Security of Data in Machine-to-Machine Communication

Nivedita Gupta, Prof. Neeraj Shrivastava

Abstract— Security of data is one of the most important issues in today's high-speed and extremely complex environment. There are several issues occurred in web environment related to data security i.e. bugs in Web pages, wrong data in Web sites, fraud in card payment system and unauthorized updating in e-mail data and other important data in Web application. Web applications are very useful and an important distributed system which is depending on both client-side and server-side mechanisms. Web applications are used to provide end users in which client access the server's functionality with a set of Web pages. Some attacks are identified in Web applications are cross-site scripting, SQL injection, cookie theft, session hiding, browser hijacking, and the self-propagating worms in Web-based email and social networking sites. These are the common vulnerabilities which affect the data security. This is the representation for Machine-to-Machine communication system, tries to makes contributions i.e. to create an environment where data is securely sent from one machine to another machine and can be used to help Security Improvement in Web Engineering.

Index Terms— Web Application Security, TOTP (Time based One Time Password), Machine-to-machine Communication, WSS (Web Service Security).

1 Introduction

Information and Security are the terms which assume an essential part in today's online world i.e. in e-trade, online business, web managing, e-government and so forth. So it is vital to verify that the information which we utilized as a part of system environment is secure. Information is put away in database, database can store enormous measure of information with different sort and capacity limit rely on upon the specific database. For security of database numerous calculations are accessible, however the most critical part is to exchange the information from customer to the server in safely way so that no unapproved client can get to that information. For sending data from sender to the receiver three types of communication are occurred:

1. Server-to-Server Communication
2. Machine-to-Machine Communication
3. Browser-to-Server Communication

Machine-to-Machine Communication system is a one-to-one communication which can we used in wired and wireless systems. It is the broad term used in many important areas like military, personal business, banking system etc. Here we work on Web Application Security, which educate us about the risk, working with internet or web based applications. Web application is the medium by which user can access the internet or online world so that user can do shopping, banking, business, get news etc. For any online work it is essential that the data which is used have to be correct and protected. For the protection of data, commonly we use HTTPs (Hyper Text Transfer Protocol Secure). This is the communication protocol which is used for securely transmission of data between internet browser and web sites. It is also known as SSL (Secure Socket Layer). But it is not sufficient for all attacks and it also a payable protocol [4] [5]. This paper describes the algorithm for securely transfer the information from one machine to another.

2 Problem Identification

2.1 Risk Assessment:

Exhaustive information security starts with a general procedure and danger appraisal. This will empower you to distinguish the dangers you are confronted with and what could happen if significant information is lost through burglary, malware contamination or a framework crash. Other potential dangers you need to recognize incorporate the accompanying:

- Physical dangers, for example, a flame, power blackout, robbery or malevolent harm.
- Human slip, for example, the mixed up handling of data, unintended transfer of information or info mistakes.
- Exploits from corporate reconnaissance and different vindictive movement.

2.2 Problem Domain:

Security is critical in today's rapid world. Data Security requires high accuracy and detection rate in light of the fact that the whole Business world, Banking work, Shopping World relies on upon the exactness of information. Vulnerability can influence any framework; it is the shortcoming of the framework which welcomes the attackers to make changes in the data for his advantage or for the loss of the information proprietor. There are numerous reasons which make issue in information security are as per the following:

1. Probability of hacking because of single layer of encryption:
   Now a day's single layer is insufficient for securing

highly confidential data. So that likelihood of hacking is expanded.

2. No Session Timeout:
   Some method has no session time out means there is unbounded time is accessible for programmer to recognize the mystery key or the key which are going between the customer and the server.

3. Key Length less than 128- bit:
   Key length under 128-bit means it takes less time to hack. So that it is vital that Key length needs to sufficiently solid to secure information.

4. Exception handling:
   Algorithm must take care of Exception Handling. There are numerous probabilities can happen when genuine client has faced the various issues.

5. Encryption method is naive:
   Encryption methods have to be strong enough to secure the data from higher level hacking. Some Terminologies for naive encryption are: Key choices are less, No use of OTP.

6. When any mobile application interacts with each other, it uses same password, which can be found using request logs or network sniffer tools.

7. Portability of code: Code has to be easily ported to other languages so that user can conveniently use it.

8. Data security can process huge amount of data. To secure the personal information from the hackers, we need to maintain the privacy of individuals. Confidentiality, integrity and availability (CIA), it is necessary to preserve it.

3 SOLUTION

In Machine to Machine (M2M) communication system when we transfer data from one to another machine then data security is important for web application. Here we use two main terms- One is TOTP which is Time based One Time Password. TOTP is generated by the server and send to the client. TOTP is different from OTP because it combines the secret key with the current timestamp using a cryptographic hash function. Timestamp is changed in a particular time interval so that after every particular time interval the generated TOTP is changed and data is safe if attacker hack that TOTP. Second is HMAC which is Hashed based Message Authentication Code. HMAC is the algorithm which used for the generation of One Time Password. HMAC algorithm plays a very important role in security of data because HMAC algorithm is a non-reversible algorithm and cannot disclose the original data. In terms of giving the Security in transmission of data following algorithm are proposed:

1. User => Enter (Username, Password)
2. Client (Request) => Server
3. Server (Generated OTP) => Client
4. Client => Encrypt (OTP, Data)
5. Client (Encrypted Request) => Server
6. Server => Decrypt (Encrypted Request)

   IF (Decrypted OTP = Generated OTP)
   Server => Decrypt (Encrypted Data)
   Server (Encrypted Positive Feedback) => Client

   ELSE
   Discard the Request
   And
   Server (Error Message) => Client
7. End Procedure.

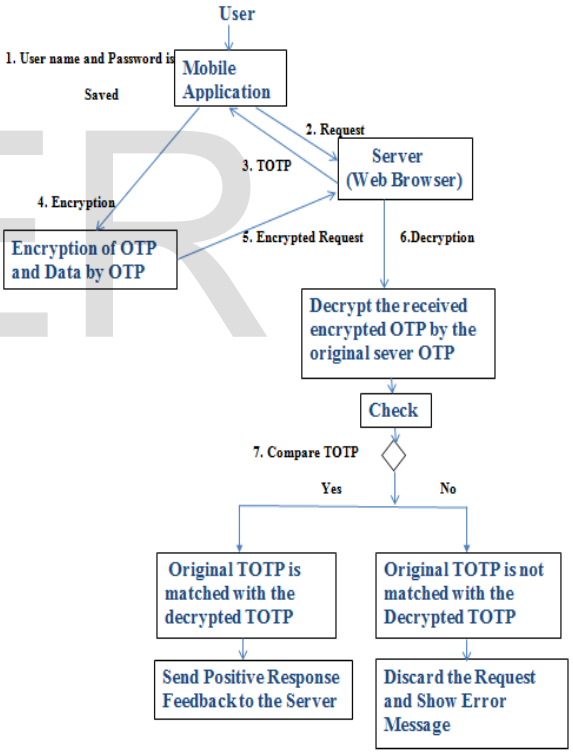

Fig.1 Block Diagram of Proposed Algorithm

The Block Diagram of the proposed algorithm is shows above which describe the steps and procedure of working of Algorithm as follows:

1. In the Mobile application when the user first time log in and enter their Username and Password then the server and the application save that Username and Password.

2. When the client generates a request to the server for sending the data then server generates two TOTP (Time based One Time Password). And send to the client.
   Server generated two TOTP because if the client request is delay by the traffic or poor internet connection or other reason than server have an option to check the request, decrypt by the current TOTP and the previous TOTP. So that true client request will not be rejected.
3. Then client Encrypt the payload (Data) and the TOTP password by the generated TOTP.
4. When server received the request then decrypts the TOTP by the generated TOTP. If the original TOTP is matched with this decrypted TOTP then server gets the positive result means the request is came from the right client and then decrypts the data as well.
5. Then send the Positive Response request to the Client. And if the TOTP is not matched then decrypted it by second generated TOTP, if still it didn't match with original message than discard the request and show error message.

There are many benefit of this algorithm given as follows:

1. It is an open source so that everyone can use it freely.
2. OTP is only valid for 15 second so that less Probability of hacking (can adjust the valid time interval according to need).
3. Sever generates 2 OTP at one time so that if the request is reached to the server after 15 second, because of network or other errors then server use both the OTPs to decrypts the Request. And if the request is come from the right user than server accept it.
4. Username is public means everyone can see it and password is hidden so that no one can see it. No need to travel original password in the network, only OTP travels from one machine to another. So that no probability of hacking the original password in the networking environment.

4 Conclusion

Web application security is a very serious and important area which requires accurate planning and true commitment about data security. Today many applications are available for the security of data but they are not enough to fight with the smart attackers. The biggest challenge is that we need to answer very quickly in the changing environments. As the new technologies are invented, it gets harder to prevent the data from the attacker because with the new level of technologies we required new level of security. The aim of the algorithm is that the systems which have valuable or confidential or private data behind their machine will safely be exchange to another machine at the server side and has strong enough to defend attacks.

References

[1] A. Garg, S. Singh, "A Review on Web Application Security Vulnerabilities", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 1,January 2013.

[2] E. Bertino, R. Sandhu, "Database Security—Concepts, Approaches, and Challenges", Dependable and Secure Computing, IEEE Transactions, 2005.

[3] G. Serme, A. S. D. Oliveira, J. Massiera, Y. Roudier, "Enabling Message Security for RESTful Services", IEEE 19th International Conference on Web Services, 2012.

[4] M. Quasthoff, H. Sack and C. Meinel, "Why HTTPS Is Not Enough – A Signature-Based Architecture for Trusted Content on the Social Web", IEEE/WIC/ACM International Conference on Web Intelligence, 2007.

[5] M. Ghafari, H. Shoja, M. Yosef Amirani, "Detection and Prevention of Data Manipulation From Client Side In Web Applications", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[6] P. Jain, G. Jain, V. Rai, "Identifying the Problem & Solution of False Positive", International Journal of Advanced Computational Engineering and Networking, 2014.

[7] W.B. Glissonand, R. Welland," Web Engineering Security: Essential Elements", Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference, 2007.s

[8] Y.W. Huang, D.T. Lee," Web Application Security—Past, Present, and Future", IEEE National Science Council under the Grants, 2005.

- *Nivedita Gupta is currently pursuing masters of engineering in computer science & engineering in IES-IPS Academy, Indore, India. E-mail: enggniveditagupta@gmai.com*
- *Prof. Neeraj Shrivastava, department of computer science & engineering in IES-IPS Academy, Indore, India. E-mail: neeraj0209@gmail.com*