INFORMATION SECURITY - CS3002

Project Proposal: Prevention of Man-In-The-Middle Attack in Diffie-Hellman Key Exchange Algorithm using Bitwise Manipulation and Hash Function

Onais Ali Shah 21K – 4691

Mohammad Zohaib 21K –3215

Muhammad 21K– 3192

Project Objectives

The main objective of the project is to develop a method that would allow clients that are using a symmetric encryption algorithm to securely share their keys and make sure that the data that is transferred between them cannot be compromised due to certain active attacks and attacks like Man In The Middle. Other objectives of this project are:

- **Enhanced Security**: Develop a method to prevent Man-In-The-Middle (MITM) attacks during the Diffie-Hellman Key Exchange (DHKE) process.
- **Implement Bitwise Manipulation**: Utilize bitwise operations to enhance the integrity of public keys exchanged during the DHKE.
- **Integrate Hash Functions:** Design a new hash function that ensures the authenticity and integrity of the exchanged keys, thereby mitigating potential vulnerabilities.
- **Evaluate Performance:** Assess the efficiency and security of the proposed solution compared to existing methods in real-world scenarios.

Proposed Solution

The proposed solution involves using Deffie-Hellman for the key exchange, and to create hash values for the key that has to be shared using bitwise manipulation and then a built in hashing library to convert the altered key to a 128-bit hash value using MD5.

Bitwise Manipulation: Implement six specific bitwise operations on the public keys exchanged between parties. This manipulation will obfuscate the keys, making it difficult for an attacker to interpret or alter them during transmission.

Hash Function Development: Create a custom hash function that operates on the manipulated keys. The hash function will be designed to vary its rounds based on the length of the message, ensuring adaptability and robustness against various attack vectors.

Implementation Details

The implementation will include:

- **Key Generation Module**: A module for generating public and private keys using the Diffie-Hellman algorithm.
- **Bitwise Operation Module**: A dedicated component that applies bitwise operations on public keys before transmission.
- **Hash Function Module:** The newly developed hash function will be integrated to validate the integrity of the exchanged keys.
- **User Authentication Mechanism**: An additional layer for user authentication will be included to ensure that only legitimate users can participate in key exchange.

Conclusion

This project is significant as it addresses a critical vulnerability in one of the most widely used key exchange protocols, thereby enhancing overall data security in cryptographic communications. By preventing MITM attacks through innovative use of bitwise manipulation and hashing, this research has the potential to contribute substantially to secure data transmission practices.

The outcomes could lead to improved standards for cryptographic protocols, influencing both academic research and practical applications in fields such as secure communications, banking, and data privacy. The findings from this project may also pave the way for future research into more robust cryptographic methods that can withstand evolving cyber threats.