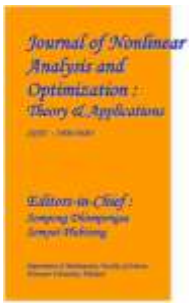
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 13, No. 1, (2022),
ISSN : **1906-9685**



NETWORK LAYER SECURITY USING STATION TO STATION PROTOCOL IN SMART APPLICATION

[1]M Anjineyulu, [2]Anil Kumar Gunda , [3]Mantru Naik, [4]Beeraka Mahesh Babu
[1,2,3]Assistant Professor, [4]Student, Dept. of Computer Science Engineering, Newton's Institute of Engineering, Macherla, Andhra Pradesh, India.

ABSTRACT
A layer that provides data routing routes for network communication. Data is transmitted in the form of packets via logical community paths in an ordered format controlled via the network layer. Logical connection setup, information forwarding, routing and shipping errors reporting are the number one obligations of the community layer. The Station-to-Station (STS) protocol is a cryptographic key settlement scheme. The protocol is based on the classic Diffie-Hellman and provides interaction key and entity authentication. In addition to protecting the installed key from attackers, the STS protocol does not use timestamps and provides strict forward secret. It also allows two-way clear key verification, which becomes the standard key contract with the key verification (AKC) protocol.In this project we present some new unknown key-share assaults on STS-MAC, that is a model of the STS Key Agreement Protocol, which makes use of the MAC set of rules to offer key verification and uses various methods to prevent attacks. Security is a key role in transferring data from one device to another. So by using this approach we can provide security for devices to share data.
Keywords: Network layer, routing, Station-to-station protocol, Diffie-hellman, sts protocol

INTRODUCTION

Cryptography is the science of information security. Cryptography is traditionally referred to as the process of converting general information (plain-text) into an inverted (i.e., cipher). The reverse of decryption, in other words, moves back from plaintext to plaintext. Alice was eager to send Bob a private message after encryption. A cryptosystem consists of a limited set of possible plaintexts. The encryption rule is to encrypt the plaintext into the cipher, and the encryption rule to encrypt the cipher back to plain text. The general idea behind any cryptosystem is that Alice and Bob must share a sector key, which is used to encrypt the message and without which the plaintext cannot be returned. Private-key cryptosystems have a way to secretly share a key k before the transmission of the Alice and Bob plaintext, and they can use encryption and decryption rules defined by the secret value of k. A mechanism for sharing keys is the key agreement protocol, whereby Alice and Bob jointly establish a secret key using values sent to each other through a public channel. On the other hand, public-key cryptosystems mean that Bob keeps his key (and his decryption rule) to himself, but knows the corresponding encryption rule publicly. Therefore, Bob is the only person who can send encrypted messages without pre-sharing Alice's keys and decrypting the message sent to him.

The Diffie-Hellman protocol is a public-key crypto-tosystem developed in 1976 and published in Earth-breaking paper [1]. Diffie-Hellman encryption is not a policy to encrypt data. Instead, it is a method to securely exchange keys that encrypt the data. Diffie-Hellman achieves this secure exchange by creating a "shared secret" (sometimes called a "key encryption key") between the two devices. The shared secret then encrypts the symmetric key (or "data encryption key" which means DES, triple DES, CAST, IDEA, blowfish, etc.) [2] for safe transmission. The security of the Diffie-Hellman key exchange depends on the difficulty of solving the discrete log-arithmetic problem. It is difficult to compute the discrete logarithm of a

http://doi.org/10.36893/JNAO.2022.V13N1.837-840

number modulo because it takes nearly the same amount of time to factorize the product of the two primes, which is the basis of the RSA algorithm.

Section II of this paper introduces the Diffie-Hellman concept, Section III describes Diffie-Hellman's security, and Diffie-Hellman, Section III describes Man-in-the-Middle Attack Diffie-Hellman. Section IV describes a solution to man-in-the-middle attack. The application of elliptic curves to prevent man-to-man attacks is described in Section V with some concepts.

The Diffie-Hellman protocol is based on the DisCrete Logarithm Problem (DLP). Protocol Re queries two large numbers p and g, where, p and g are both publicly available numbers. Parameter p is a prime number with at least 512 bits and is less than integer than the parameter (called generator) property: For each number of combinations of 1 and p-1, the power of k is k = n = gk mod p. Suppose Alice and Bob accept the Shared Secret Key using the Diffie-Hellman Key Agreement Protocol, they generate the Shared Key as follows: First, Alice generates a random private value and Bob generates a random private value b. Both a and b are derived from the same type of integers. Suppose Alice and Bob accept the Shared Secret Key using the Diffie-Hellman Key Agreement Protocol, they generate the Shared Key as follows: First, Alice generates a random private value and Bob generates a random private value b. Both a and b are derived from the same type of integers.

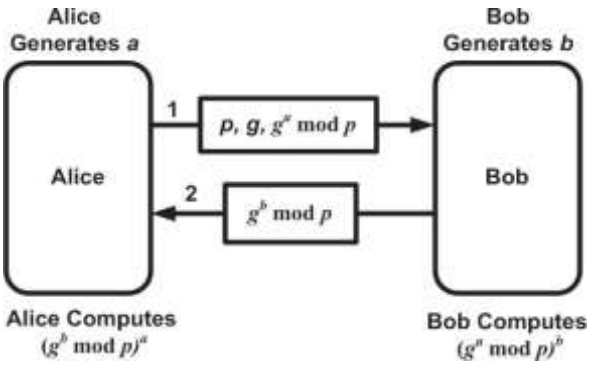


Figure 1: Diffie Hellman Protocol

A. Security of Diffie-Hellman

Evdroper, Mallory, learns the integers p, g, x, y but the discrete logarithm of a and x of b is not the base of y. She wants to determine the secret key k = gab mod p from p, g, x, y. This is known as the Diffie-Hellman problem. She can calculate the discrete log-rhythms mode p and try to solve the Diffie-Hellman problem. She determines the discrete logarithm of y to the base g and calculates the key k = xb. The only known method is to break the Diffie-Hellman protocol. So far, no one has succeeded in overcoming the Diffie-Hellman problem. Finding such proof is an important issue of public-key cryptography. As long as the Diffie-Hellman problem is difficult to solve, no evader can determine the secret key from publicly known information.

A. **Applications of Diffie–Hellman in Network Pro- tocols**

Diffie-Hellman is currently used in many network protocols, such as:

- Secure Sockets Layer(SSL)/Transport Layer Security (TLS).
- Secure Shell (SSH).
- Internet Protocol Security (IPSec).
- Public Key Infrastructure (PKI).
- In all major VPN gate way's today (PKI).

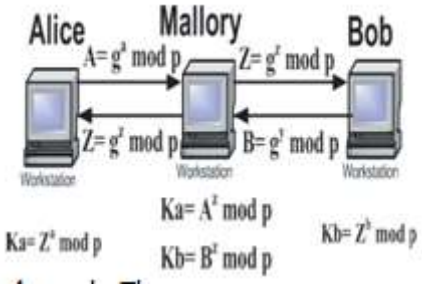
MAN-IN-THE-MIDDLE ATTACK ON DIFFIE–HELLMAN

The Diffie-Hellman key exchange is vulnerable to man-in-the-middle attack. Although this system is not broken, it can be skipped. In this attack, an adversary Mallory not only sets up Alice and Bob, but also sends different messages and stops sending the original message: an adversary Mallory blocks Alice's public value and sends Bob his own public value. When Bob transmits his public value, Mallory substitutes it with her

http://doi.org/10.36893/JNAO.2022.V13N1.837-840

and sends it to Alice. Mallory and Alice agree on one shared key, and Mallory and Bob agree on another shared key. After this exchange, Mallory decrypts any messages sent to Alice or Bob, and then reads them, edits them, and transmits them to the other party before re-encrypting them with an approved key. This vulnerability exists because the Diffie-Hellman key exchange does not authenticate participants.

The man-in-the-middle attack is shown in Figure.



man-in-the-middle attack is shown in Figure.

The Imagine now that an adversary Mallory is capa- ble of now not most effective intercepting messages among Alice and Bob, however additionally stopping them and substituting his personal messages instead. Then Mallory can do the subsequent: pick his own random e ∈ Z∗, and compute gz mod p. Then intercept ga that Alice sends to Bob, and substitute gz as an alternative. Note that Bob does not notice any difference (because, in any case, each ga and gz are random elements of Z∗) and dutifully replies with gb. Mallory intercepts gb, and sends gz to Al- ice as a substitute. This manner, Alice finally ends up questioning that she is sharing ka = (gz)a mod p with Bob, while Bob ends up questioning that he's sharing kb = (gz)b mod p with Alice. Note that, in truth, they are both sharinga key with Mallory, who can compute ka and kb. Now each time Bob tries to ship something to Alice, he will possibly encrypt (and/or authenticate) it using kb . Mallory can intercept it, decrypt with kb, re-encrypt with ka, and send it directly to Alice. So Bob and Alice will in no way realize they may be not sharing a key with each different. This is known as “guy-in-the- center” assault, and is simply one of the motives why key settlement is a tough trouble. In reality, satisfactory formal definitions for key agreement took about a decade and a half longer to appear than definitions for encryption and signature.

Authentication

Possible solutions include using digital signatures and different protocol versions. The authenticated Diffie–Hellman key agreement protocol, or Station- to-Station (STS) protocol, become evolved through Diffie, van Oorschot, and Wiener in 1992 [6] to defeat the man-in-the-center attack at the Diffie–Hellman key agreement protocol. The immunity is executed with the aid of al- lowing the two parties to authenticate themselves to every different via the usage of virtual signatures and public- key certificate. The fundamental idea is as follows: previous to execution of the protocol, the two parties Alice and Bob each obtain a public/personal key pair and a certificate for the public key. During the protocol, Alice computes a signature on sure messages, covering the general public price ga mod p. Bob proceeds in a similar way. Even though Carol continues to be capable of intercept messages among Alice and Bob, she cannot forge signatures without Alice’s non-public key and Bob’s private key. Hence, the improved protocol defeats the person-in-the-center attack.

Digital Signature Algorithm

Digital signatures are used to sign electronic documents. They are just like handwritten signatures. If Alice symptoms a file with her hand- written signature, then all of us who sees the document and also knows Alice’s signature can verify that Alice has in fact signed report. For example, the signature can be used in a trial as proof that Alice has know-how of the document and has agreed to its contents. In precept, digital signatures paintings as fol- lows: assume that Alice wants to sign the report

m. She uses a mystery key d and computes the signatures. Using corresponding public key e, Bob can verify this is in truth the signature of m [5].

http://doi.org/10.36893/JNAO.2022.V13N1.837-840

The DSA signature scheme consists of DSA = (DSA.Key, DSA.Gen, DSA.Ver). DSA.Key generates a non-public-public key pair for the celebration. That is, a public key consists of a top p, an order q which is likewise a prime, a generator g, and y. A private key's x such that y = gx mod p. DSA.Gen makes a signature (r, s) for a message m with the private key x such that r = ((gk mod p) mod q) and s = (k−1(H(m) + xr)) mod p, wherein ok is a random cost and H is a hash characteristic. DSA . verifies a message-signature pair (m, r, s) with the public key y and returns 1 if legitimate or 0 in any other case. That is, the set of rules tests for zero <r,s< q and

A. Message authentication

In this approach, the receiver should make certain approximately the senders identification. One method to provide authentication is with the assist of virtual signature. The concept is similar to signing a record. Digital Signature affords the ultimate three safety offerings; Authentication, Integrity and Non-repudiation. Dig- ital Signature There are two alternatives for Digital Signature: signing the entire report, signing the digest. In the primary case, the entire file is en- crypted using personal key of the sender and on the receiving quit it's far decrypted using the public key of the sender. For a huge message this technique could be very inefficient. In the second case a miniature model of the message, known as digest, is encrypted the use of the non-public key of the digest created using the acquired message is in comparison the decrypted digest. If two are equal , it's miles assumed that the sender is authenticated .This is truly similar to blunders detection the use of parity bit.

User authentication

User authentication is different from message authentication for the reason that identity of the sender is validated for each and each message for message authentication. On the other hand, person authentication is according to- shaped handiest as soon as all through machine access.

References

1. SRDP: Securing Route Discovery in DSR by Jihye Kim and GeneTsudik.
2. Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks by Yuh-Ren TsaiandShiuh-JengWang.
3. A Security Enhanced AODV Routing Protocol by Liu Jun, Li Zhe, Lin Dan and LiuYe.
4. MSR: a novel MPLS-like Secure Routing protocol for Mobile Ad-hocNetworks
5. Y.-C. Hu and A. Perrig, “A survey of secure wireless ad hoc routing,”.
6. Sanzgiri, B. Dahill, B. N. Levine, and E. M. et al. Belding- Royer,“A secure routing protocol foradhoc networks,”.
7. Y.-C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: a secure on-demandrouting protocol for adhocnetworks,”
8. G.Acs , L . Buttyan, and I. Vajda, “Provably secure on- demand sourcerouting in mobile adhoc networks,” IEEE Transactions onMobile
9. Perrig, R. Canetti , D . Tygar , and D. Song, “The tesla broadcastauthenticationprotocol.
10. Authentication and Authenticated Key Exchanges,Paul C. van Oorschot and Michael J. Wiener
11. Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol,Simon Blake-Wilson and Alfred Menezes.
12. Use of Public Key Cryptography in Communication System Design, Leonard M. Adleman AND Ronald L. Rivest.
13. ESSTCP: Enhanced Spread-Spectrum TCP , Amir R. Khakpour, HakimaChaouchi .
14. Dynamic Group Communication Security,Ghassan Chaddoud and ,Ballardie, 1996; Desmedt and Burmester, 1993
15. Sherman, L.W., &Weisburd, D. (1995). General deterrent effects of police patrol in crime“hotspots”: Arandomized,controlled trial.Justice Quarterly, 16, 633–654.
16. Skogan,W. G. (1990). Disorder and decline: Crime and the spiral of decay in Americanneighborhoods.Berkeley: University of CaliforniaPress.