International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

© Global Society of Scientific Research and Researchers

http://ijcjournal.org/

A General Approach of Authentication Scheme and its Comparative Study

Sanjeev Kumar Mandal[a]*, A. R Deepti[b]

[a]Research Scholar, Department of Master of Computer Application, Acharya Institute of Technology Bangalore-56010, India.

[b]Associate Professor(fka), Dept. of Master of Computer Application, Acharya Institute of Technology Bangalore-560107, India.

[a]Email: sanjeev.mandal93@gmail.com

[b]Email: ar.deepti@gmail.com

Abstract

The field of information security is a vast area which is continually evolving and expanding relative to network data and global communication security. This literature review contrasts the research that has been published in the area of cryptography and authentication protocols, by providing a comparative and analytical study to secure the web servers and services.

Keywords: Authentication; Certificate based authentication; Zero knowledge proof; Single sign on with windows.

1. Introduction

Cryptography is the discipline of art and science by ensuring that messages are secure from possible attacks like eavesdropping, impersonation or corruption. Therefore cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, access control, and authentication. There is an enormous increase in the development and use of networked and distributed systems, by providing increased functionality to the user and more efficient use of resources. To obtain such benefits, the parties have to cooperate by exchanging messages over networks. These parties may be users, hosts or processes; generally referred as principles in authentication literature. Authentication plays an important role in the security of Internet-based applications by providing two-party or multi-party communications.

----

* Corresponding author.

A few types of authentication are user authentication, remote user authentication, mutual authentication, message authentication, and implicit authentication. Authentication is a fundamental concern of providing service related to identification in a secure distributed system. For example, in the established client-server computing paradigm, a server must verify a client's identity before it can make authorization decisions; similarly, a client must ascertain a server's legitimacy before it would proceed with its service request. In other words, authorization and accounting schemes can be built on top of authentication, resulting in the required security to the network system. Therefore, in distributed environment, authentication is typically carried out by protocols, called authentication protocols. The design of authentication protocols is notoriously error-prone. Indeed, many authentication practices have been published and later found to contain subtle weaknesses or flaws which are shown in this review paper. The rest of the paper is organized as follows: by describing the concept of related authentication factors and its environment in section 2. Comparative and analyses study of few authentication protocols is seen in section 3. Finally, the paper is summarized with conclusions and the future work in section 4.

2. Authentication Aspects

The ways in which someone can be authenticated usually fall into three categories known as the factors of authentication, which include: i) something the user knows, such as a password or shared secret. ii) Something the user has such as an ID card or a smartphone.iii) something the user is like face and voice recognition. Despite of the above well-known security issues, passwords are still the most popular method of end-user authentication. Here in this paper, we will focus and discuss on authentication factors over the networks which is given below.

2.1. Single-Factor Authentication (SFA) and Two-Factor Authentication (2FA)

Single-factor authentication (SFA) is a process to secure access to a given system, like network or website that identifies the party requesting access through only one category of credentials. Example of SFA is password-based authentication. As far as SFA services go, user ID and password are not the most secure. One problem with password-based authentication requires knowledge and diligence to create and remember strong passwords. Passwords require protection from many, like carelessly stored sticky notes with login credentials, old hard drives and exploits. Passwords are also prey to external threats, such as hackers using or attacks. Given enough time and resources, an attacker can usually breach password-based security systems. Because of low cost, ease of implementation and familiarity, passwords have remained the most common form of SFA. Also, multiple challenge-response questions can provide more security, depending upon their implementation, and stand-alone biometric verification methods to secure single-factor authentication.

2FA often referred to as two-step verification, is a security process in which the user provides two to verify they are who they say they are. 2FA can be contrasted with a single factor authentication (SFA), by providing an additional layer and makes it harder for attackers to gain access to a person's device and online accounts, because knowing the victim's password alone is not enough to pass the check. 2FA authentication can be divided into two parts; i) tokens that are given to users to use when login, ii) infrastructure or software that recognizes and authenticates access for users who are using their tokens correctly. The tokens may be physical devices or software app to generate PIN codes for authentication which is summarized below. So, the organizations need to have some system in place to accept process to allow or deny access to users authenticating with their tokens. This may be server software, a dedicated hardware server or provided as a service by a third-party vendor.

2.2. Hardware Tokens

Hardware tokens are widely used in two-factor authentication, by providing tokens in hardware device for strong security and easy integration. This device may be in the form of a smart card, USB, Wallet-cards, mobile or may be embedded in a key fob. Examples of tokens applied in devices are car central lock remote system, mobile trusted device unlock system, and ATM etc., Even though the hardware token is used widely it has its own limitation like high cost of implementing the authentication procedure, securing the device, and the user’s chain-of-custody [2]. The chain-of-custody means it involves person-to-person delivery, identification checking and signing the token which goes from manufacturer to vendor to distributor and finally to the customer.

2.3. Soft Tokens

Soft tokens are software-based tokens or applications used to authorize the use of computer services by generating one time password (OTP). A one-time password (OTP) is an automatically generated pseudorandom number that authenticate the user for a single transaction or session to improve the security. One major advantage of using OTP is that no additional hardware or infrastructure is required to implement this method [14].Software tokens are stored on a general-purpose electronic device such as a desktop computer, laptop or a mobile phone. The widespread use of mobile devices has made soft tokens popular and convenient to use and less cost.

However, in contrast with hardware tokens, software tokens can be duplicated, because a user cannot physically possess them. Therefore, these token may be copied or stolen from any of these machines. Another threat is the intruder may use malicious software, to infect any machine to collect the stored soft tokens.

2.4. Certificate-Based Authentication

Certificate-based authentication uses to identify a user, machine, or device before granting access to a resource, network, application, etc. It relies on what the user has, and what the user knows. These certificates are easy to manage, no additional hardware needed and need of minimal involvement from end users. A few examples of certificate involvement are i) automatic certificate creation and validation, including the handling of the corresponding directories like Active Directory, ii) certificate authentication on systems and protocols like ActiveSync, VPN, Wi-Fi and iii) incorporated certificate based client authentication into mobile apps etc. The drawback of certificate-based authentication requires a public-key infrastructure (PKI). This can increase the cost of initial deployment in some environments when compared to public-key authentication. The Certificate Status reporting and updates are not simple. Because revoking a user credential that has become corrupted is difficult, due to the size and complexity of the infrastructure. Usually a CA generates a Certificate Revocation

List (CRL) that may or may not be provisioned within an Online Certificate Status Protocol (OCSP) server. Then each application should check their login for the CRL/OCSP status. This introduces a time delays into the system between the time a PKI credential is reported as compromised and the time when the systems that rely on that credential actually start denying access. Thus the speed of status update can be accelerated to a greater system complexity cost. Finally, the CA still requires a password/pin which may be tampered by the intruder. EAP, MD5, CHAP are few certificate authentication protocol used in the organizations.

2.5. Zero Knowledge Proof authentications (ZKP)

A zero knowledge based entity authentication protocol, allows one party to prove to another party without revealing the secret. As the verifier does not learn anything about prover's secret, he/she cannot impersonate the prover's to a third person. Also the prover cannot cheat the verifier with several iterations of the protocol. The ZKP must satisfy three conditions because of interactive proof of nature: completeness, soundness and zero knowledge property. These protocol can be solved by using mathematical problems like discrete logarithms and integer factorization [8] etc., to improve security. It is simple to use, where critical encryption methods are not required. The drawbacks of ZKP are limited like, i) translation might be necessary if a secret is not a number. ii) Lengthy, as almost 2k entity, so it takes a lot of time to compute. iii) Imperfect, where the intruder can still intercept the message. Nowadays most of organization uses ZKP in real world like cellular radio tower, Network Authentications, Smart Cards, Key Exchanges, Graph coloring problem and cloud database management.

2.6. Single Sign-On with Windows

Single Sign-On with Windows or NTLM is a window Challenge/Response protocol based on data obtained during the interactive login process; consist of a domain name, a user name, and a one-way hash of the user's password. Here it uses an encrypted challenge/response protocol to authenticate a user without sending the user's password over the wire. Instead, the system request authentication by performing mathematical calculations to prove to access the secure NTLM credentials [9]. NTLM authentication comprises into three messages; Type 1 (negotiation), Type 2 (challenge) and Type 3 (authentication). This type of authentication establish a shared context between two parties that include a shared session key for signing and sealing operations by giving NTLM a proprietary authentication. The Single Sign-On with Windows has its own weakness like, NTLM authentication protocol does not support smart card log in. In a multi-tier application, authentication happens on different tiers. In such a setup, to set authorization on the database by using the user's identity, one should be capable of using the user's identity to authenticate on web and database server. Therefore, it is impossible to use NTLM for authentication on every link, because delegation is not supported. Also, the NTLM protocol is not supporting mutual and slower authentication because of pass-through authentication and also not specified in an open standard document (for example in an IETF RFC).

3. Comparative Study of Different Authentication Protocol

3.1. Tables

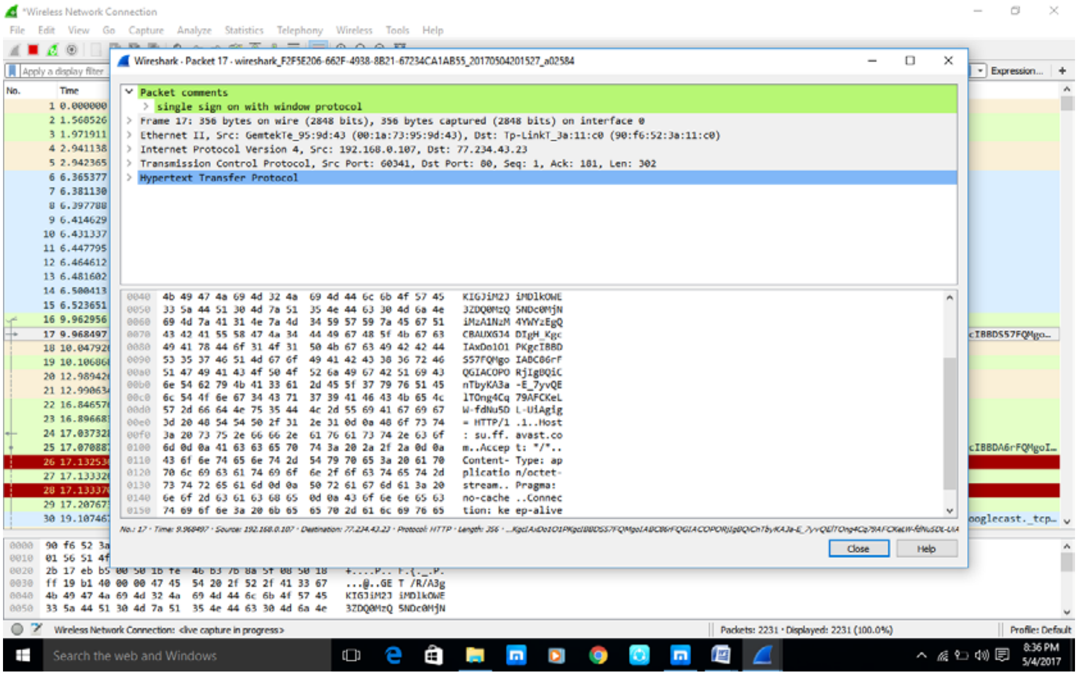
In this paper, a comparative study is done by selecting few authentication protocols and its practices in the real world. The table1 shows the different types of threats, attacks and its strength of different authentication schemes.

Table 1: Security comparison of the defined authentication protocols

Authentication Protocol	Passwords (SFA)	Single Sign-On with Windows	EAP (Certificate based Authentication)	LEAP (Certificate based Authentication)	RADIUS (Certificate based Authentication)	PEAP (ZKP)	Fiat-Shamir Protocol (ZKP)	Software Tokens (2FA)	Hardware Tokens (2FA)
Year of Development	1992	1994	2005	2005	1991	2005	1986	2003	2002
Authentication Scheme	Weak	Strong	Strong	Weak	Strong	Strong	Zero Knowledge	Strong	Strong
Eavesdropping	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Replay Attack	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Man-in-the-middle	Yes	No	Yes	Yes	No	Yes	Yes	Yes	No
Password-Guessing Attack	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No
Dictionary Attacks	Yes	No	No	Yes	Yes	No	No	No	No
Brute-force Attacks	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Reflection Attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Impersonation	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

3.2. Analyze protocols in the Protocol tab

From the comparative study, it is proved that single sign on with window, hardware tokens and Fiat Shamir protocols are more secure. So, with the help of wireshark tool, used in sign on with window is analysed and shows that it is secure from ProRat, Google Hacks, Httrack, Site Digger threats and attacks which is given in Figure1.

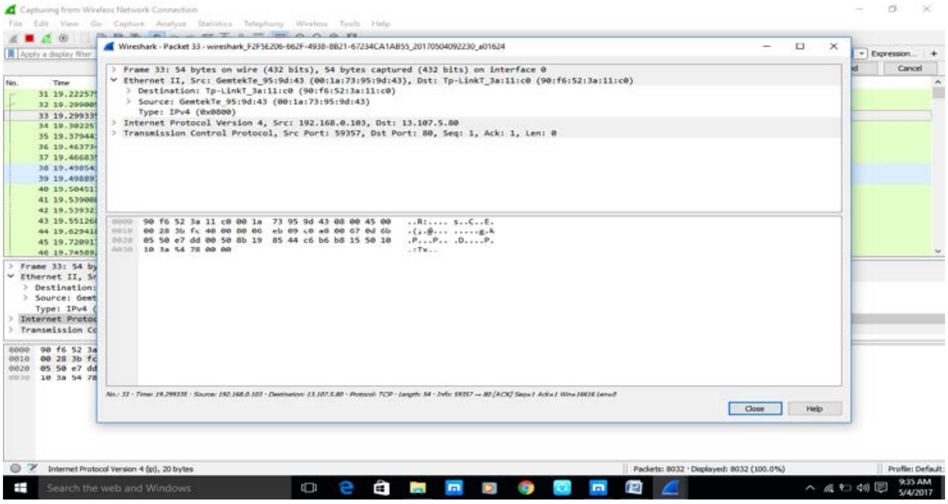


```
Wireshark · Packet 17 · wireshark_F2F5E206-662F-4938-8B21-67234CA1AB55_20170504201527_a02584

Packet comments
  single sign on with window protocol
Frame 17: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits) on interface 0
Ethernet II, Src: GemtekTe_95:9d:43 (00:1a:73:95:9d:43), Dst: Tp-LinkT_3a:11:c0 (90:f6:52:3a:11:c0)
Internet Protocol Version 4, Src: 192.168.0.107, Dst: 77.234.43.23
Transmission Control Protocol, Src Port: 60341, Dst Port: 80, Seq: 1, Ack: 181, Len: 302
Hypertext Transfer Protocol

0040  4b 49 47 4a 69 4d 32 4a  69 4d 44 6c 6b 4f 57 45   KIGJiM2J iMDlkOWE
0050  33 5a 44 51 30 4d 7a 51  35 4e 44 63 30 4d 6a 4e   3ZDQ0MzQ 5NDc0MjN
0060  69 4d 7a 41 31 4e 7a 4d  34 59 57 59 7a 45 67 51   iMzA1NzM 4YWYzEgQ
0070  43 42 41 55 58 47 4a 34  44 49 67 48 5f 4b 67 63   CBAUXGJ4 DIgH_Kgc
0080  49 41 78 44 6f 31 4f 31  50 4b 67 63 49 42 42 44   IAxDo1O1 PKgcIBBD
0090  53 35 37 46 51 4d 67 6f  49 41 42 43 38 36 72 46   S57FQMgo IABC86rF
00a0  51 47 49 41 43 4f 50 4f  52 6a 49 67 42 51 69 43   QGIACOPO RjIgBQiC
00b0  6e 54 62 79 4b 41 33 61  2d 45 5f 37 79 76 51 45   nTbyKA3a -E_7yvQE
00c0  6c 54 4f 6e 67 34 43 71  37 39 41 46 43 4b 65 4c   lTOng4Cq 79AFCKeL
00d0  57 2d 66 64 4e 75 35 44  4c 2d 55 69 41 67 69 67   W-fdNu5D L-UiAgig
00e0  3d 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   = HTTP/1 .1..Host
00f0  3a 20 73 75 2e 66 66 2e  61 76 61 73 74 2e 63 6f   : su.ff. avast.co
0100  6d 0d 0a 41 63 63 65 70  74 3a 20 2a 2f 2a 0d 0a   m..Accep t: */*..
0110  43 6f 6e 74 65 6e 74 2d  54 79 70 65 3a 20 61 70   Content- Type: ap
0120  70 6c 69 63 61 74 69 6f  6e 2f 6f 63 74 65 74 2d   plicatio n/octet-
0130  73 74 72 65 61 6d 0d 0a  50 72 61 67 6d 61 3a 20   stream.. Pragma:
0140  6e 6f 2d 63 61 63 68 65  0d 0a 43 6f 6e 6e 65 63   no-cache ..Connec
0150  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive

No.: 17 · Time: 9.968497 · Source: 192.168.0.107 · Destination: 77.234.43.23 · Protocol: HTTP · Length: 356 · ...KgcIAxDo1O1PKgcIBBDS57FQMgoIABC86rFQGIACOPORjIgBQiCnTbyKA3a-E_7yvQE...
```

Close
Help
Wireless Network Connection: <live capture in progress>
Packets: 2231 · Displayed: 2231 (100.0%)
Profile: Default
8:36 PM
5/4/2017

Figure 1: Single Sign on with Window is analyzed with wireshark tool for its efficiency

The remaining protocols from table1 are also analyzed in order to check its security by using the Wireshark tool to show its weakness in Figure 1.1.



```
Wireshark · Packet 33 · wireshark_F2F5E206-662F-4938-8B21-67234CA1AB55_20170504092230_a01624

Frame 33: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: GemtekTe_95:9d:43 (00:1a:73:95:9d:43), Dst: Tp-LinkT_3a:11:c0 (90:f6:52:3a:11:c0)
  Destination: Tp-LinkT_3a:11:c0 (90:f6:52:3a:11:c0)
  Source: GemtekTe_95:9d:43 (00:1a:73:95:9d:43)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.0.103, Dst: 13.107.5.80
Transmission Control Protocol, Src Port: 59357, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

0000  90 f6 52 3a 11 c0 00 1a  73 95 9d 43 08 00 45 00   ..R:.... s..C..E.
0010  00 28 3b fc 40 00 80 06  eb 09 c0 a8 00 67 0d 6b   .(;.@... .....g.k
0020  05 50 e7 dd 00 50 8b 19  85 44 c6 b6 b8 15 50 10   .P...P.. .D....P.
0030  10 3a 54 78 00 00                                  .:Tx..
```

Close
Help
Internet Protocol Version 4 (ip), 20 bytes
Packets: 8032 · Displayed: 8032 (100.0%)
Profile: Default
9:35 AM
5/4/2017

Figure 1.1: Weakness of EAP, RADIUS, LEAP, PEAP etc., is analyzed by using wireshark tool

Thus, from the above test, it is prove that these protocols should be improved in order to protect the security.

4. Conclusion and future work

In this paper, a general approach of authentication practices is presented. Then, a comparative study is made between the protocols to check its security complexity. Furthermore, analysis is done in order with the help of tool to provide a satisfying security level in terms of data transmission and time. Since the research on authentication protocols is a relatively young area, the number of new formulate protocols is increasing as long as many attacks are appearing so direction of the future research work is about verifying their efficiency.

References

[1] L.C.K. Hui, J.C.K. Yau, E.K. Wang, S.M. Yiu, Z.L. Jiang. The WHO Hardware Token Security Model. In June 26, 2006, HKU CS.

[2] Kingpin Attacks on and Countermeasures for USB Hardware Token Devices. 196 Broadway, Cambridge, MA 02139, USA.

[3] Manav Singhal and Shashikala Tapaswi, “Software Tokens Based Two Factor Authentication Scheme.” in International Journal of Information and Electronics Engineering, Vol. 2, No. 3, May 2012.

[4] LiPing Du, JianWei Guo Ying Li. “Research on Micro-Certificate based Authentication Protocol.” Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013).

[5] Karthik Sadasivam, T. Andrew Yang. Evaluation of Certificate-Based Authentication in Mobile ad hoc Networks. University of Houston-Clearlake Houston, TX, USA.

[6] Davaanaym, Y.S. Lee, H.J. Lee, S.G. Lee, and H.T. Lim. “A ping pong based one-time-passwords authentication system.” In 2009 Fifth International Joint Conference (NCM ’09) on INC, IMS and IDC, pages 574–579. IEEE Computer Society, 2009.

[7] Yeen-Yin Choong, Kristen K. Greene, Mary F. Theofanos, “Authentication and Lifecycle Management.” Internet: www.pages.nist.gov/800-63-3/sp800-63b.html, [TBD 2017].

[8] U. Fiege, A. Fiat, A. Shamir. “Zero Knowledge Proofs of Identity.” in Proceedings of ACM Symposium on Theory of Computing (STOC), 1987.

[9] Microsoft. “Microsoft NTLM.” Internet: https://msdn.microsoft.com/enus/library/windows/desktop/aa378749 (v=vs.85).aspx.

[10] Eman El-Emam, Magdy Koutb, Hamdy Kelash, and Osama Farag Allah. “A Network Authentication Protocol Based on Kerberos.” IJCSNS International Journal of Computer Science and Network Security, Vol.9 No.8, August 2009.

[11] Sanket Bhat, Damle, Priyanka Chaudhari, Abhijeet. “An Authentication Protocol.” International Journal of Advance Research in Computer Science and Management Studies, [On-line]. Volume 2, Issue 2, Available: www. ijarcsms.com/docs/paper/volume2/issue2/V2I2-0081.pdf February 2014.

[12] L. Gong, M. Lomas, R. Needham, and J. Saltzer, “Protecting Poorly Chosen Secrets from Guessing Attacks." IEEE Journal on Selected Areas in Communications, [On-line]. Vol. 11, No. 5, June 1993, pp.648-656, Available: www.pdfs.semanticscholar.org/6b47/9047219fc565a478efbe95572806cd03a7a1.pdf.

[13] M. Bellare, D. Pointcheval, P. Rogaway, “Authenticated key exchange secure against dictionary attacks.” in Advances in Cryptology— Eurocrypt 2000, Vol. 1807, Springer, Berlin, 2000, pp. 139–155.

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

[15] M. Steiner, G. Tsudik, and M. Waidner, “Refinement and Extension of Encrypted Key Exchange." ACM Conference on Operating Systems Review, vol. 29, Iss. 3, pp. 22- 30 July 1995.

[16] Manav Singhal and Shashikala Tapaswi, “Software Tokens Based Two Factor Authentication Scheme.” in International Journal of Information and Electronics Engineering, Vol. 2, No. 3, May 2012.