Project 3: CS6035

Yasser Makram
ymakram3@gatech.edu

1 TASK 2

Adding a salt can partially protect a weak password form:

- Offline dictionary and rainbow table attacks
- Discovery of duplicate passwords

The salt needs to be different for different users, and sufficiently large.

The weak password is still vulnerable to online dictionary attacks. Also, weak hashing algorithms prone to hash collisions.

For improved security hashing algorithm like BCrypt and requiring strong passwords with limited minimum length, mix of capitalization, numbers, and special characters. Limiting the number of online login trials can help protect against online dictionary attacks. (Stallings & Brown, 2017)

2 TASK 3

Another consensus protocol is Tendermint, which is used in Proof of Stake PoS chains (Buchman, E., Kwon, J., & Milosevic, Z. 2018). The protocol starts with a proposer broadcasting a state of the network. The proposer is selected via a weighted round robin process according to its voting power. The novel aspect of the protocol is the termination process. The algorithm broadcasts PREVOTE, and PRECOMMIT messages. The protocol has a configurable value f with condition n (total voting power) > 3f. When a correct process receives 2f + 1 PREVOTE messages, it should send a PRECOMMIT message. Upon reception of 2f + 1 PREVOTE message a new round is scheduled. Timeout is configured to prevent processes from blocking.

Compared to proof-of-work

- Gossip based consensus require less computing power and therefore more environmentally friendly.

- PoS can be more scalable and have higher throughput.
- PoS is criticized for being less democratic, as it depends on voting power which is usually correlated with number of tokens owned.
- PoS can be less secure with the possibility of buying enough stake to control the network, while PoW is harder to acquire sufficient computing power.

3 TASK 4

The signature is a hashed digest of the message encrypted with the sender's private key. To verify the signature, the receiver calculates the digest of the received message, decrypts the signature using the public key, and finally compares the two digests (Stallings & Brown, 2017). The steps are:

- Calculate message hash
- Extract signature
- Decrypt signature with public key: M = C Mod N
- Compare the calculated hash to the decrypted digest
- If the values are equal, then the message has not been tampered

4 TASK 5

The first step to get the private key was to factorize the public key. The public key is composed of two parts, Modulus N, and exponent e. The modulus N is computed as a product of two prime number p, q. The numbers p, and q are the prime factors of the modulus N. Getting the prime factors is a hard problem, but since the key space is small, calculating it was feasible.

I tried to get the prime factors using a brute force approach, but the time taken was too long. Instead of brute force, Fermat's factorization method was used (Wikipedia contributors, 2022).

The private key is calculated as d = e^-1 mod phi(N) where phi(N) = (p-1) * (q-1). Since we retrieved the p, and q via factorization, the value phi can be calculated, and the private key is retrieved by getting the reverse modulus of e and phi using Extended Euclidean Algorithm (Wikipedia contributors, 2021).

The underlying mathematical principles were:

- Fermat’s factorization to efficiently get the prime factors of a small key space. Fermat’s factorization has diminishing returns for large key space, but with the provided keys, the calculation was fast.
- Knowledge that the private key is calculated as e^-1 mod phi(N)
- Extended Euclidian Algorithm to calculate the private key from the exponent e and phi(N)

5 TASK 6

The key provided used a weak random generator with low entropy. The weakness in the RNG caused the key to share one factor with some other key. The shared factor can be derived by getting the greatest common denominator between the two keys. Once one factor is known, the other factor is derived by simply dividing the key by the known factor (Heninger, N., Durumeric, Z., Wustrow, E., & Halderman, J. A. , 2012).

The steps to get the private key were:

- Iterate through the key list
- Get the greatest common denominator between the provided key and current key from the list
- If the greatest common denominator not equal to one, the two key share the factor.
- Use the greatest common denominator as p
- Calculate q = provided key divided by p
- Get the private key using p, q as Task 5

6 TASK 7

The broadcast attack works when a small exponent e is used for key construction. The attacker needs e number of messages to decrypt the message using only the public key. The attack is not a full attack as it doesn’t reveal the private key, but it compromises the privacy of the messages.

The vulnerability is caused by using a small exponent. In practice, RSA uses exponents of values 3, 17, and 65537 which are Fermat primes and used to make the modular exponentiation faster (Wikipedia contributors, 2022a).

The attacker can then use the Chinese Remainder theorem to calculate the decrypted message (Wikipedia contributors, 2022b). In the simplest form where the same message M is sent 3 times using different public keys, Ci is calculated where Ci = M^3 (mod N1N2N3) and since M^3 is less than N1N2N3, then C = M^3 and the message can be calculated using cube root of C.

To recover the message the following steps were used:

- Use existence construction method by the computation of Bezout coefficients using extended Euclidean algorithm (Wikipedia contributors, 2022b).
- Calculate Bezout coefficient for pair (N1, N2)
- Use the coefficient in existence construction proof formula to calculate c (N1N2)
- Calculate Bezout coefficient for pair (N3, N1*N2)
- Use the coefficient in existence construction proof formula to calculate c (N1N2N3)
- Calculate cube root of c(N1N2N3) to get the deciphered message.

7 REFERENCES

1. Stallings, W., & Brown, L. (2017). Computer Security: Principles and Practice (4th ed.). Pearson.
2. Buchman, E., Kwon, J., & Milosevic, Z. (2018). The latest gossip on BFT consensus. arXiv preprint arXiv:1807.04938.
3. Wikipedia contributors. (2022, March 19). Fermat's factorization method. Wikipedia. Retrieved March 21, 2022, from https://en.wikipedia.org/wiki/Fermat%27s_factorization_method
4. Wikipedia contributors. (2021, October 24). Extended Euclidean algorithm. Wikipedia. https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm
5. Heninger, N., Durumeric, Z., Wustrow, E., & Halderman, J. A. (2012). Mining your Ps and Qs: Detection of widespread weak keys in network devices. In 21st USENIX Security Symposium (USENIX Security 12) (pp. 205-220).
6. Wikipedia contributors. (2022a, February 15). Coppersmith's attack. Wikipedia. https://en.wikipedia.org/wiki/Coppersmith%27s_attack
7. Wikipedia contributors. (2022b, March 18). Chinese remainder theorem. Wikipedia. https://en.wikipedia.org/wiki/Chinese_remainder_theorem