Information Security: Issues, Processes, and Challenges

Balsam A.J. Mustafa **Loai Alamro, Enas Al Zaidi**

Department of Computer Science

Al Turath University College, Baghdad, Iraq

Abstract

With the increasing use of the internet which is a global network, Information security is a substantial issue in today's business. Information security has become one of the most important aspects of modern electronic society. Security of information, networks, and systems is vital to make information systems work satisfactory and enable people to safely get the information they need. Security is the practice of defending information from unauthorized access. This paper discusses the basic characteristics of secure information and the important processes that used by administrators to protect data and systems.

Keywords: Security attributes, Authentication, Authorization, User identity, Access control

1. Introduction

In today's life, it is well known that the internet which is a global network that connects millions of computers around the world providing communication between them and easy access to information via the internet from anywhere comes with risks. Among the important risks are that information may be deviated, stolen, or misused. Whenever there is unauthorized access to a system or network to make a harmful effect on that system data, it is regarded as cyber security. The Committee on National Security Systems (CNSS) in the U.S. defines information security as the "protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information" [1]. It is common sense that as technology advances, these advancements are done by humans and again the harm will be caused by humans. Among the important information that needs to be kept secure for people and organizations are personal information, the company's financial results, confidential business plans for years ahead, trade secrets, research, and other information that gives the company a competitive edge [2]. Computer security gaps may give attackers the ability to access computer systems without the person's or organization's awareness through different ways, e.g. hacking, viruses, worms, denial of services, spaying, mobile malware, etc. causing severe damage to the systems leading them to not working properly and denying the service for legal users [2].

2. Essential Security Attributes

The fundamental security concepts related to information on the internet are confidentiality, integrity, and availability. The concepts related to users of the information are authentication, authorization, and nonrepudiation. These security attributes constitute the main requirements for secure communication and security management [4].

Confidentiality:

When someone not authorized is able to read or make a copy of information from a system, this makes a loss of confidentiality. This includes medical and patients information, personal bank details and credit card information, information of intellectual property, invention and patent, Exam results, individuals or agencies that offer services such as psychological counseling or drug treatment, contact details of staff, customers, pupils, etc. Confidentiality is important because it builds trust and respect in the workplace, prevents misuse of information, and protects reputation of people and organizations [3].

Integrity:

It can be defined as the property that data has not been altered in an unauthorized manner [5]. Information can be perverse when it is available on an insecure network. When information is altered in unexpected ways, the result is known as loss of integrity. This means that changes by unauthorized parties are made to information. Integrity is generally impacted by hardware and software errors, human errors and intrusions [6]. Access authorization is an important issue to maintain information security. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting.

Availability:

As defined by [7], availability is the "timely, reliable access to data and information services for authorized users". Denial of service (DoS) attack is one of the threats to information security, the main target of DoS attacks is making an information resource unavailable for the user [8]. Whereas the attribute "availability" means that authorized users are enable to access information and related resources when they need it. [9] argued that information availability depends upon several components such as system software, hardware, and network. Dependence on network is important as users who cannot access the network or specific services provided on the network will be exposed to "denial of service". Availability is of significant importance in service-oriented businesses that depend on information such as (airline schedules and online inventory systems) [9].

To allow users to access information they need to use, the permission should be given to whom can be trusted with it, therefore, organizations use authentication and authorization.

3. Authentication and Authorization

Authentication and authorization are two vital information security processes that administrators use to protect systems and information. Authentication is defined as "the process that enables recognition of a user described to an automated data processing system" [10]. This means that a user presenting himself to a computer system by using certain information like a user name and password, i.e. the authentication is done based on information that the user knows to log into a system. The provided identity is verified by the system and permits the user to access it. However, the research of [10] pointed out different problems of this authentication method, one of them is that passwords are hard to remember especially when they are long and random, and become harder if users need to remember a different passwords for each service provided by a system, in case that the systems provides many services. To mitigate this problem, one way is suggested by using single sign-on on the network that allows users to sign on once to a system during the session, even if they are using different services of the system[10].

Other methods for providing identity in the computer security context exploit biometric properties of the user. If the properties are unique for each person, it can be used to authenticate the user. For Example, fingerprint, face recognition, and voice recognition. Although fingerprint automation technology is used widely in biometric-based authentication systems in terms of convenience and low error rates, research [11] explained that there are several challenges related to this method, one of the most important is the quality of the fingerprint image which strongly affects the overall system performance. Capturing a precise digital image of fingerprint without distortion or partial image with low quality still needs more research to ensure that the system will perform properly.

Authorization, simply defined as the access right to a network services and applications. It is the second step after authentication, after user is authenticated, authorization allows user to access different levels of information and perform functions based on regulations and access policy for specific types of users. Authorization is the process of verifying what files, data, and applications that user is allowed to access [12]. Specifically, users access should be limited to those who have the right to do so. For example, a person working in the financial department in an organization should not have access to personnel data and records.

Authorization restricts access to a secured component depending on a user's access privileges, i.e. can't access the files or information that their role in the organization does not permit. According to [13], there are different models for the specification of the access rights, i.e. the components needed and their interactions. An authorization model is described by three main components, (Subject) is the active entity (e.g. user, group, organizational role) that requests access, (Object) is the entity of the system, that needs protection (e.g. a file, a database table or record), (Action) determines what the subject can perform on the object (e.g. access right, type of activity).

Both, authentication and authorization, are security processes that prevent unwanted access to a secured system.

3.1 How Authentication Works

The main goal of authentication is to prove the identity of the user through authentication methods such as a username and password, biometric information such as facial recognition or fingerprint scans, and phone or text confirmations [14]. For identity authentication with a login and password (the most common form of authentication), the process is done by:

1. The user creates a username and password to log in to the account they want to access. Those logins are then saved on the server.
2. When that user starts to log in by entering his unique username and password the server checks those credentials against the ones saved in its database. If they match, the user can access to the system.

3.2 Types of Authentication

1- Single-Factor Authentication

Single-factor authentication (SFA) or one-factor authentication uses a username and a password to gain access to a system. Although this is the most common and well-known form of authentication, it is considered of low-security [14]. The main weakness is that single-factor authentication provides just one barrier. Intruders need only to steal the credentials to gain access to the system. Also, reusing the password practice, admin password sharing, and using a weak passwords make it much easier for hackers to guess or obtain them [15].

2- Two-Factor Authentication

Two-factor authentication (2FA) adds a second layer of protection to user's ability to access a system or network. Instead of just one authentication factor, 2FA requires two factors of authentication out of the three categories:

- Something you know (i.e., username and password)
- Something you have (e.g., a smart card)
- Something you are (e.g., biometric credentials)

The two- factor authentication means that in addition to provide a user name and password as a first layer of protection, it is necessary to add a factor from the other two categories as a second layer of protection [15].

3- Three-Factor Authentication

Three-factor authentication (3FA) demands confirming the identity credentials from three separate authentication factors (i.e., one from something you know, one from something you have, and one from something you are) [15].

4. Emerging Authentication Trends

It is obvious that security threats increase and become more complex with the increasing cyber crimes and malicious attacks. Authentication methods need to continually evolve to provide higher protection against harmful attacks. It is expected to see more and more advanced authentication protocols to ensure secure access across industries. One of the biggest trends will be in improving and expanding biometric authentication capabilities [3]. This is especially important as "Statista" [16] (the statistics portal for market data) reports that the global biometric system market is expected to explode in the coming years, reaching a size of $83 billion by 2027.

Another key area of growth will be in adaptive authentication. This next generation of Multi factor authentication (MFA) relies on artificial intelligence (AI) and machine learning to identify additional user information such as location, time, and device to observe the login attempt and lock any suspicious access behavior [12]. Moreover, AI has been utmost importance in building automated security systems and enabled threat detection systems to predict new attacks and notify admins for any data breach instantly.

5. Conclusion

With the Digital transformation around all businesses, small or large, corporates, organizations and even governments are more relying on computerized systems to manage their day-to-day activities. Cyber security has become essential in today's society and has become a primary goal to protect data from various online attacks or any unauthorized access. This paper discussed the main characteristics of secure information and the processes of authentication and authorization which are of great value and play a substantial role in protecting data and networks from harmful attacks, and prevent unwanted access to a secured system.

References

[1] National Security Telecommunications and Information Systems Security (1994). National Training Standard for Information Systems Security (Infosec) Professionals. File 4011

[2] The Importance of Information Security, https://pecb.com/article/the-importance-of-information-security-nowadays accessed on 14/02/2023

[3] Dutta,N. , Jadav, N. , Tanwar, S., (2022). Cyber Security: Issues and Current Trends, Springer publisher
[4] Siponen, M. T., Kukkonen, H., (2007). A review of information security issues and respective research, The DATA BASE for Advances in Information Systems, 38(1)
[5] Nieles, M., Dempsey, K., Pillitteri, V., (2017). An Introduction to Information Security, NIST Special Publication 800-12 Revision1
[6] Talha, M., Abou El Kalam, A., Elmarzouqi, N., (2019). Big Data: Trade-off between Data Quality and Data Security. The 9th International Symposium on Frontiers in Ambient and Mobile Systems (FAMS2019), Leuven, Belgium
[7] Martin, A., Khazanchi, D., (2006). Information Availability and Security Policy, Proceedings of the 12th Americas Conference on Information Systems, Mexico, 2006
[8] Whitman, M.E. (2003). Enemy at the Gate: Threats to Information Security, Communications of the ACM, 46, 91-95
[9] Qadir, S. and Quadri, S.M.K, (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. Journal of Information Security, 7, 185-194
[10] Alenius, F., (2010). Authentication and Authorization, Achieving Single Sign-on in an Erlang Environment, UPSALA UNIVERITET, Independent thesis Basic level
[11] Uliyan, Diaa M., Sadeghi, S., Jalab, H., (2020). Anti-spoofing method for fingerprint recognition using patch based deep learning machine. Journal of Engineering Science and Technology, 23(2), 264-273
[12] Kizza, J.M. (2020), Access control and authorization. Kizza, J.M. (Ed), Guide to Computer Network Security Texts in Computer Science, Springer Publishing, pp. 187-206, ISBN 978-3-030-38140-0
[13] Mohamed, A.K.Y.S., Auer, D., Hofer, D., Küng, J. (2022), A systematic literature review for authorization and access control: definitions, strategies and models, Journal of Web Information Systems, Vol. 18 No. 2/3, pp. 156-180
[15] Matt, B. (2018), Computer Security: art and Science, Addison-Wesley Professional, ISBN 978-0-13-409714-5.
[16] Statista Report, https://www.statista.com/statistics/1048705/worldwide-biometrics-market-revenue/ accessed on 14/02/2023