Rust Cryptography Engineering (Uncloak):

Assignment 1

Tal Derei

24 November 2022

Discord Username: Margulus#4273

Github Repistory: `https://github.com/TalDerei/rust-cryptography-course`

Q1. Describe a concrete example where improving the security of a system against one type of attack can increase the likelihood of other attacks.

Imagine a building as a collection of locked doors and a single false ceiling. The weakest link property states that the burglar can lift up the ceiling panel and climb over any door or wall. Therefore locking the doors simultaneously makes it more challenging for the burglar to break in, and the security guard to check for break-ins.

Q2. Consider a group of 30 people who wish to establish pair-wise secure communications using symmetric-key cryptography. How many keys need to be exchanged in total.

Symmetric keys = (30 x 29) / 2 = 435

Assymetric keys (PKE) = 30

Q3. Suppose Bob receives a messages signed using a digital signature scheme with Alice's secret signing key. Does it prove that Alice saw the message and chose to sign.

In digital signature schemes, Alice doesn't compute the signature herself. Since her compute generates the signature, we can't be sure Alice saw the message or chose to sign it.

Q4. Suppose a chosen-ciphertext attacker cannot recover the secret decryption key for an encryption scheme. Does this mean the encryption scheme is secure?

Not necessarily, there are other attacks such as frequency analysis on ciphers that can be deployed for example.

Q5. Consider a symmetric-key cryptosystem in which cryptographic keys are randomly selected from the set of all n-bit strings. Approximately what should n be in order to provide 128 bits of security against a birthday attack.

If an element can take on N different values, then you can expect a 50% collision after choosing $\sqrt{N}$ random values. If there are 2^n possible values, you need almost $\sqrt{n^2} = 2^{n/2}$ values (birthday bound) before you can expect a collision. Therefore to achieve 128-bit security, you'd need a 256-bit hash.

Q6. What is a side channel attack?

Side channel attacks reveal additional channels of information about a system, e.g. the time it takes to encrypt / decrypt a message of length N.

Q7. Benchmark the speed of an algorithm with Criterion.

1. RSA by @RustCrypto

Benchmarking Results: `https://github.com/TalDerei/rust-cryptography-course/tree/main/week-1`

Q8. What is the difference between symmetric vs asymmetric encryption?

Symmetric Encryption (block ciphers, hash functions, AES) use the same private key for encryption / decryption, while Asymmetric Encryption (RSA, Diffie Hellman, Elliptic Curve) also known as Public Key Encryption involves a pair of private and public keys.