Network Security (Spring 2022) Due: Thursday, April 14, 11:59 pm

Assignment V

Aniket Kate Purdue University

Please read the questions carefully. There are also 6 bonus points to earn beyond the standard 50 points.
Your answers **must** be typed and uploaded as a PDF document on gradescope. **Only** answer one question/subquestion per page; i.e., start every (sub)question on a different page. If you answer every question (including bonus questions), your written part submission pdf must include at least 18 pages. Include the question number (e.g., **Question 1.a** or **Question 4**) in a bigger font at the top of the page. While submitting on gradescope, use gradescope's answer assignment tool to assign one or more pages to every question. Include and assign an empty page for all unanswered questions.
There is *no* programming part in this assignment.

A: Understanding Questions

As we near the completion of this course, we now focus more on conceptual understanding questions instead of factual questions. The first set of questions in this assignment explores this critical aspect of computer security practice. When you become a security programmer/expert/czar, you will be expected to employ your understanding of previously unseen communication scenarios. This set of questions aims at introducing you to such challenges in a controlled setting.

Question 1: Certificates Infrastructures [2+2+3 points]

a Public key infrastructures employ certificate revocation mechanism using certificate revocation lists (CRLs). In presence of CRLs, why do we include expiration dates in certificates? Envision two advantages of including expiration dates in certificates.

b Every CA must reissue its CRL periodically. It is true even when no new certificates have been revoked after the previous issue CRL has been published. Why? Suggest a possible attack if CRLs are not issued periodically.

c In certificate transparency (CT), explain how the use of a Merkle hash tree makes it possible for a CT log to prove the following three things *efficiently*.

- The later version of a log includes everything in the earlier version, in the same order.
- All new entries come after the entries in the older version.
- A particular certificate has been included in the log.

To demonstrate efficiency, you should compare the Merkle hash tree mechanism with other trivial solutions.

Question 2: Nymity Level [4 pt]

In the lecture, we discussed the (ano)nymity levels as unlinkable anonymity, linkable anonymity, pseudonymity, and veriminity. Suggest the nymity levels for the monetary transactions with each of the following medium:

- Cash
- Gift Certificates,
- Loyalty card + cash
- Credit card

Question 3: TLS [6 pt]

For each of the following threats, explain in detail what mechanism is used in SSL/TLS to provide protection, and how it is used. Do not make any assumptions about the specific encryption/key exchange/signature scheme used by SSL/TLS, as it is supposed to be compatible with multiple schemes.

a A man-in-the-middle adversary records all of the server's messages in an SSL handshake. Later, he impersonates the server by replaying these messages to a client. [2 pt]

b A network attacker poisons DNS cache on the client's recursive resolver and tricks the client into visiting an attacker-controlled IP address instead of an actual IP address of the domain that the victim client was hoping to reach. [2 pt]

c A network attacker modifies the client's "Hello" message in transit and tricks the server into thinking that the client supports only relatively weak cryptographic algorithms. [2 pt]

Question 4: Verified By Visa [3+2 pt]

Many websites invoke third-party payment services, such as PayPal or 'verified by Visa'. These services reduce the risk of exposure of client's credentials such as credit-card number, by having the seller's site open a new 'pop-up' window, at the payment provider's site, say PayPal; and then having the users enter their credentials at PayPal's site.

a Assume that a user is purchasing at the attacker's site. Explain how that site may be able to trick the user into providing their credentials to the attacker. Assume typical user, and exploit typical human vulnerabilities. Present the most effective attack you can.

b Propose and explain two things that may help to reduce the chance of such an attack significantly.

Question 5: Understanding Privacy Risks [10 pts]

Imagine you were in year 2020. All of us are concerned about the spread of COVID-19. To prevent the spread of the disease, your local public health department would want to have information about the contacts of all infected individuals. One way of achieving this is the following: All residents have a health app installed on their phones. When two users A and B come in close contact with one another, the phone apps exchange some information through the use of Bluetooth. Thus, if A is infected, the information on A's phone can be turned over to the health department and used to contact B and notify B of possible

exposure to the disease. While having access to such information is useful, the residents are also worried about being surveilled by the public health department, other residents, and/or the app developers. As a security expert, you have been given the task of designing a system that helps the public health department as well as the residents while solving privacy concerns. In this context, answer the following questions:

a A first suggestion is to share the following information between the phone apps: when in close contact, each phone app shares the following tuple (name, phone number) of the phone owner. If resident A is infected, the health department retrieves all the contact tuples on A's phone and publicly announces them on a website. Does this satisfy the correctness requirement from the perspective of the public health department? What are the integrity and privacy concerns with such a system design against an active/passive adversary? [4 pts]

b A second suggestion is to instead share the tuple $(r, H(r||\text{name}), H(r||\text{phone number}))$ where H is a cryptographic hash function, r is a random 258-bit salt, and $||$ is concatenation operation. Does this satisfy the correctness requirement? What are the integrity and privacy concerns with such a system design against an active/passive adversary? [4 pts]

c Suppose I own a restaurant in your locality and I install a phone with this app installed at the entrance of my restaurant. What information can I learn about my customers just based on the information collected by my phone for each of the above two approaches? [2 pts]

B: Exploratory Questions

Another important aspect of security practice is to read and understand technical material such as blogs, tech-report, and research papers, and employ those in your work. This section explores this essential brach.

Question 7: Cryptocurrencies Only Needs Consistent Broadcast [5+3 pt]

In the lecture, we studied that basic two-party (payer-payee) payment mechanism doesn't require consensus mechanism such as atomic broadcast. We described that consistent broadcast can be sufficient for the task. One of the first paper to discuss that was Fastpay (`https://arxiv.org/abs/2003.11506`) from Novi/Facebook. Read the FastPay paper (reading only first fours pages until the end of Section 4.1 will be sufficient) and answer the following two questions:

a FastPay protocol requires $3f + 1$ equally-trusted authorities, assuming a fixed (but unknown) subset of at most f authorities among those are malicious/active adversaries. This amount to roughly 67% honest (non-malicious) authority servers.

If you recall from the lecture, something like Bitcoin only assumes 51% honesty level. This amounts to $2f + 1$ equally-trusted total authorities for f malicious authorities.

Can you give an example attack when Fastpay reduces its replication factor from $3f + 1$ to $2f + 1$?

b Can you compare the privacy of transactions over Fastpay with the Bitcoin privacy that we discussed in the lecture?

Question 7: Cryptocurrencies Makes Software Updating Harder [4+2+4 pt]

In the lecture, we discussed Bitcoin and Ethereum cryptocurrency/blockchain systems, and the financial service it offers to its users. During the last five years, several hundred other cryptocurrencies and blockchain systems have emerged. Similar to other secure networking protocols, blockchains are also prone to attacks. Read the article 'Responsible Vulnerability Disclosure in Cryptocurrencies' at `https://dci.mit.edu/s/3372115.pdf` and answer the following questions:

a Using two real-world examples explain why vulnerability disclosures are particularly challenging for cryptocurrencies.

b Explain why the authors do not recommend cryptocurrencies to present bug bounties in their own coin.

c With an example, explain how obscurity and lies are employed during cryptocurrency vulnerability disclosure and patching.

[Bonus Question 8]: Simplifying Tor session key establishment [6 pt]

In the lecture, we have studied the ntor protocol (slide 23) to perform 1W-AKE and thereby get a shared session key between a client and a server. In this approach, the server needs to perform two exponentiations to get the session key: in the last step, the server needs to compute $H(g^{xy}, g^{bx})$.

In this exercise, we will look at a variant of this protocol. Assume that we modify the 1W-AKE protocol presented in the lecture such that the session key is calculated as $g^{xy} \cdot g^{xb} = g^{x \cdot (y+b)}$. In this way, the server could calculate $z = (y + b)$ and then do only one exponentiation $(g^x)^z$.

Is this modified version secure? If not, provide an attack.