Authentication Role and Its Measures on Security Threats

[1]Varsha Jotwani, [2]Dr.Amit Dutta, [3]Dr.Pratima Gautam
[1]Research scholar, [2]Deputy Director, AICTE, New Delhi, [3]Dean of Computer Science and Application, AISECT University
[1]Computer Science and Application,
[1]AISECT University, BHOPAL,INDIA

Abstract : E-commerce is increasing at fast pace same its related applications are increasing at the random manner As its working , transactions and its related expansions making an web based ecommerce concept generating proliferations security threats issues as world is moving towards in making of digitalized business several threatening issues are at a very high levels of vulnerability in the arrangements which result into cyber-attacks. As online activities are increasing at a fast pace, In Internet based environment two servers authentication procedure considered to be secure for authenticating user and the success rate of two server is much better comparatively to single server.

***IndexTerms* –E-commerce,Threats,Authentication**

I. Introduction

Electronic commerce or E-commerce is currently one of the most significant aspects of the Internet to emerge. It covers a range of different types of businesses, from consumer based retail sites, through auction or music sites, to business exchanges trading goods and services between corporations. E-commerce allows consumers to electronically transfer goods and services with no restrictions of time or distance. Electronic commerce has broadened expeditiously over few years and is envisioned to continue at the fast rate. In the near future the difference between "conventional" and "electronic" commerce will become increasingly widen, more and more businesses moving towards their operations onto the Internet. As E-commerce is increasing at fast pace same its related applications are increasing at the random manner, some of the commonly used applications are: - Online shopping, Online marketing, Online payment, net banking, digital distribution etc.As there are numbers of threats which affect our ecommerce transaction which hamper our security some are intentionally and some are accidental. Various types of threat issues which are affecting our working in our business terms they are as follows:-

II Threats Issues

Irrelevant management- When ecommerce security is not meeting the expectations of management it poses as very fatal threat to the network and systems. Sometimes, the organization is not having the sufficient budget for purchasing licence antivirus software to prevent from harmful security threats which leads a organization into higher risk zone for them.

- **Spam mail –** Every user who having their mail account now days facing Spam mail problem, unlike a regular spam message it is not sent from a single user but it is sent by so many users ,so sometime it is difficult to manage these spam message by anti spam software
- **Malicious Code Threats-**Viruses are also biggest issue of an ecommerce websites, they attack this website and affect the whole working of business operation, and they do come from various external sources.
- **Destruction of Data-**Data Destruction is one way of harming and stealing the confidential data and there are so many reason in which our data is destructed due to negligence by someone working in the company, sometime accidental cause is also the reason for hampering of data ,so remedial action is done by securing our data by taking a proper backup in case it is lost so that it can easily be recovered, yet proper security is required to handle this kind of situation .
- **Spyware-**Spyware is software that is used to collect information from a computer and transmit it to another computer .The information which spyware exports to the another system could be same type as done by viruses, but the essential difference is that spyware do not replicate .Spyware often get downloaded when we are viewing some webpage, the phenomenon being called drive by download.
- **Executable file Infectors-**A file infector is a virus which infects files which the operating system considers to be executables are the common targets of these viruses .The viruses can be placed at the beginning, end, over-written or inserted into a file. Viruses which place its code at the beginning of loaded file. Thus the virus gets control first when the infected file is run.
- **Phishing Attacks-**Phishing is a type of fraud in which malicious emails with their links sent by the attackers so that they can retrieve login credential or some other confidential information of the user. Phishing attacks are totally based on social networking techniques applied by email and Phishers try to trace out the activities of the users interest and pattern and according to that it flow malicious information.

III PRINCIPLES OF SECURITY

Principles of security helps to find out the attack better and also help us in thinking about the possible result to tackle them. There are four prominent principles of security they are as follows:

- Confidentiality: The principle of confidentiality mention that only the sender and the intended recipient(s) should be able to access the gist of message .Confidentiality gets break if an unauthorized person is able to access a message. Interception causes damage of message confidentiality.
- Authentication: Authentication process helps to create the identity proof which ensures the source of electronic message is correct or false one.
- Integrity: When there is modification of the contents of message after the sender sends it, but before it reaches the intended recipient that means the integrity of the message is lost. Modification leads to deprivation of message integrity.
- Non-repudiation: Number of times when a user sends a message at certain time, and later on refuses that certain message had been sent by them. Non-repudiation does not allow the sender of a message to refute the claim of not sending that message.

IV BASIC CONCEPT OF PASSWORD BASED SCHEME

Password based verification is done by almost every organization, it is one of the most simplest method through which user identity is verified and it is totally believe in verification of server too where keywords and its resultant password are stored in database. Classical technique for password based confirmation to undertake a single server which provides all the proofs which are required to confirm a user authenticity. The computation involved for single server system operation and maintenance user's password and their related verification and validation is non complex one but it also feasible for attacker to make a successful of offline dictionary attempts and made speculation easy of passwords which sometime leads to the exposure of security .To overcome from these problems there are various techniques proposed which are as follows:

V TWO SERVERS PASSWORD AUTHENTICATION

In Internet based environment two servers authentication procedure considered to be secure for authenticating user. As online activities are increasing at a fast pace, various proposal are coming forward to make our security feature more stronger ,most of the password based verification is done at a single server system and according to request server responds to users. Single server are more prone to attacks and sometime its difficult to remember user identification along with passwords. In two server authentication system role of key is introduced in which user has to identify its secret key and password exchange is done by secret key that is secure from offline dictionary or other related attacks.

The notion of a user identification name and password is a charge actual and well-organized technique. Recognizing and permitting the sanctioned operator to admittance the possessions is unique of the important characteristics of confirmation organization. A solitary waitron organization is an organization in which the watchword will be kept in alone waitron as revealed in Figure.1 Though seeing the confirmation organization grounded on a solitary waitron, nearby are approximately problems. The solitary waitron organization is susceptible to all categories of bouts from interlopers. The impostor can drudge the organization by tiresome all conceivable explanations till the organization gets cooperated the maximum positive in the unsociable waitperson arrangement, and thorough exploration also can be positive as publicized in Figure.2.

USER
Password
SERVER

FIGURE 1: SINGLE SERVER SYSTEM BLOCK DIAGRAM.

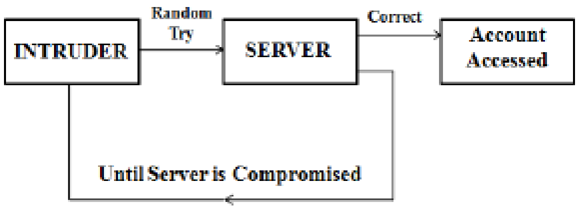

FIGURE 2: SINGLE SERVER SYSTEM HACKED BY INTRUDER EXAMPLE

Consequently, it is essential to familiarize the notion of two waitron confirmation organization. In the circumstance of a solitary waitron organization, the attacker can execute negotiation effortlessly. Nevertheless, in the two waitron organization, it would not be simply bargained by the aggressor. Below is Figure 3

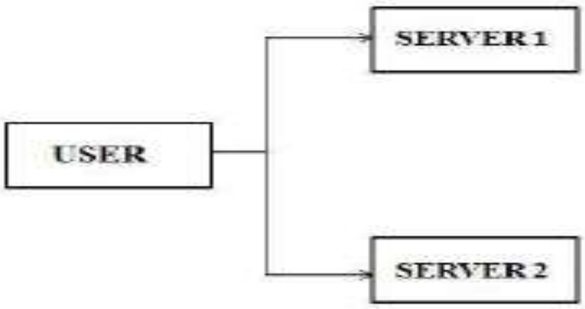

FIGURE 3: TWO SERVER SYSTEM BLOCK DIAGRAM

In a two server system , the hash included pseudo-random password has been divided into two parts. The segmented portions are kept in the two servers to conceal the accessibility of password attacker. Even if one segment is being revealed, the whole watchword will not be under the danger of expose. The one segment of the breach watchword is stored in the frontend server also called as service server. The end users usually interact with the service server for retrieving the data. The other broken watchword is stowed in back end server also named as Control Server. The user watchword authentication is operated by the union of two split watchwords between the front and back end servers. Hence in public internet applications the two server model maintains high security of the user password.

VI PRIVACY PRESERVING AND ITS TYPES

Today the data storage requirements are becoming large, as a large number of data is evolving day by day. As the large database is required to store a large amount of data, so the privacy of the data is also an important factor. Maintaining privacy needs to develop protocols that do not disclose any confidential information parties. As there are many challenges technically wise it is quite tough job to segregate the confidential data from public based data. Mutual authentication is a concept in cryptography in which one party proves it credibility to another party. [1], [2], [3] helps to achieve the aim of data mining by preserving the privacy of sensitive data By, maintaining privacy unauthorized access and revelation of data would be saved .

According to today’s world scenerio, there is a need for different trust levels. We had different user groups and different access needs, and hence the motivation for exploring different levels of trust. For example, a government organization may have an internal and external group of data access users. Moreover, it also wants to provide data to the public. So, it will have to keep more copies of data based on different trust or access levels. However, there may be an issue with this approach as well. When the users get copies of the data, they can also get also get the identity information from the data. Therefore, it is very challenging to implement multiple level trust based PPDM(Privacy Preserving Data Mining). To avoid this problem before giving data to data miner, it is perturbed in such a way that sensitive information is encoded or altered to guarantee that the discretion of information is conserved. There were many types of research on the PPDM [4], [5-6], when compared to single level trust scenario, many perturbed copies are required by the data owner to ensure non-disclosure of sensitive details. The number of perturbed copies and redundancy depends on the trust level of the data miner. However, from multiple diverse and perturbed copies, the miner might produce original information accurately. This is the problem with the approach, Preventing such diversity attacks is a challenging task in multi-level trust based PPDM.

VII PERFORMANCE OF TWO FACTOR AUTHENTICATION

Two factor authentication concept controls a privacy of control server information against both inside and outside attackers. The user’s computation overhead as it is produced by the two factors password authentication system is comparatively low to that of the single server classical password system. On a single concept of vulnerability, users manage service provider to manage security of watchword. The proposed two factor password substantiation model represent it potential in it computation and communication operations to all users’ website with single password. For each user the communication overhead is particularly low in terms of both bits and rounds which is being conducted between the two servers. To identify the success rate of two factor authentication is represented by testing multiple instances.

Single and two factor success Access	Single factor Substantiation Success Rate (%)	Two factor Substantiation Success Rate (%)
1	82	88
2	80	90
3	87	82
4	81	85

The success rate of two factor authentication ranges from 82% to 96% which is more successful comparatively to single factor authentication.

VIII CONCLUSION

Two-Factor substantiation system is one in which the amalgamation of two different techniques are needed (such as a smart-card, PIN or a biometric and a watchword) to verify a user. Using two factors provides strong authentication features. To achieve the sturdy security features any two or more of the following factors are to be combined:

- *Something you experience:* The authenticity is checked based on what the user experiences. The observations includes all kinds of secrets which the users can easily remember such as PIN, watchword, Passcode etc.Password based authentication systems based on the technique of something you experience.
- *Something you possess: Users* authenticity is checked based on what you acquire. This includes users having extra devices the user possess such as crypto tokens, smart-cards, watchword generating tokens or any USB enabled devices etc.It generally needed an extra substantiation feature in the form of PIN or password.

IX REFERENCES

[1]O. Goldreich. "**Foundations of Cryptography", Volume 2**. Cambridge University Press, 2004

[2] J. Yedidia, W. Freeman, and Y. Weiss. **"Understanding belief propagation and its generalizations, In Exploring Artificial Intelligence in the New Millennium**". Morgan Kaufmann, 2003.

[3] Chen, C.L., Lu, M.S., Guo, Z.M.: **"A non-repudiated and traceable authorization system based on electronic health insurance cards"**, Journal of Medical Systems pp. 1–12, doi: 10.1007/s10916-011-9703-4, 2011

[4] Chen, Y.L., Chou, J.S., Huang, C.H.: **"Improvements on two password-based authentication protocols."** Cryptology ePrint Archive, Report 2009/561, http://eprint.iacr.org/2009/561.pdf, 2009.

[5] Khan, M., Kim, S., Alghathbar, K.: **"Cryptanalysis and security enhancement of a more efficient & secure dynamic id-based remote user authentication scheme"** Computer Communications 34(3), 305–309, 2011

[6] Pu, Q., **"An improved two-factor authentication protocol".** In: 2010 International Conference on Multimedia and Information Technology (MMIT). vol. 2, pp. 223– 226. Ieee, 2010.