Pedro A. Arias Matos

Dr. Chad Williams

CS 492 – Final Project

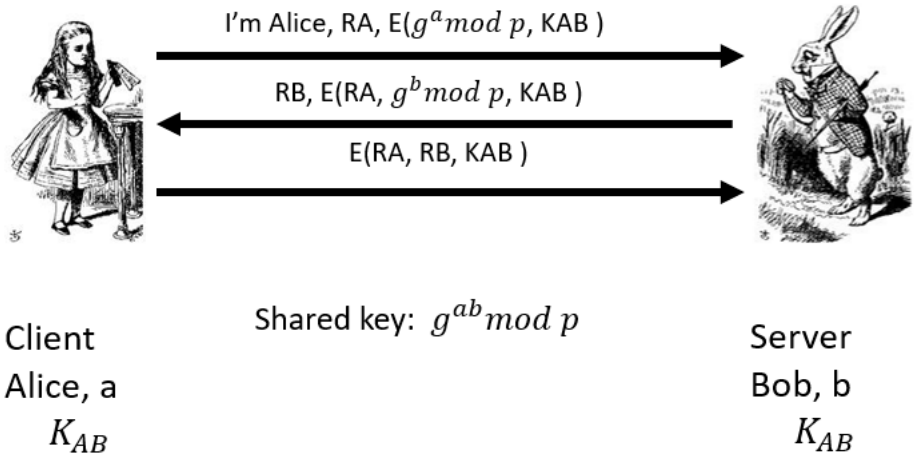
May 1, 2023

Secure Chat Room

The goal of this project is to implement the functionality of a 1-room chat server. The application follows a client-server architecture with mutual authentication, both the client and server authenticate each other to ensure the security of the communication channel. This type of authentication helps to prevent unauthorized access to the network and protect against attacks such as man-in-the-middle (MITM) attacks. The protocol is based on a **shared symmetric key** that is used to establish a session key having perfect forward secrecy. The application makes use of the Diffie-Hellman key exchange protocol to allow the server and client to establish a shared secret key that they used to encrypt and decrypt messages.

The application uses the Advanced Encryption Standard (AES) cipher in Cipher Block Chaining (CBC) mode with PKCS5 padding. CBC mode is a block cipher mode that encrypts each plaintext block using the previous ciphertext block. PKCS5 padding is a method of padding the plaintext before encryption to ensure that the plaintext is an integral number of blocks. It adds padding bytes to the plaintext to fill out the last block, with the value of each byte set to the number of padding bytes added. For example, if two bytes of padding are needed, then both bytes would have a value of 0x02.

Protocol overview



The Diffie-Hellman protocol with perfect forward secrecy allows us to generate a unique session key for each conversation, which means that even if an attacker gains access to the current session key, they will not be able to decrypt past conversations or future conversations.

AES/CBC/PKCS5Padding encryption provides strong encryption and padding to ensure the integrity and confidentiality of the messages sent between the client and server. CBC mode ensures that each plaintext block is encrypted using the previous ciphertext block, adding an element of randomness and making it more secure than simpler block cipher modes. PKCS5 padding ensures that the plaintext is an integral number of blocks, ensuring the ciphertext is of the correct length. Overall, the AES/CBC/PKCS5Padding algorithm is widely used for secure transmission and storage of sensitive data. It provides strong encryption and ensures that the ciphertext is of the correct length, making it a reliable and effective method for securing data.

Overall, the decision to use Diffie-Hellman key exchange and AES/CBC/PKCS5Padding encryption provides a strong and secure method for establishing a session key with perfect forward secrecy in a client-server architecture for a 1-room chat server application. This approach helps to protect the privacy and security of the messages sent between the client and server and ensures that the communication channel is secure even if the secret key is compromised.

Ethical implementations

One of the main ethical implications is the protection of user privacy. Users have a reasonable expectation that their communications will be kept private and secure. The use of strong encryption protocols like Diffie-Hellman and AES/CBC/PKCS5Padding helps to ensure that users' conversations are kept confidential and secure from unauthorized access, providing ethical benefits in terms of privacy and security. However, it is important to note that the use of these protocols also has ethical implications with regards to access and availability of information. Encryption can make it difficult for law enforcement and other authorities to access information that may be necessary for investigations or other lawful purposes. This can create ethical dilemmas around balancing individual privacy rights with broader societal interests. Another ethical implication of using these protocols in a 1-room chat server application is the issue of key distribution. While Diffie-Hellman key exchange provides a secure method for generating a shared secret key, the distribution of the public keys remains a challenge. This means that a public key infrastructure (PKI) would be more appropriate to address the key distribution problem. A PKI provides a framework for managing digital certificates and public key encryption. It enables the secure distribution of public keys, ensuring that the communication channel is secure and authenticated. The use of a PKI can provide greater confidence in the identity of the communication partners, which is particularly important in situations where trust is essential.