International Journal of Engineering & Technology, 7 (4.12) (2018) 58-62

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Analysis of information security service for internet application

Ravi Shanker[1]*, Dr. Sahil Verma [2], Dr. Kavita[3]

[1] *Department of Computer Science & Engineering, Lovely Professional University*
[2] *Department of Computer Science & Engineering, Lovely Professional University*
[3] *Department of Computer Science & Engineering, Lovely Professional University*
**Corresponding author E-mail: sahil.21915@lpu.co.in*

Abstract

Background/Objectives: With the proliferation of online platforms, information is generated every second, and there is an urgent need to firstly store the huge amount of data and secondly to secure that data. The level of sophistication is increasing day by day, so alongside the demand for excessive computational power and resources also hikes up. With the advancements in technology and with the concepts like globalization coming into picture, people find the need of sharing information important. Methods/Statistical Analysis: Information security aspects are analyzed based on confidentiality, integrity, availability, authentication, authorization and non-Repudiation. Findings: Different web application needs different security parameter and out of these authentication and access control are among the top security issues which can be resolved by using two factor and three factor authentication and are more effective with respect to mobility. Application/Improvement: Most handheld devices have built-in sensors which can be used for self authentication and authorization. Device ID, fingerprint, iris, SMS based OTPs add extra security to information security.

Keywords: *Authentication, Authorization, fingerprint, Information security, OTP, Two-factor.*

1. Introduction

With the progress of internet and networking technologies everything is going on the web. From government to business organizations everything is accessible online. The information related with business and government associations is extremely classified. Therefore, it is critically necessary to shield the data from unknown and unauthorized access. Keeping in mind the end goal a large portion of the users utilize cryptographic methods with the aim of encrypting their personal data so that only authorized people have access to it. There are so many services which provide online storage of data and for securing such data user need to create strong password and more secure communication channel. Data security is a main concern for the user, as the user doesn't know the location of the stored data. To reduce the storage and computing burden, users stores their personal and sensitive information at the data centre offered by the server. An example a patient stores their health record on the data centre offered by the Cloud Service Providers (CSP). Patient must prefer to share his information with trustworthy user, as any modification with information may risk the patient life.

There are some factors required to enhance the security requirements for network environment. Data needed to be stored in encrypted form on the server and communication must be made through secure channel. A proper access control mechanism is required to control the access of user data by semi-trusted or fully trusted by the service provider. Weak username and password cannot verify the valid user as they are easily estimated; even strong passwords don't provide the required security. Hence, a proper identification method is required to verify the validity of the user. Identify the trust worthy clients who want to access the data. To enhance the data security service providers are required to maintain proper logs. Proper scheme must be identified to evaluate the trustiness of service provider and third party. In existing technology, when data owner saves their data on the server, it requires the data owner to be online to grant the access permission to the data requester.

2. Literature survey

According to Das A, Bonneau J (2014), people (especially in public sectors) generally utilize passwords which are frail and simple to figure out [1]. Proper guidelines must be followed for strong password. Common guidelines proposed by security experts of software system security include a password length of eight or more characters as per required validation. It must include lowercase and uppercase alphabetic characters, and some combination of numbers and symbols. A strong password is made up of a number of different combinations of numbers, alphabets and symbols. For instance, it should be at least 6 - 8 characters long and should include at least one or two uppercase letters, lowercase letters and minimum one or two number. Many people think that a strong password is a harder task to create, tough to remember and to access the online accounts they need to type. Due to this unawareness most of the passwords generated or set by user are very weak and easy to crack by using just guessing, social engineering or by some tools. Strong passwords are an essential for keeping crackers and hackers away from accessing personal data from online portals.

Online accounts with weak passwords are definitely not hard to crack since various password cracking online tools and software's are getting more sophisticated and can be easily broken within few minutes or hour due to technology enhancement of computing hardware [2] analyzed by De Carnavalet XD, Mannan M (2014). Thus, just a username/password combination isn't adequate to ensure online safety of users account. Hence, Grosse E, Upadhyay

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

M (2013) concluded that there is a strong need of more advanced and sophisticated authentication techniques [3]. But using Password-only authentication is not a solution. So the need is to combine passwords with multifactor authentication, social login with limited use, biometrics etc.

Use of distributed networks is progressing at a rapid rate. With the rapid growth of online users, sensitive information sent across the network needs to be secured using advanced security mechanisms [4] identified by Zissis D, Lekkas D (2011) specially for the distributed networks. In order to protect sensitive information authentication needs to be done before exchanging the data. A distributed network is a joint combination of different networks. In a distributed system, organization resources are divided over a number of processors and networks. Birman KP, van Renesse R (1994) identified objective for Network management software powered the distributed network that monitors the core networking processes, data routing, bandwidth usage etc. These objectives need to meet while building a distributed system: Making Resource Accessible, Distribution Transparency, Openness and Pitfalls [5].

According Carlin S, Curran K (2013) to For instance in cloud computing user stores the data on the cloud but don't know the location of the data being stored. Data exchanged or stored could be any sensitive data (like health report of any user). For security reasons, some basic security administrations are required, for example authentication, authorization, encryption and decryption. As storage location of data is unknown, users cannot trust the cloud services completely. Cloud Computing shares resources and distributed services that belong to different locations or organizations [6]. Sharing confidential information without any security measure can be handy for an organization or users.

According to Perlman R, Kaufman C (2016), two simple goals of network security are [7]:

1. Preventing unauthorized access to resources.
2. The required resources can only be accessed by authorized person.

According to a research published in 2018 Data Breach Investigations Report by Verizon, 24% of breaches affected healthcare organizations, 15% of breaches involved accommodation and food services, 14% were breaches of public sector entities and 58% of victims are categorized as small businesses More than 20% of all the data breaches were related to financial institutions (e.g. bank account details, credit card information or other bank information). Furthermore, less than 10% of the Gmail account holders were found to be using two-factor authentication service [8]. A stronger security mechanism like Two-factor authentication 2FA provides an additional layer of security instead of using just a password which makes it harder for attackers to gain access to a user's devices and online accounts. Using 2FA it very tough task to pass the authentication check by just knowing the user's password. Google is using 2FA using password and a code sent over phone. Two-factor authentication has long been implemented by Google for preventing unauthorized access to personal information and device access. Among several other methods, SMS based two-factor authentication is most common for online services are increasingly used these days to prevent users' data from being accessed by hackers proposed in [9] by Aloul F, Zahidi S (2009).

The new age Smartphone is a standout amongst the most dependable options for multi-factor verification. A location based OTP (One-Time Password) technique is proposed in [10, 11] by Sun H, Sun K (2015) which was quite successful in avoiding many attacks. An OTP is an automatically generated number that authenticates the user for only one transaction at a time or may be used for creating session between user and server. OTP enhances the level of security by adding random password to the traditional user ID and password and it changes every time user login for a service. Time-based OTP (TOTP) and HMAC-based OTP (HOTP) are two most common types of OTP solutions. For generating OTPs various mechanism are available. It can be a random number generated by the application itself or rely on hardware used for generating tokens.

In order to eliminate vulnerabilities in the existing system, another two-step authentication system was proposed by the author in [12] proposed by Abdurrahman UA, Kaiiali M (2013) who used GPS location and timestamp. Stage 1: Login - The user requests his personal web page URL through any mobile device. The web server will respond back with the login page requesting the user to provide his user ID and password. The user provides his user id and password to web page which is post back to server for verification. If the user credential is verified, Server asks for the one time password in the form of security token. In stage 1 when the user login to the server, it record user timestamp and GPS information to the server. Both client and server must be synchronized for the first time when a user register with the server for the first time.

Stage 2: Token Generation – an application for generating security token must be installed on the user GPS enabled mobile device which is responsible for generating the security token according to the following equation where current time stamp: Token =hash (Pre-Shared Number + GPS + time stamp).

Stage 3: Token Verification - Authentication Server receives the security token and it calculate its own hash value based on user timestamp and GPS information using equation used in stage 2. Then it compares both token, if the received token hash is matched with the server calculated hash value, the user is authenticated and user will be respond back with the requested web page i.e. user can log in back to the URL which user had requested earlier. Furthermore, several other mechanisms which can enhance the authentication can include biometrics and graphical passwords as proposed by Sae-Bae N, Ahmed K (2012) and Biddle R, Chiasson S (2012) in [13] and [14] respectively.

3. Methodology

3.1. Information Security

The term information security implies keeping the information safe from unauthorized access and protection from any data breach [15].

Table Error! No text of specified style in document.**:** Contents of Information Security

Information security					
Confidentiality	Integrity	Availability	Authentication	Authorization	Non-Repudiation
Problem					
Network Monitoring	Modification of data	Malware attack	Masquerade	Unauthorized Read	Denying
Traffic analysis	Message Fabrication	DoS attack	Impersonate	Unauthorized write/update	False information
Man-in-the-Middle attack	False data injection	DDoS attack	Fraud	Unauthorized delete	Fabrication
Solution					
RSA	SHA	Disaster recovery plan	Biometric/ User Validity	Digital Signature	Digital Certificate
Triple-DES	MD5	Backup	CHAP-PAP	Resource Access Permission	Trusted third party
AES	DSA	RAID	Kerberos	Digital Watermarking	Public Key infrastructure

3.1.1 Confidentiality

Data confidentiality is shielding the valuable data from the information leakage to unknown sources or attackers. Information breach may include confidential data exchange of any organization, corporate, financial institution (that may involve bank account details, credit card statements, personal health record, any government identification etc.) Encryption is a strategy utilized for ensuring data safety from any unauthorized access. User can upload data on cloud

a) Without encrypting data by trusting cloud service provider
b) By encrypting all the data before sending
c) By providing a set of security parameters like access list to third party or cloud service provider.

3.1.2 Integrity

Data integrity is like putting a checkpoint from any modification by authenticated use. It gives assurance and consistency of data. Data integrity has similarity with Confidentiality of data, just like it adds information such as algorithmic check, quality confirmation, review logs, as opposed to the encryption of complete datasets. Integrity likewise alludes to the reliability of data sources [16]. Most of the banking transaction corporate confidential data integrity is a must component. Mirroring and checksum are the most commonly used data Integrity Techniques. Integrity check is practically beneficial for validity of trusted networks, in intrusion detection and prevention system and self validation using certificates [17]. It enhances the performance of system by eliminating duplicates and keeping an indexing service.

3.1.3 Availability

Data availability is responsible for access of data which is accessible to the authenticated/intended user when required. In view of system upgrades, power outages or preventing system impedance, hardware failures, high accessibility framework intend to stay accessible at all the circumstance [18]. Counter to the data availability is Denial-of-Service (DOS) attack [19]. Because of the unavailability of important data, due to

a) Physical hazards such as power failure
b) Hardware failures or earthquake, building collapse and flood
c) External or internal attempt to flood junk data.

Backup is useful for ensuring data availability. Backup can be in form of duplicity or network devices or storage media. Storage of data on offsite locations will help to overcome downtime of important services.

3.1.4 Authentication

Authentication refers to validating the user identity who tries to access some data from the server. A security aware organization must put access control specification for a registered user account by its network administrator. Aspect of a person's personal information such as fingerprint scan, iris scan, secret password, physical stored certificates, smart card or token can be associated with user accounts [20]. This information is compared with the database containing the user's personal information for its authenticity and is referenced for future comparisons and modifications. Information that is stored on the server includes for authentication purpose may contains:

a) A secret security question, a good password or some kind of PIN or token.
b) Biometrics, full palm scan, fingerprints, audio scan and iris (eye) scans.
c) A smart card, NFC enabled card, a secure barcode or some personal identity card.

Working of Authentication

Theoretically, authentication is relatively simple: Credentials like - digital certificate, a password, smart card, fingerprint provided by the user helps to identify whether the person trying to access the system is authorized or not. This can be accomplished using multiple methods and protocols. The basic process to authenticate remains the same regardless of the method or protocol used.

Multi-layered Authentication

In a highly secure environment the system is made more secure using multi-layered authentication which adds up extra protection. In simple words more than one type of credential is provided by the user in order to gain access to the system, e.g. user may require to provide fingerprint as well as login password. In this type of approach chances of unauthorized access are further decreased in case where primary goal is to authorize the user who wants to get more secure access to a system.

Authentication Methods and Protocols

Selection of the appropriate authentication method from a huge number of authentication methods and protocols depends on the security and application requirements. The commonly used authentication methods and protocols are Kerberos, CHAP and MS-CHAP, SSL, Microsoft NTLM, EAP, RADIUS, PAP and SPAP, Certificate services etc.

Kerberos: It is an authentication protocol use to provide client/server authentication using secret key cryptography that works on the basis of tickets to allow host communicating over an unprotected network to validate their identity to one another in a secure manner [21]. Temporary certificates (tickets) containing the information which help the servers to identify user on the network. The data contained in the tickets is encrypted including user's password in the latest Kerberos v5. The network server runs a service known as Key Distribution Centre which authorize user by its username and password and it issue tickets known as Ticket Granting Ticket (TGT) to the clients which authenticates a particular service to user for which the user is subscribed using Ticket Granting Service (TGS). Clients access TGS using TGT.

Secure Sockets Layer (SSL): Another Internet standard which uses combination of public and secret key technology to provide secure communication between user's browser and web server. SSL ensures that data transmitted between browser and web server remain encrypted so symmetric encryption or asymmetric encryption is used. Symmetric private key encryption is faster as compared to asymmetric public key encryption but asymmetric provides more security. Most of the web server software, like IIS and Apache supports SSL [22].

Microsoft NTLM (NT LAN Manager): Windows Challenge/Response (NTLM) is the authentication protocol for window operating system or stand-alone system for authenticating client on network. Client's authentication to an NT domain is done using NTLM authentication by Windows NT servers. NTLM credentials are based on data obtained when a user tries to login to a system and consist of a domain name, a user identity, and a generated one-way hash of the user password. NTLM uses an encrypted challenge/response protocol to validate a user without sending the user's password between client and server [23].

PAP: It is used for used for remote access security. Password Authentication Protocol (PAP) is a password-based authentication protocol to validate users. Pre shared password is exchanged between two intermediate devices for authentication. All network operating system with access to remote servers support PAP. The passwords are sent in plain text to the authenticating server across the network so it is considered weaker protocol compared to CHAP or EAP [24].

SPAP: It improves the PAP in terms of security by encrypting password instead of sending password in clear text by Shiva remote access servers. User name and encrypted password is sent by the client. The encrypted password is decrypted by the remote server. The credentials are matched with the server's database, if they match an acknowledgement message is sent by the remote access server and communication is allowed [25].

CHAP and MS-CHAP: CHAP is also used for remote access security with an enhancement over PAP and uses MD5 for hashing. It is a one-way encryption technique where hash operation is performed on the password. The resultant hashed value is transmitted over the remote network instead of the sending encrypted password. MS-CHAP created by Microsoft for similar purpose for supporting its operating system. [26].

EAP: Point-to-Point Protocol (PPP) and wireless network connection is authenticated using EAP. It provides some basic functions and handshaking of authentication methods called EAP methods. These EAP methods are vendor specific. An example of such methods is mutual authentication between client and server for exchanging information is provided using EAP-TLS (EAP used with TLS) or EAP-MD5 [27].

RADIUS: Dial-up or VPN users are often authorized and authenticated by Internet service providers (ISPs) using RADIUS. Authentication of dial-up clients to the network is done using a RADIUS server which receives connection information and user credentials from dial-up clients. Accounting services can also be performed by RADIUS and EAP messages can also be authenticated by passing them to a RADIUS server. It allows the use of PAP, CHAP, MS-CHAP as well as EAP and implements the RADIUS standards [28].

Digital Certificate Services: Digital Certificates are issued by Certification Authorities (CA). A CA fulfil the role of the Trusted Third Party by approving certificate applications from user, authenticating installed applications, issuing certificates and maintaining validity information about the issued certificates. The data used for authentication and encrypting communications, especially on unsecured networks like http communication are contained in digital certificates. Public Key Infrastructure (PKI) maintains the certificate services information. X.509 specification is the standard for the certificate service.

3.1.5 Authorization

Authentication and authorization both have different meanings, and need not be confused as same. User's identity is verified using authentication while the appropriate rights and permissions in order access requested resource verified using authorization. Both of them work together. First the user requesting to access a resource is authenticated and then the user is authorized to check if he has the rights to access the resource or not. For example for a publicly shared resource no authentication or authorization are required but patient's saved on a hospital computer server need proper authentication and authorization [29]. In many examples, the user's authentication and privileges are determined with username and its associated password. This provides basic authentication but if combination of biometric check like iris scan, fingerprinting, palm scan, face scan, smart card and password combination or combination of password with PIN enhances the authentication process. These combinations can be matched with database containing the user's credential is referenced for future authentication.

3.1.6 Non-repudiation

Non-repudiation gives assurance that someone cannot deny the validity of information and gives proof of the originating source and its data integrity. Digital signatures is the mechanism which can offer non-repudiation and widely used in online transactions, where there is an insurance that a person to whom you are going to communicate in your contract or a communication can't deny about the exchanged information.

4. Current trends

Multi-factor Authentication

Multi-factor authentication is exceptionally effective in providing high security to the online internet user accounts. Basic validation techniques which are legacy i.e. by asking username and password, secret information, PIN, etc. is no more asked from the user. These security mechanisms can request for more of such specific pieces of information which are randomly generated can be asked from the client. This information can be a token in the form of OTP or some secret question asked by the server when a user tries to access online service or accessing stored user data. This procedure is similar to biometric mechanism which needs some unique distinguishable proofs of identity like iris scan or fingerprint scan. The two-step authentication incorporates secret key and additional password or user identity.
In a report Google has said that only less than 10 per cent of active Gmail users are using two-factor authentication. That means almost remaining 90 per cent of the user are vulnerable to cyber attacks.

Table 2: A typical multi factor authentication system

A	Combination of A & B	B	Combination of B & C	C
Fingerprint	Two Factor authentication	Password	Three Factor authentication	Smartcard
Face		Pin		USB Token
Iris		Security question		RFID Badge

6. Weaknesses and limitations

In each type of information security techniques there are certain limitation. Most confidentiality related encryption algorithms are weak or resource intensive. Increasing the security may leads to more energy consumption. Mobility is an important requirement and from the mobility aspects we cannot put security and mobility together i.e. more the complex system more the battery drainage. Internal security system of device such as various sensors of mobile devices like fingerprint, iris systems etc. can be used.

7. Conclusion

Several security aspects of network is analyzed and concluded that in today's world, the multi-factor authentication system are safer way for using internet application. Since the network is vulnerable to scanning so it can be improved by using secure communication like SSL or TLS connection between server and client application. If the user authentication is done through two-factor and three-factor authentication and the network is shared using secure connection the communication is never exposed. This type of system can be compared to a standalone system having its offline passwords without having its dependency on the network. SMS based OTP incorporated security is also very common these days. Some mechanism can be generated to develop offline key generation

techniques so that client does not need to ask every time to authenticate server.

The communication must be done through a secure channel and data must be encrypted. Need of authentication is required with 2FA or 3FA which can be done for all the internet enabled platform using SMS based OTP where the server will send an SMS to the phone after successful login just to verify the user. In case the user lost his/her phone two alternate phone number or email can be provided during registration to the server. Use of biometric like iris, face, fingerprinting can also be used in such case for secure authentication. At last, for secure authenticated communication, user awareness about the security approach is most important aspect of how people are accessing internet.

References

[1] Das A, Bonneau J, Caesar M, Borisov N, Wang X. The Tangled Web of Password Reuse. In NDSS 2014 Feb 27 (Vol. 14, pp. 23-26).

[2] De Carnavalet XD, Mannan M. From Very Weak to Very Strong: Analyzing Password-Strength Meters. In NDSS 2014 Feb (Vol. 14, pp. 23-26).

[3] Grosse E, Upadhyay M. Authentication at scale. IEEE Security & Privacy. 2013 Jan;11(1):15-22.

[4] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation computer systems. 2012 Mar 1;28(3):583-92.

[5] Birman KP, van Renesse R, editors. Reliable distributed computing with the Isis toolkit. Los Alamitos: IEEE Computer society press; 1994 Mar.

[6] Carlin S, Curran K. Cloud computing security. In Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments 2013 (pp. 12-17). IGI Global.

[7] Perlman R, Kaufman C, Speciner M. Network security: private communication in a public world. Pearson Education India; 2016.

[8] https://www.google.com/landing/2step/index.html

[9] Aloul F, Zahidi S, El-Hajj W. Two factor authentication using mobile phones. In Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on 2009 May 10 (pp. 641-644). IEEE.

[10] Sun H, Sun K, Wang Y, Jing J. Trustotp: Transforming smartphones into secure one-time password tokens. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security 2015 Oct 12 (pp. 976-988). ACM.

[11] Hsieh WB, Leu JS. Design of a time and location based One-Time Password authentication scheme. In Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International 2011 Jul 4 (pp. 201-206). IEEE.

[12] Abdurrahman UA, Kaiiali M, Muhammad J. A new mobile-based multi-factor authentication scheme using pre-shared number, GPS location and time stamp. In Electronics, Computer and Computation (ICECCO), 2013 International Conference on 2013 Nov 7 (pp. 293-296). IEEE.

[13] Sae-Bae N, Ahmed K, Isbister K, Memon N. Biometric-rich gestures: a novel approach to authentication on multi-touch devices. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2012 May 5 (pp. 977-986). ACM.

[14] Biddle R, Chiasson S, Van Oorschot PC. Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR). 2012 Aug 1;44(4):19.

[15] Alsmadi I, Burdwell R, Aleroud A, Wahbeh A, Al-Qudah MA, Al-Omari A. Introduction to Information Security. In Practical Information Security 2018 (pp. 1-16). Springer, Cham.

[16] Chen D, Zhao H. Data security and privacy protection issues in cloud computing. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on 2012 Mar 23 (Vol. 1, pp. 647-651). IEEE.

[17] Zhao X, Chen G, Xing H, inventors; Trend Micro Inc, assignee. Portable secured computing environment for performing online confidential transactions in untrusted computers. United States patent US 8,024,790. 2011 Sep 20.

[18] Daswani N, Garcia-Molina H, Yang B. Open problems in data-sharing peer-to-peer systems. In International conference on database theory 2003 Jan 8 (pp. 1-15). Springer, Berlin, Heidelberg.

[19] Senie D, Ferguson P. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. Network. 1998 Jan.

[20] Black GR, inventor; Pen One Inc, assignee. Security authentication method and system. United States patent US 7,363,505. 2008 Apr 22.

[21] Miller SP, Neuman BC, Schiller JI, Saltzer JH. Kerberos authentication and authorization system. InIn Project Athena Technical Plan 1987.

[22] Bhiogade MS. Secure socket layer. In Computer Science and Information Technology Education Conference 2002 Jun (pp. 85-90).

[23] Jaganathan K, Zhu L, Brezak J. SPNEGO-based kerberos and NTLM HTTP authentication in microsoft windows. 2006.

[24] Lloyd, Brian, and William Simpson. "PPP authentication protocols." (1992).

[25] Lantto J, Ensuque G, inventors; Alice Systems AB, assignee. Method and arrangement to secure access to a communications network. United States patent US 7,152,160. 2006 Dec 19.

[26] Simpson, William Allen. "PPP challenge handshake authentication protocol (CHAP)." (1996).

[27] Blunk, Larry J. "PPP extensible authentication protocol (EAP)." (1998).

[28] Rigney C, Willens S, Rubens A, Simpson W. Remote authentication dial in user service (RADIUS). 2000.

[29] Mohammadi M, Larijani B, Razavi SH, Fotouhi A, Ghaderi A, Madani SJ, Shafiee MN. Do patients know that physicians should be confidential? A study on patients' awareness of privacy and confidentiality. Journal of Medical Ethics and History of Medicine. 2018;11.