International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 06, June-2015

Secure Data Protection in Insecure Networks using One Time Password based Encryption

Devaraj Verma C,
Department of Information Science
Assistant Professor, PESIT
Bangalore, India

Naveen K R
Department of Information Science
MTech (CFIS), PESIT
Bangalore, India

***Abstract*— Nowadays, due to the sophistication of attacking techniques used by attackers it is becoming very difficult to protect sensitive data. This threat increases exponentially when the data is in transmission in an insecure network such as internet where the data is passed on many devices which are not under the control of the sender of this sensitive information. The first thought that comes to our mind in such circumstance is deployment of encryption but it has its own drawbacks such as compatibility issues, mere usage of some encryption will not solve this problem since any malicious attacker may use advanced cryptanalysis methods to break the encryption to get access to the sensitive information.**

This paper presents some methodologies which involves continuously changing passphrase generation for the encryption of the sensitive information which is passing through an insecure network such as internet. The major challenge here is keeping two nodes informed of the current passphrase which is handled by TOTP (Time based One Time Password) algorithm.

***Keywords* — Encryption, Insecure Network, OTP, One Time Password**

I. INTRODUCTION

Due to the evolution of cloud based services it is becoming more important to protect the data both in storage and transmission. Protection of data in storage is not a big problem as many types of encryption can be employed (even custom methods) without any compatibility problem. But when it comes to the protection of data which is in transmission many challenges are there such as compatibility where both nodes will not have the capability to encrypt or decrypt the packets.

Difficulty of the problem increases more when we consider encryption packet level where dedicated hardware is needed many times which increases the complexity of the solution and may not be possible in all circumstances.

This paper explains a cost effective methods to encrypt the data which is transmitting in an insecure network where the sender of the data has no control or any third party has access to the devices where data travels. In cases like this there is a good chance that third-party may access the data in an attempt to get access to the sensitive information transmitting.

Even if the data is encrypted before sending in the insecure network, many cryptanalysis methods can be employed which involves analysis of large collection of cyphertext and reverse engineering the passphrase. This method is effective when done in massive scale, where the malicious attacker collects large amounts of cyphertext and performs analysis using large computational power.

Most of the traditional methods of encryption involve a single passphrase per node or per session. This is believed to be a weak method for encryption as an attacker with infinite resources can acquire the passphrase even using methods such as brute force. To avoid situation like this a method can be employed where passphrases are changed every few minutes so that even if the attacker decides to the cryptanalysis he will be having a very small time window where brute forcing is very difficult to perform.

Long term analysis will be useless as the packets containing same plaintext after few minutes will completely different cypher text response.

This method involves sharing a secret passphrase between all nodes using a secure channel such as SSL connection for the initial setup. The shared key will be used as a seed key for the generation of passphrase using TOTP (Time based One Time Password) generation method. The time intervals in which passphrase changes can be adjusted according to the convenience and should be set such that it is same in all node which needs to be communicated.

This method works in the higher level before sending the data out to the insecure network the data is encrypted with the OTP (One Time Password) for that time. The packet will be received by the node in the receiving end; once packet is received the receiving node will generate the OTP (One Time Password) for that time if the time is more than the window time the data will be discarded and that data will be requested again from the sending node.

.

II. DATA TRANSMISSION IN INSECURE NETWORK

An untrusted medium of communication is any medium of communication wired or wireless which pass through the network devices which are not controlled by both sender andreceiver of such communication without proper protection such as encryption. Since it is owned and administered by a third party the device and communication channel cannot be trusted. A classic example will be the internet where the communication between two parties normally goes through

many third party devices such as ISP owned router which are not controlled by both sender and receiver.

In any untrusted and unencrypted medium there is a potential for attack or exploitation is more as the potential an attacker can sniff the communication channel and collect data.

If the communication is in unencrypted format the potential attacker can perform following attacks.

A. Passive data sniffing

In passive data sniffing the attacker silently catches all the information going through the devices that he controls. The intention of the attacker may vary depending on the situation, which is normally to gain access to sensitive information without alerting both sending and receiving parties.

B. Active data modification or injection

In active data modification or injection, the attacker silently inject or modify data to the unencrypted communication channel this attack is also known as MITM (Men In The Middle) Attack. It is a dangerous attack since the attacker can impersonate both receiver and sender of the data.

In untrusted and encrypted medium also susceptible to many types of attack such as,

A. Brute forcing of week encryption

when weak encryption is used to protect the data being transmitted in an untrusted medium it is vulnerable to brute forcing. Since in case of weak encryption key will be short an attacker can try out each and every combination to break the encryption and know the key with manageable computing power.

B. Cryptanalysis

It is a cryptographic method where an attacker collects huge amount of encrypted data or cypher texts and performs data analysis algorithms to identify patterns based on this information the attacker can know the type of encryption used and can try brute forcing with more efficient parameters significantly reducing the amount of computing time needed for the brute force attack.

These attacks pose significant risk to any communication which is made in an untrusted communication channel such as internet.

Certain methods such as SSL have been proved to be more effective in this type of environment where a third trusted Third party Certificate Authority (CA). This method may not be suitable in all situations since both parties have to trust the Certificate Authority and should pay annual fee to keep it active. Security infrastructure based on Certificate authority may not be always secure, there are recent incidents where private keys of Certificate Authorities are compromised causing a major security problem for parties who trust that particular certificate authority. Even private key of one particular party in the communication can be compromised and attacker might use them to perform "Man In the Middle Attack".

This demands a need for a secure and easily deployable solution which can provide strong encryption in untrusted communication medium for communicating highly sensitive information. The solution should integrate with any existing system without much modification to the existing system.

III. PROPOSED SOLUTION

The proposed system will have at least two nodes. Initial setup is needed for the system to function which involves exchange of a shared secret.

A. Exchange of shared secret

Shared secret should consist of multiple alpha, numerical and special characters with at least 20 characters in size. Higher key size is imposed to make sure that the system is less susceptible to brute forcing. They should be exchanged in a secure channel preferably SSH or SSL within the secure local environment. An easy ways to do this is using QR codes if mobile devices are involved.

The shared secret which has been exchanged between these devices is used as a seed key for TOTP (Time base One Time Password) generation. The parameters are set such that a new passphrase is generated every few minutes (defined initially). The pass phrase will be used for the encryption of the sensitive content. The encrypted data will be received by the receiving node which will generate the same key by taking pre shared master key and current time as argument. The generated password is only valid for few minutes after which it will be expired and useless.

Due to the involvement of the time there is more than one scenario how data transfer can happen. In the first scenario Node 1 and Node 2 will send encrypted data in the different time window. Where as in scenario both Node 1 and Node 2 will send encrypted data in the same time window thus using the same session keys two times. This increases risk so it should be avoided by using shorter time window. Using shorter time window will make sure that the session key is expired soon giving enough time for the transfer.

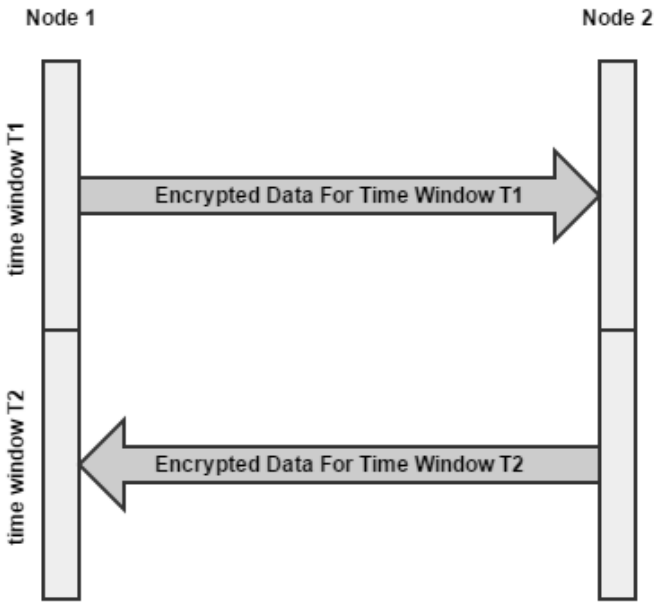

Fig 1. Data transmission is different time window

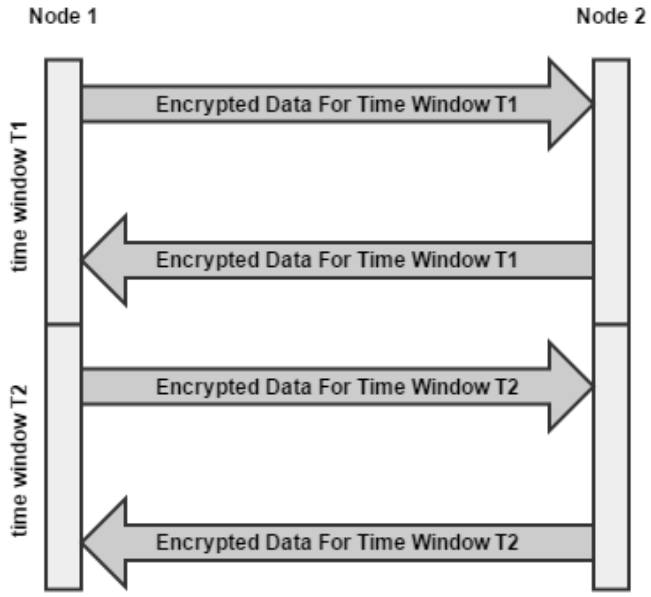

Fig 2. Data transmission is same time window

If a key generated by the receiver is found to be invalid the receiver will again ask for the new data and again same steps will be followed.

In brief following operations will take place during communication.

- The sender will generate a key taking master key and current time as argument.
- The data will be appended with a header identifier to the data.
- Data will be encrypted using AES 256 encryption method.
- The encrypted data will be transmitted to the receiver on other end.

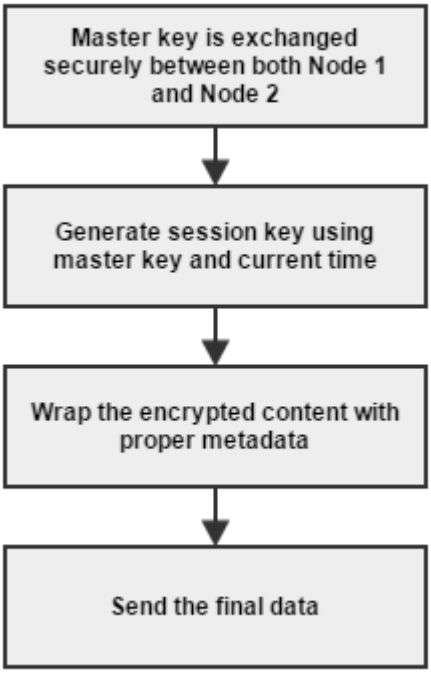

Fig 3. Data encryption life cycle

- Receiver generates a key taking master key and current time as argument.
- 6. Receiver attempts to decrypt the packet.
- 7. After decryption method, header is verified.
- 8. If header is not present as expected, the data will be disposed and sender is asked to send the data again.
- 9. If header check passes, unencrypted data will be extracted.

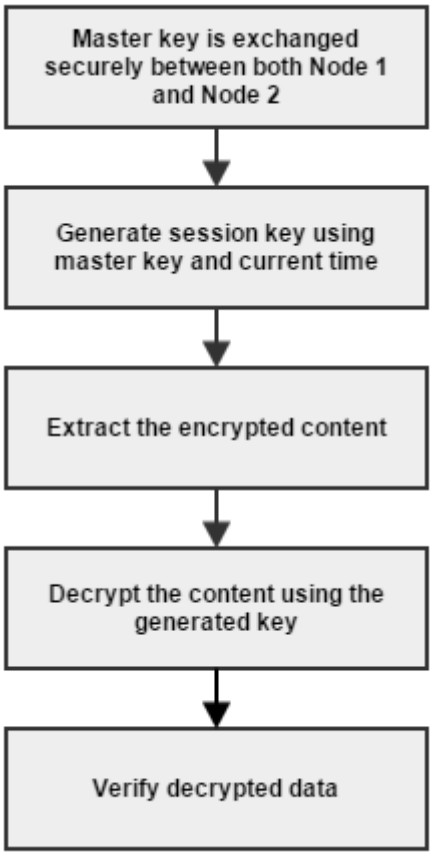

Fig 4. Data decryption life cycle

IV. CONCLUSION

Protection of sensitive data is a very important operation which gets more important when the data is travelling an untrusted medium. Using many techniques avoids situation where these sensitive information is accessed by unauthorized third party. There are many techniques and technologies which help in many cases but in some cases it's difficult to have a procedure which protects the data under transmission but will not expect much modification when it comes to the lower levels of the system. The method described in this paper works well in situation where changes to some parts of the system are not possible. Due to the dynamic passphrase system it's difficult to break the encryption using traditional methods. But here exchange of master key phrase poses risk when handled in an insecure channel. The key exchange should be taken place in a trusted and secure environment where such communications are previously done.

REFERENCES

[1] Ms. E.Kalaikavitha, ,Mrs. Juliana gnanaselvi , "Secure Login Using Encrypted One Time Password (Otp) and Mobile Based Login Methodology", International Journal Of Engineering And Science, 2013
[2] Collin Mulliner, "SMS-Based One-Time Passwords: Attacks and Defence"(short paper), 2012
[3] Uymatiao, M.L.T, "Time-based OTP authentication via secure tunnel (TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystore", IEEE
[4] Neha Sharma, KiranGautam, Praveen Nagar, "One Time Password System for Security over Clouds", International Journal of Advanced Research in Computer Science and Software Engineering, July 2014
[5] Kenneth G. Paterson, Douglas Stebila, "One-time-password-authenticated key exchange", Information Security Group, Royal Holloway, University of London
[6] M. Abadi, L. Bharat, and A. Marais, "System and method for generating unique passwords," U.S. Patent 6 141 760, 1997
[7] Young Sil Lee, HyoTaekLirn, HoonJae Lee ,"A Study on Efficient OTP Generation using Stream Cipher with Random Digit"
[8] Vishal Paranjape, VimmiPandey,"An Approach towards Security in Private Cloud Using OTP", International Journal of Emerging Technology and Advanced Engineering, March 2013
[9] BayalagmaaDavaanaym, Young Sil Lee, HoonJaeLee, SangGon Lee and HyoTeak Lim," A Ping Pong One-Time Password system in Java application".
[10] Michel Abdalla, Olivier Chevassut, and David Pointcheval."One-time verifier-based encrypted key exchange", 2005
[11] Steven M. Bellovin and Michael Merritt. "Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise". In Proc. 1st ACM Conference on Computer and Communications Security (CCS)
[12] Victor Boyko, Philip MacKenzie, and Sarvar Patel, "Provably secure Password-Authenticated Key exchange usingDiffie-Hellman", Preneel [Pre00]
[12] Liang Fang, Samuel Meder, Olivier Chevassut, and Frank Siebenlist, "Secure password-based authenticated key exchange for web services", Proc. 2004 Workshop on Secure Web Service (SWS)