CS528 Assignment V

Luke Jiang, jiang700@purdue.edu

April 2022

1 Question 1.a

1. Suppose a CA is compromised and issuing rogue certificates undetected. The expiration dates provides an upper bound on how long they can be used. Without the expiration date, such rogue certificates may be used indefinitely.
2. Suppose a new algorithm is proposed. The expiration date promotes more prompt update of the algorithm.

2 Question 1.b

3 Question 1.c

Suppose N represents the number of certificates. Compare Merkle Tree against an array of certificates:

- Using a Merkle tree, one can prove that the root hash of the old tree can be computed from the corresponding nodes in the new tree, which requires O(1) time. Using an array, one must verify that all elements in the old array appear at the beginning of the new array, which requires O(N) time.
- Using a Merkle tree, one can compute the hash of the new entries and check it against the posted value, which requires O(log N) time. Using an array, one must scan all elements, which requires O(N) time.
- Using a Merkle tree, one can verify that the root hash computed from the audit hash matches the current root hash, which requires O(log N) time. Using an array, one can use a binary search of O(log N) time.

4 Question 2

- Cash: Unlinkable Anonymity
- Gift Certificates: Linkable Anonymity
- Loyalty Card + Cash: Peudonymity
- Credit Card: Verinymity

5 Question 3.a

SSL/TLS can prevent replaying attack by using MAC with encrypted message.

6 Question 3.b

SSL/TLS uses certificate to validate server identity, which a spoofing website cannot provide.

7 Question 3.c

SSL can embed version number into the shared secrets sent by the client for the server to check against modifications.

8 Question 4.a

The attacker can implement a phishing pop-up resembling the real third-party payment service.

9 Question 4.b

1. Third-party payment services can send a pin code to a phone number previously selected by the user, and real login window requires the pin code to login. Fake windows do not know the associated phone number, so it cannot send the pin code to the user.

2. Websites can use more restricted payment methods such as Apple Pay, which performs transaction on Apple's private platform.

10 Question 5.a

Assume each resident has a unique (name, phone number), then this suggestion satisfies the correctness requirement. An active adversary can send spoofed tuples through Bluetooth such that two users that are not in close contact are stilled recorded and renders the app useless. A passive adversary can monitor the Bluetooth communication and retrieve all (name, phone number) information of the app users.

11 Question 5.b

This suggestion satisfies correctness requirement, but does not provide forward secrecy. If r is obtained by an attacker, then the attacker can decrypt all previous communications.

12 Question 5.c

For approach a, the owner knows all the phone numbers and names of people walking by the restaurant. For approach b, the restaurant owner knows how many people walking by the restaurant.

13 Question 6.a

14 Question 6.b

15 Question 7.a

1. Monero devs discovered a CryptoNote key image bug and used it to sabotage Bytecoin, which created over a million dollars' worth of coins.

2. DAO, an Etherum smart contract with a reentrance bug was exploited to steal coins worth around $50 million. After a community vote, the patch rolled out was opposed by a minority users arguing that the patch violates the code-is-law principle.

16 Question 7.b

The value of the coin might diminish once the vulnerability is disclosed.

17 Question 7.c

Zcash dev team found a bug but concealed this information from other parties of a disclosure agreement. The dev team tried to silently fix the bug by putting it within a major update and fabricated a markup story.

18 Question 8 (Bonus)