)? Explain.

(iii) Suppose the management changes the staff page URLs described in sub-part (ii), but in the process accidentally removes the Domain property; that is, the Domain property isn’t specified when the cookie is set. Does this change your answer to sub-part (ii)? Explain.