Homework 02

Due: 11:59 pm, Monday February 25

Please handin your homework assignment on gradescope as a PDF file with each problem on a separate page.

Public Key Encryption

Problem 1

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 in the sense that encrypting a given plaintext multiple times will always produce the same ciphertext). Alice has a public key/private key pair, (PK_A, SK_A), and Bob has a public key/private key pair, (PK_B, SK_B). Whenever Alice wants to send a message, m, to Bob, she encrypts it using his public key and sends the ciphertext, $c = Enc_{PK_B}(m)$, to him. Similarly, Bob's messages to Alice are of the form $Enc_{PK_A}(m)$. Assume that they always meet at a Brown building and that the messages they exchange are always of the following form:

Bob: `CIT, 7:00pm`
Alice: `NO`
Bob: `GCB, 8:30pm`
Alice: `YES`

Assume that when referring to a specific Brown building, the name they use is consistent (i.e. they won't alternate between "SciLi" and "Sciences Library").

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. Assume Trudy knows all possible Brown buildings.

b) Alice and Bob found out that Trudy can learn about their meetings. Describe a simple modification of the protocol in order to avoid the attack that you described.

Physical Security

Problem 2

A security checkpoint of an airport is a facility where passengers and their carry-on are screened. At the checkpoint, passengers have to present a valid ID and boarding pass. Also, their luggage is scanned and they go through a metal detector or a more advanced full-body scanner (such as a millimeter-wave scanner).

Airports in the US typically have one or more security checkpoints at the entrance of a terminal. Once screened at a checkpoint, passengers can freely move within the terminal and access any gate area. Also, they can linger in the terminal for hours, and possibly even days at major airports that remain open 24×7. We call this arrangement *terminal checkpoints*.

Instead, at some airports abroad, each gate has a separate enclosed area and a dedicated security checkpoint. Passengers are admitted to the enclosed area for a gate only if they are boarding the next flight from that gate. They are screened at the dedicated security checkpoint for that gate and must remain in the

gate area until they board. In case they wish to leave the gate area and come back, they will have to be re-screened at the gate checkpoint. Finally, once the flight departs, any passengers left in the gate area (e.g., they changed their mind about flying, or were denied boarding due to overbooking) must leave. The gate area then becomes available for the next flight. We call this alternate arrangement *gate checkpoints*.

a) Compare terminal checkpoints with gate checkpoints in terms of security, passenger convenience, and cost to operate. Which one is more secure and why? Which one is more convenient and why? Which one is more expensive and why?

b) Can you think about some other arrangement for airport security checkpoints that would provide a reasonable trade-off between security, convenience, and cost?

Web Security

Problem 3

While many sites use cookies to track users and store information about their browsing habits, there exist more sophisticated techniques that are not as easy to detect. This is called browser fingerprinting, and it allows sites to target ads and track users without ever storing any cookies on the client machine.

a) By just visiting a website, what are some possible ways your browser could reveal information about you that could be used to fingerprint you? (Hint: what might make your browser different than someone else's?) Are any of these mitigated by using a private browser session?

b) A common cookie-less tracking technique is called a tracking pixel (also known as web beacon), where a single pixel is loaded onto your webpage from a different server. How could the loading of this image alone be used to track users?

c) An ETag is an identifier (which the browser may treat as a meaningless string) that a server uses to uniquely identify a particular version of a resource for the purposes of caching. When a resource is cached by the browser, any associated ETag is cached as well. When a future request is made for the cached resource, the browser will include the ETag, which allows the server to identify the version of the resource in the browser's cache. It can then respond with the current version or, if the cached version is up-to-date, simply respond with response code 304 ("Not Modified"), indicating to the browser that it should simply use the version in its cache.

   Explain how a server could abuse ETags to track users. That is, explain how a server could use ETags to be able to tell that two HTTP requests came from the same user, even if that user had deleted all of their cookies.

Problem 4

For this problem, it may be useful to consult the ***Request methods*** *section of Wikipedia's article on HTTP.*[1]

Many web pages utilize two common HTTP request methods, GET and POST, for various API calls. Note: For all sub-questions, assume we are using HTTP (not HTTPS/SSL).

a) When is it more appropriate to use a GET request, and when is it more appropriate to use a POST request?

b) When sending data to a server, GET and POST store data in different places in the HTTP request. Explain.

c) What are some ways that sensitive data could be accidentally leaked when using a GET request?

[1] `https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol#Request_methods`

d) There is no way, by clicking on a link or typing a URL into your browser's navigation bar, to initiate a POST request—both of these will initiate GET requests. Given the semantics of GET vs. POST (see the referenced article for details), explain why it's a security feature to prevent either of these (clicking on a link or typing a URL in the navigation bar) from initiating POST requests.

Problem 5

Imagine that Eve is eavesdropping on Alice's internet connection, and that Alice is currently logged into Bob's website, `bob.com`, but she is not actively using it (that is, if she were to visit a page on `bob.com`, she'd be logged in, but she is not currently browsing `bob.com`, and no page from `bob.com` is loaded in her browser). Assume that all connections to `bob.com` use HTTP (not HTTPS), and are thus unencrypted. Assuming that Alice is actively browsing a website that Eve controls, `eve.com`, explain how Eve can acquire Alice's session cookie for `bob.com`.