ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

Multi-Level Secure From the Web Intrusions and Query Attacks on Web Database

Divya.M[1] , S.Jayanthi[2] , K.Jayalakshmi[3], X.Nancy[4]

UG Student, Department of Computer Science and Engineering, Veltech Multitech DR.RR & DR.SR Engineering College, Chennai, India[123]

Asst. Professor, Department of Computer Science and Engineering, Veltech Multitech DR.RR & DR.SR Engineering College, Chennai, India[4]

ABSTRACT: Most information systems and business applications built now-a-days have a web frontend and they need to be universally available to clients, employees and partners around the world, as the digital economy is becoming more and more prevalent in the global economy. These web applications, which can be accessed from anywhere, become so widely exposed that any existing security vulnerability will most probably be uncovered and exploited by hackers. Two of the most widely spread and critical web application vulnerabilities: SQL Injection and XSS. SQLI and XSS allow attackers to access unauthorized data (read, insert, change or delete), gain access to privileged database accounts. . We introduce Trusted DB, an outsourced database prototype that allows clients to execute SQL queries with privacy and under regulatory compliance constraints by leveraging server-hosted, tamper-proof trusted hardware in critical query processing stages, thereby removing any limitations on the type of supported queries.

KEYWORDS: SQL Injection, Function Call, Raw Data, Trusted DB

I. INTRODUCTION

In the field of security, the popularization and application of Internet, communications and computer network technology has been rapid development, especially the emergence of the Internet, makes the computer used in government, business, business, education, health care and other areas of society at an unprecedented rate, which are profound impact on people's economic, work and live. Network brings you convenience while brings more and more malicious attackers. Attackers target the network, database; make the database information security under serious threat. The SQL attack is one of common attacks, the tool of the SQL attack is SQL statements. Attackers towards programming vulnerability of application developers, submit well-constructed SQL statement to the server to achieve the goal of attacking. SQL is a language that is used to query, operate, and administer database systems such as Microsoft SQL Server, Oracle, or MySQL.[1]-[3] The general use of SQL is consistent across all database systems that support it; however, there are intricacies that are particular to each system[7].

The main objective is to keep database in a well secured manner under serious SQL injection attacks and to analyze the principle of SQL attacks, since it is considered to be a serious attack on a database[12]. It provides safety methods to both users as well as administrators. It also avoids the administrators bypassing the user accounts. Various Illegal functions such as deleting records from the database, adding unwanted information to the database, running the innermost function in the database are also can be eradicated using various counter measures that were implemented in project.

II. EXISTING SYSTEM

As network security practitioners put more resources and effort in to defending against SQL INJECTION ATTACKS, attacks, hackers will develop and deploy the next generation of SQLIA (SQL Injection Attacks) bonnets with different control architecture.[5],[10] A SQL injection attack is an attack that is aimed at subverting the original intent of the

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

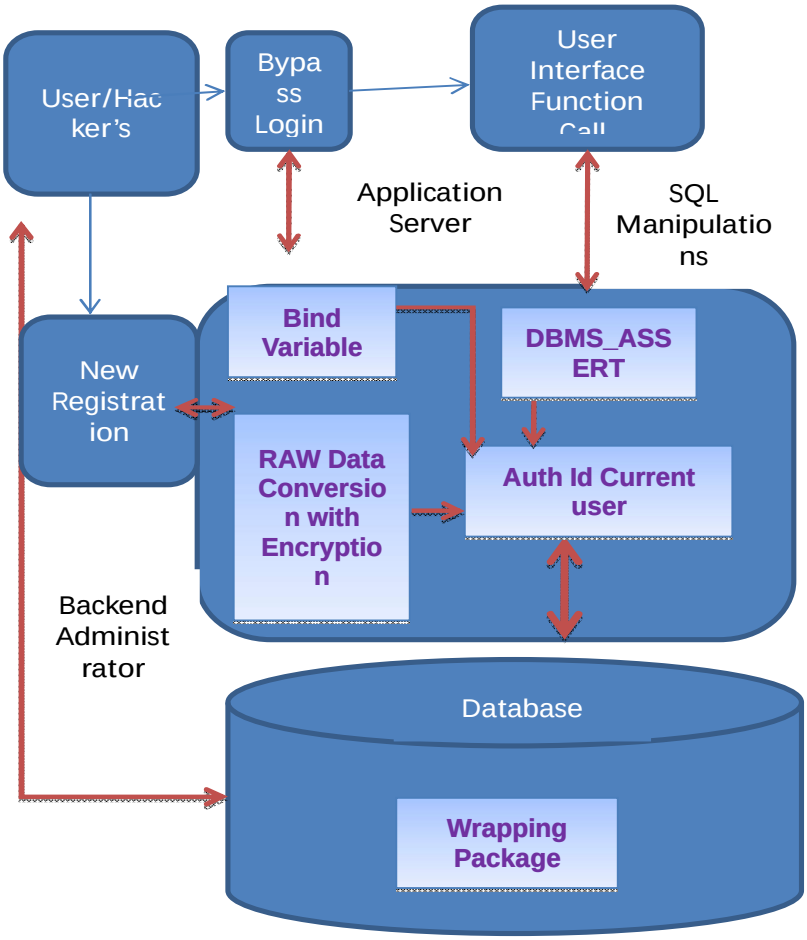
Vol. 5, Issue 3, March 2016

application by submitting attacker-supplied SQL statements directly to the backend database. Through this a hacker can easily enter into a user account and access their own information[14]. It can easily execute oracle function or custom function from the select statement. If a DBA knows the user password, he can easily access user account without user permission. Traditionally, as soon as confidentiality becomes a concern, data are encrypted before outsourcing to a service provider.

III. PROPOSED SYSTEM

The proposed system developed with the things that eradicate the drawbacks of the existing system. The security level very much enhanced from its actual level. The DBA cannot view the user details in its original form. The hacker cannot enter the user login by using the tricky queries, cannot run the inbuilt function in it etc.This work's inherent thesis is that, at scale, in outsourced contexts, computation inside secure hardware processors is orders of magnitude cheaper than equivalent cryptography performed on provider's unsecured server hardware, despite the overall greater acquisition cost of secure hardware.Any software-based cryptographic constructs then deployed, for server-side query processing on the encrypted data, inherently limit query expressiveness.

IV. PROPOSED BLOCK DIAGRAM



ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

This diagram showsprocess are just they apply the encryption process on the sensitive information so it's not that much secure because every encryption process have decryption also, so hackers easily to overcome this problem, we using the RAW Data Conversion and we apply the encryption process on the RAW Data, so it's more secure compare to existing process.It Convert our secure information into RAW Data after the convert to Hexadecimal Bit Using Md5 Algorithm and Stores to the Database

V. CONCLUSION

The principles of SQL attacks and attack processes are analyzed. It introduces the visiting process based on client/server model. On this basis, a database protection system against SQL attacks, mainly including the protection for ordinary users and administrators is achieved. Experiments show that this is a very effective protection system. But there are also some lacks of the protection system, protective measures taken by this system can protect the common SQL attacks, but not prohibit some rare attacks. Therefore, more research in the SQL attacks based on the protection system should be done. Of course, new attack methods are emerged with the network's development; the system protection systems should also be continuously improved and perfected.

REFERENCES

[1] FIPS PUB 140-2, Security Requirements for Cryptographic Modules, http://csrc.nist.gov/groups/STM/cmvp/standards.html#02, 2013.
[2]TPC-H Benchmark, http://www.tpc.org/tpch/, 2013.
[3]IBM 4764 PCI-X Cryptographic Coprocessor, http://www-03. ibm.com/security/cryptocards/pcixcc/overview.shtml, 2007.
[4]G. Aggarwal, M. Bawa, P. Ganesan, H. Garcia-Molina, K. Kenthapadi, R. Motwani, U. Srivastava, D. Thomas, and Y. Xu, "Two Can Keep a Secret: A Distributed Architecture for Secure Database Services," Proc. Conf. Innovative Data Systems Research (CIDR), pp. 186-199, 2005.
[5]Iliev and S.W. Smith, "Protecting Client Privacy with Trusted Computing at the Server," IEEE Security and Privacy, vol. 3, no. 2, pp. 20-28, Mar./Apr. 2005.
[6]M. Bellare, "New Proofs for NMAC and HMAC: Security Without Collision-Resistance," Proc. 26th Ann. Int'l Conf. Advances in Cryptology, pp. 602-619, 2006.
[7]B. Bhattacharjee, N. Abe, K. Goldman, B. Zadrozny, C. Apte, V.R. Chillakuru, and M. del Carpio, "Using Secure Coprocessors for Privacy Preserving Collaborative Data Mining and Analysis," Proc. Second Int'l Workshop Data Management on New Hardware (DaMoN '06), 2006.
[8]M. Canim, M. Kantarcioglu, B. Hore, and S. Mehrotra, "Building Disclosure Risk Aware Query Optimizers for Relational Databases," Proc. VLDB Endowment, vol. 3, nos. 1/2, pp. 13-24, Sept. 2010.
[9]Y. Chen and R. Sion, "To cloud or Not to Cloud?: Musings on Costs and Viability," Proc. Second ACM Symp. Cloud Computing (SOCC '11), pp. 29:1-29:7, 2011.
[10]V. Ciriani, S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Combining Fragmentation and Encryption to Protect Privacy in Data Storage," ACM Trans. Information and System Security, vol. 13, no. 3, pp. 22:1-22:33, July 2010.
[11]T. Denis, Cryptography for Developers, Syngress, 2007.
[12]E. Damiani, C. Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati, "Balancing Confidentiality and Efficiency in un-trusted Relational DBMSs," Proc. 10th ACM Conf. Computer and Communications Security (CCS '12), 2003.
[13]E. Mykletun and G. Tsudik, "Aggregation Queries in the Database-as-a-Service Model," Proc. 20th IFIP WG 11.3 Working Conf. Data and Applications Security, pp. 89-103, 2006.
[14]F.N. Afrati and V. Borkar, and M. Carey, and N. Polyzotis, and J.D. Ullman, "Map-Reduce Extensions and Recursive Queries," Proc. 14th Int'l Conf. Extending Database Technology (EDBT), pp. 1-8, 2011.
[15]V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R. Motwani, "Distributing Data for Secure Database Services," Proc. Fourth Int'l Workshop Privacy and Anonymity in the Information Soc. (PAIS '11), pp. 8:1-8:10, 2011.