ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Comparative Analysis of Various PPP Authentication Protocols

Surjit Paul, Sanjay Kumar

M.Tech Scholar, Department of Computer Science and Engineering, NIT Jamshedpur, Jharkhand, India

Associate Professor, Department of Computer Science and Engineering, NIT Jamshedpur, Jharkhand, India

ABSTRACT: With the advent of information and communication technology most of the information is accessed or sent through internet. Large no. of users use internet to access and transmit information as per their requirement. But internet is an insecure environment of communication and needs protection against unauthorized access and transmission of information. Thus, security is one of the major issues due to open nature of internet. To achieve confidentiality, integrity, authentication and availability, security is the major issue to protect internet against unauthorized access. Authentication is the process through which one party verifies the identity of the claimed identity. The claimed identity is called claimant and the entity that verifies the claimed identity is called verifier. For authentication, various PPP authentication protocols have been proposed for transfer of authenticated data between entities. All these authentication protocols have their own merits and limitations. In this paper, we have examined various authentication protocols, their merits, limitations and various types of security threats and attacks applicable on them. From the comparative analysis, the suitability of use in a particular application area can be easily recognized and also pave a path to design new PPP authentication protocol free from vulnerabilities and attacks i.e. quantum safe.

KEYWORDS: Network Security, Protection, Confidentiality, Integrity, Authentication Protocol, PPP.

I. INTRODUCTION

Due to advent of information and communication technology, the use of internet for accessing and transmission of information is widely used. In order to protect information accessed through internet a secure authentication is required. Authentication plays a vital role to protect information against unauthorized access and use.Entity authentication is the technique design let one party prove the identity of another party. An entity can be a person, process, client or a server.The entity whose identity is proved is called claimant and the party that tries to prove the identity of the claimant is called verifier In entity authentication, a claimant proves his/her identity to the verifier using one of the three kinds of witnesses: something known, something possessed or something inherent.In password based authentication a claimant uses a string of characters as something he/she shows. Password based authentication can be divided into two broad categories: fixed or one time. Attacks on password based authentication include eavesdropping, stealing a password, accessing the password file, guessing and there is dictionary attack. In challenge–response authentication, a claimant proves that he/she knows a secret without actually sending it. Challenge-response authentication use symmetric key ciphers, keyed hash function, asymmetric key cipher and digital signature. In zero knowledge authentication, the claimant does not reveal his/her secret rather just proves that he/she knows it. Authentication can be categorized as massage authentication and entity authentication. Message authentication also known as data origin. It might not happen in real time and it simply authenticates one message at a time whereas entity authentication deals in real time and authenticates the claimant for the entire duration of the session. The most of the authentication schemes use either password or combination of password and identification token. The task of authentication protocol is to specify a finite series of steps required for authentication. Most of the authentication protocols verify the identity of the claimant before granting them access to information stored in the server. Few protocols use remote authentication for authentication process.

DOI: 10.15680/IJIRCCE.2017. 0502017

The paper is organized as follows: Section II describes the related work carried out; Section III deals with security threats and attacks; Section IV deals with comparative analysis of various authentication protocols and finally section V deals with conclusion and future work.

II. RELATED WORK

Halevi and Krawczyk [1] introduced a notion of security for password authentication. They provide a list of basic attacks that a password-based protocol needs to guard against. The first work to deal with the use of public key techniques in conjunction with password authentication was by Gong et. al.[2]. In that paper, it was suggested that by providing the authentication server with a pair of private/public keys one could protect weak human passwords against strong attacks via the use of public key encryption. Bellare et al. [3] defined a model for the password-based protocol problem and claimed that their model is rich enough to deal with password guessing, forward secrecy, server compromise, and loss of session keys. Another very influential work, by Bellovin and Merrit [4], introduced Encrypted Key Exchange (EKE) which became the basis for many of the subsequent works in this area, e.g. [5, 6, 7, 8, 9, 10]. The Challenge-Handshake Authentication Protocol (CHAP) is used to periodically verify the identity of the peer using a 3-way handshake [11]. Microsoft's PPP CHAP dialect (MS-CHAP), which extends the user authentication functionality, provided on Windows networks to remote workstations [12]. The PPP Extensible Authentication Protocol (EAP) is a general protocol for PPP authentication which supports multiple authentication mechanisms. EAP does not select a specific authentication mechanism at Link Control Phase, but rather postpones this until the Authentication Phase [13]. Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. RADIUS was developed by Livingston Enterprises, Inc. in 1991 as an access server authentication and accounting protocol and later brought into the Internet Engineering Task Force (IETF) standards [14]. Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well [15]. Diameter protocol came as a result of developments to eliminate limitations with the radius gateway. It serves similar purpose in AAA applications however, advanced processes and operations were added to the protocol to make it reliable [16]. In the Fiat-Shamir convention, a trusted outsider picks two vast prime numbers p and q to ascertain the quality of n=p*q. The quality of n is affirmed to general society; the qualities of p and q are kept mystery. Alice the inquirer picks a mystery number s between 1 and n-1[17]. The Feige-Fiat-Shamir convention is like the Fiat-Shamir approach aside from it utilizes a vector of private keys [s1, s2….,sk] , a vector of open keys [v1, v2,… ..vk] and a vector of difficulties (c1, c2… .ck). The private keys are picked arbitrarily, yet they must be relatively prime to n. The Guillou-Quisquater Protocol is a growth of Fiat-Shamir convention in which fewer rounds could be utilized to demonstrate the personality of the petitioner. A trusted outsider picks two prime numbers p and 1 to compute the worth of n=p*q. The trusted gathering likewise declares the example e, which is co-prime with φ=(p-1)(q-1) [18].

III. SECURITY THREATS AND ATTACKS

In this section we have discussed about the various security threats and attacks from the adversary.

a. Eavesdropping: -It is the kind of attack in which attacker listens on the line and tries to learn some useful information from the ongoing communication.
b. Replay Attack: -In this attack the attacker records messages of the past communications and re-sends them at a later time.
c. Man-in-the-middle: - In this type of attack an adversary tries to intercepts the messages sent between the parties and replaces them with its own messages. Here adversary plays the role of the user in the messages which it sends to the server, and also at the same time plays the role of the server in the messages that it sends to the user.
d. Password-Guessing attack: - The attacker is assumed to have access to a relatively small dictionary containing common choices of passwords. There are primarily two ways in which the attacker can use the dictionary

i) On-line attack in which the adversary records past communication, and then goes over the dictionary and looks for a password which is consistent with the recorded communication. If such a password is found, the attacker concludes that this is the password of the user.

ii) Another form of On-line attack in which the attacker repeatedly picks a password from the dictionary and tries to use it in order to impersonate as the user. If the impersonation fails, the attacker eliminates this password from the dictionary and tries again, using a different password.

e. Dictionary attacks:- In cryptanalysis and computer security, a dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or password phrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.

f. Brute-force attacks: - In cryptography, a brute-force attack is an attack in which attacker are trying many passwords or password phrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and password phrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

g. Reflection attack: -It is a method of attacking a challenge-response authentication system that uses the same protocol in both directions. That is, the same challenge-response protocol is used by each side to authenticate the other side. The essential idea of the attack is to trick the target into providing the answer to its own.

h. Impersonation: - The attacker impersonates the client or the server to get some useful information.

IV. VARIOUS PPP AUTHENTICATION PROTOCOLS

Various authentication protocols have been developed but each authentication protocols have some advantages and some disadvantages. In this section we will discuss the advantages and disadvantages of various PPP authentication protocols.

PAP Protocol: It is password based authentication protocols used to authenticate users.

Advantages: Validating Users, Flexible Protocol.
Validating users before allowing them access is an easy way to catch an intruder from stepping into boundaries that they shouldn't cross. P.A.P. will make you go through a small "test" if you will, to insure that the correct person is actually logging in to the system. As far as flexible protocol goes, this is pretty much self-explanatory in the sense that the procedures of P.A.P. can easily be done under any circumstance with its plain text. It passes a plaintext password to the authentication server enabling the server to compare the password with almost any type of storage format.

Disadvantages: Password Strength, Lack of Identity Check, Shoulder Surfing, Plain Text.

CHAP Protocol: It authenticates a user or network host using three way handshaking manner.

Advantages:CHAP provides protection against playback attack by the peer through the use of an incrementally changing identifier and a variable challenge value. The use of repeated challenges is intended to limit the time of exposure to any single attack. The authenticator is in control of the frequency and timing of the challenges.

This authentication method depends upon a "secret" known only to the authenticator and that peer. The secret is not sent over the link.
Although the authentication is only one-way, by negotiating CHAP in both directions the same secret set may easily be used for mutual authentication.

Since CHAP may be used to authenticate many different systems, name fields may be used as an index to locate the proper secret in a large table of secrets. This also makes it possible to support more than one name/secret pair per system, and to change the secret in use at any time during the session.

Disadvantages:CHAP requires that the secret be available in plaintext form. Irreversibly encrypted password databases commonly available cannot be used.
It is not as useful for large installations, since every possible secret is maintained at both ends of the link.

EAP Protocol: It is an authentication framework not a specific kind of authentication mechanism.There are currently about 40 different methods defined for EAP protocol.

Advantages: The EAP protocol can support multiple authentication mechanisms without having to pre-negotiate a particular one. Network Access Server (NAS) devices (e.g., a switch or access point) do not have to understand each authentication method and may act as a pass-through agent for a backend authentication server. Support for pass-through is optional. An authenticator may authenticate local peers, while at the same time acting as a pass-through for non-local peers and authentication methods it does not implement locally. o Separation of the authenticator from the backend authentication server simplifies credentials management and policy decision making.
Disadvantages: For use in PPP, EAP requires the addition of a new authentication Type to PPP LCP and thus PPP implementations will need to be modified to use it. It also strays from the previous PPP authentication model of negotiating a specific authentication mechanism during LCP. Similarly, switch or access point implementations need to support [IEEE-802.1X] in order to use EAP. Where the authenticator is separate from the backend authentication server, this complicates the security analysis and, if needed, key distribution.

Kerberos Protocol: It is a network authentication protocol designed to provide strong authentication for client/server applications by incorporating secret-key cryptography. It was implemented by MIT, USA.

Advantages: The Kerberos is one of the most secure protocols, preventing various types of intrusion attacks.Cross-Forest Trusts permissions in order to use transitive properties and eliminate the “full mesh” scenario; all domains in both forests establish a trust with a single Kerberos trust at the root.Permits interoperability with other Kerberos realms such as Unix operating system; this permits non-Windows clients to authenticate to Windows domains and gain access to resources.
The Kerberos uses “tickets” that can be securely presented by a client or a service on the client’s behalf to a server for access to services.

Disadvantages: Kerberos has a single point of failure: if the Key Distribution Center becomes unavailable, the authentication scheme for an entire network may cease to function.
Password-Guessing Attacks is a second major class of attack on the Kerberos protocols involves an intruder recording login dialogs in order to mount a password-guessing assault.
Spoofing Login In a workstation environment, it is quite simple for an intruder to replace the login command with a version that records users’ passwords before employing them in the Kerberos dialog. Such an attack negates one of Kerberos’s primary advantages, that passwords are never transmitted in plaintext over a network.

RADIUS Protocol: It is a protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.

Advantages: Each individual user session is encrypted uniquely, which prevents other users from acquiring private information. This differs from a PSK network, in which each user shares the same encryption key.A particular user or device can easily be deauthorized by deactivating the corresponding unique encryption key. This simple deactivation ensures that the deauthorized user cannot access the network with any other key and does not affect the security keys for other users.

Network permissions, such as firewall policy, scheduling, and QoS settings, can be assigned within a particular user profile, based on user identity.
A RADIUS server does not require significant server horsepower and can be installed in a way that best fits your needs without changing your current system.
Robust yet inexpensive solution for simplifying security administration while maintaining multivendor interoperability.

Disadvantages: Flaws in the User-Password protection technique, as a relatively new standard vendor support is currently limited.

Fiet-Shamir Zero Knowledge based entity authentication protocol: It is a zero knowledge based entity authentication protocol which allows one party to prove to another party without revealing the secret.

Advantages: It doesn't require someone to reveal secret.Simple – Critical encryption methods are not necessary.
As the verifier does not learn anything about prover's secret s (no knowledge transferred between two parties), he cannot impersonate the prover to a third person. Also the prover cannot cheat the verifier with several iterations of the protocol.
The computational efficiency of ZK protocol is because of its interactive proofs nature. The costly computation related to encryption is avoided.
The security of protocol itself does not get degraded with continuous use as no information about the secret is divulged.
ZK protocols are based on various mathematical problems like discrete logarithms and integer factorization.

Disadvantages: Limited – Translation might be necessary if secret is not a number.
Lengthy – As it has almost 2k entity, it takes a lot of time to compute.
Imperfect – The Intruder can still intercept the message (i.e. messages to the Verifier might be modified or destroyed).

Table 1 shows the comparative analysis of various authentication protocols with different types of threats and attacks. In this we have shown the various security threats to different authentication protocols along with their air of development and strength of the different authentication schemes.

Table 1. Comparison among various authentication protocols

Authentication Protocol	**Year of Development**	**Authentication Scheme**	**Eavesdropping**	**Replay Attack**	**Man-in-the-middle**	**Password-Guessing Attack**	**Dictionary Attacks**	**Brute-force Attacks**	**Reflection Attack**	**Impersonation**
PAP	1992	Weak	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CHAP	1994	Strong	Yes	No	No	No	No	Yes	Yes	No
EAP	2005	Strong	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
LEAP	2005	Weak	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RADIUS	1991	Strong	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Kerberos	1980	Strong	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
PEAP	2005	Strong	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Fiat-Shamir Protocol	1986	Zero Knowledge	No	Yes	Yes	Yes	No	Yes	Yes	Yes
Feige-Fiat-Shamir Protocol	1988	Zero Knowledge	No	Yes	Yes	Yes	No	Yes	Yes	Yes
Guillou-Quisquater Protocol	2004	Zero Knowledge	No	Yes	Yes	Yes	No	Yes	Yes	Yes

V.CONCLUSION AND FUTURE WORK

Various authentication protocols have been proposed and developed for transfer of authenticated data between entities. All these authentication protocols have their inherent advantages, disadvantages and prone to different type of attacks as shown in the table. Hence there is an utmost requirement of proposing a new PPP entity authentication protocol free from different attacks as stated in the table. Our future plan is to propose a quantum safe authentication protocol.

REFERENCES

[1] S. Halevi, H. Krawczyk, "Public-key cryptography and password protocols", ACM Trans. Inform. System Security 2 (3) (1999) pp230–268.

[2] L. Gong, M. Lomas, R. Needham, and J. Saltzer, "Protecting Poorly Chosen Secrets from Guessing Attacks", I.E.E.E. Journal on Selected Areas in Communications, Vol. 11, No. 5, June 1993, pp.648-656.

[3] M. Bellare, D. Pointcheval, P. Rogaway, "Authenticated key exchange secure against dictionary attacks", Advances in Cryptology—Eurocrypt 2000, Lecture Notes in Computer Science, Vol. 1807, Springer, Berlin, 2000, pp. 139–155.

[4] S. M. Bellovin and M. Merritt, "Encrypted Key Exchange: Password- Based Protocols Secure Against Dictionary Attacks", Proceedings of the IEEE. Symposium on Research in Security and Privacy, Oakland, May 1992.

[5] S. M. Bellovin and M. Merritt, "Augmented Encrypted Key Exchange: a Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise", Proceedings of the First ACM Conference on Computer and Communications Security, 1993, pp. 244-250.

[6] D. Jablon, "Strong Password-Only Authenticated Key Exchange". Computer Communication Review, ACM SIGCOMM, vol. 26, no. 5, pp. 5-26, October 1996.

[7] M. Steiner, G. Tsudik, and M. Waidner, "Refinement and Extension of Encrypted Key Exchange", Operating Systems Review, vol. 29, Iss. 3, pp. 22- 30 (July 1995).

[8] S. Lucks, "Open Key Exchange: How to Defeat Dictionary Attacks Without Encrypting Public Keys", The Security Protocol Workshop '97, Ecole Normale Superieure, April 7-9, 1997.

[9] S. Patel, "Number Theoretic Attacks On Secure Password Schemes", IEEE Symposium on Security and Privacy, Oakland, California, May 5-7, 1997.

[10] T. Wu, "The Secure Remote Password Protocol" , in Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium, San Diego, CA, Mar 1998, pp. 97-111.

[11] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, Day Dreamer, July 1994.

[12] G. Zorn and S. Cobb, "Microsoft PPP CHAP Extensions," Network Working Group Internet Draft, Mar 1998. http://www.ietf.org/internet-drafts/draft-ietf-pppext-mschap00.txt.

[13]B. Aboba, L. Blunk,J. Vollbrecht, J. Carlson, H. Levkowetz, Network Working group Request for Comments(RFC: 3748, June 2004.

[14] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[15] B. Clifford Neuman and Theodore Ts'o, "Kerberos: An Authentication Service for Computer Networks", IEEE Communications Magazine, Volume 32, Number 9, pages 33-38, September 1994.

[16] Naman Mehta ,"Introduction to Diameter Protocol - What is Diameter Protocol?", Sun Microsystems. Retrieved 30 April 2009.

[17] U. Fiege, A. Fiat, and A. Shamir ,"Zero Knowledge Proofs of Identity", In Proceedings of ACM Symposium on Theory of Computing (STOC), 1987.

[18]Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography. 5th Ed. CRC Press, 2001.

[19]https://en.wikipedia.org.

BIOGRAPHY

Surjit Paul is an M.Tech scholar of Department of Computer Science and Engineering, National Institute of Technology, Jamshedpur, India. He qualified UGC-NET-JRF and his area of research is mobile computing, wireless sensor network, IOT & IOE, VANET, Cryptography and Network Security.

Sanjay Kumar is an associate professor of Department of Computer Science and Engineering at National Institute of Technology, Jamshedpur, India. His areas of research are mobile computing, network security, parallel computing and VANET.