The People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
Unviversity Mohamed MOHAMED - M'SILA
Faculty of Mathematics and Informatics

COMPUTER SCIENCE DEPARTMENT

Case Number:.....

Research Paper

Presented in partial fulfillment of the Requirements for the Degree of Master

Field : Mathematics and Informatics

Branch : Computer Science

Specialty : ICT

By: Marwan Radjai

TOPIC

Preventing SQL Injection Attacks Using a Cryptography Technique

Publically defended on : / /2016 Before a Jury composed of :

Mr.....	**Université of M'sila**	**Chairman**
Dr. Noureddine Chikouche	**Université of M'sila**	**Supervisor**
Dr. L Belabdelouahab-Fernini	**Université of M'sila**	**Co-Supervisor**
Mr.....	**Université of M'sila**	**Examiner**
Mr.....	**University of M'Sila**	**Examoner**

Class: 2015 /2016

Elements | SUMMARY | Page

General Introduction

Web applications are everywhere on the Internet. Almost everything you do online is done through a web application whether you know it or not. They come in the form of web-based email, forums…, it is important to understand that these types of websites are all database driven.

Databases are aprincipal element of web applications because they are able to store user's preferences, personal identifiable information, and other sensitive user information.Web applications interact with databases to dynamically buildcustomized content for each user,the web application communicates with the database using structured query language (SQL).

SQL is a programming language for managing databases that allows you to read and manipulate data in MySQL, SQL Server, Access, Oracle, and other database systems, the relationship between the web application and the database is commonly abusedby attackers through SQL injection.

The SQL injection is a type of injection attack in which SQL commands are supplied(provided) in the user-input variables, such as a web form entry field, in atry to trick the web application into executing the attacker's code on the database.

The results of SQLI (SQL injection) can be disastrous because the successful SQL injection can read sensitive data from the database, modify database data (insert/update/delete), execute administrative operations on the DB, recover the contents on the DBMS file system.

There is a lot of approach that assistance to protect web and preventing SQL injection, but not all this technique offer the same levels of security, so had better to select best technique which help us to protect personal information against hackers,we think the approach that rely on cryptography system gives more security compared to other strategies.

In our project, we present the implementation of a novel idea to prevent SQL injection, which relies on a cryptography system, where we use effective cryptography system (public key cryptography) to build a strong digital signature, hence access to a novel mechanism that helps to offer more a secure web application, we also explain the Random encryption algorithm and use it in our application.

The goals of this work

The objective of the work entitled «**implementation of a cryptography system to prevent a SQL injection** »is to give a maximum security to protect the web application against SQL injections, we can summarize our work in the following steps:

- ✓ Explain the SQL injection vulenirability
- ✓ Study and analyse some public-key cryptosystems and digital signatuers
- ✓ Discuss about existing solution that based on cryptography system.
- ✓ Implement digital signature on the web application to prevent a SQL injection.

Research paper outline

Our research paper is divided into fourchapters:

- ✓ The first chapter presents thedefinition of the SQL injection and the SQLI mechanism and different kinds ofSQLI which are used by the hackers to avoid security of web application.We also explain some strategies to prevent anddetect a SQL injection.
- ✓ The second chapter studies some public-key cryptography systems like (RSA, Elgamal, NTRU, ECC…).We also attempt to clarity the principal roles of digital signateures andthe hashing secure technique.
- ✓ The third chapterdeals withthe exsisting techniqueto prevent a SQL injection, which uses a cryptography system.
- ✓ The fourth chapter discusses the implementation of some public-key cryptosystems to prevent a SQL injection, the implementation of adigitalsignature to make anauthentication.

General Conclusion:

A SQL injection is one of the most important web security threats that needs attention so as to improve security for the users and their data. In this dissertation, we showed the security techniques used to secure web applications against a SQL injection, hence protect sensitive data from hackers. These security techniques have problems and do not ensure the necessary security rules. There are some techniques which offer less security compared to others.

The cryptographic techniques are the most interesting tools to prevent SQL injections. We presented in our work the basic rules of public-key cryptosystems like encryption, decryption, digital signature, and we showed how we can use public-key cryptography to ensure security of web application through use digital signature .

We also presented an authentication scheme for preventing SQL Injection attacks using ECC and RSA. Signing username and password are used to improve the authentication process, and avoid to deal with natural input. Our strategy relies on random, algorithm based on randomization and used to convert the input into a cipher text. For any input in the registration phase, we apply the random (ECC, RSA).

Future perspectives

In this work, I have concentrated on the particular kind of a SQL injection. I think that this kind needs more research, mainly because of various reasons: SQL injection attacks are most probable to change and new vulnerabilities will be found, collectively with new countermeasures to deal with them. As many hacking sites exist on the web, and since attack methods are well described and circulated between hackers, we believe that information about new attack methods must be constantly surveyed and new counter measures should be developed. As future recommendations, we had better adjust some points that are explained below:

- ✓ Use another cryptography algorithm that maybe better in the future compared to algorithms that were used in our application.
- ✓ Find another way to reduce time consumed during the login process
- ✓ In the future, I will try to develop a technique that enables total prevention against other kinds of SQL Injection Attacks.
- ✓ Also, we can added other cryptography algorithm to our strategy, that mean became use 3 or 4 algorithm in **Random** function.

REFERENCES

[1]Neha Mishra,SunitaGond, *Defenses To Protect Against SQL Injection Attacks*, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013.

[2] AtefehTajpour, Suhaimi Ibrahim, Maslin Masrom,*SQL Injection Detection and Prevention Techniques,*International Journal of Advancements in Computing Technology Volume 3, Number 7, August 2011, University Technology Malaysia.

[3]Manisha A. Bhagat Prof Vanita Mane, *protection web application against SQL injection attack*, International Journal of Scientific and Research Publications, Volume 3, Issue 10, October 2013 ISSN 2250-3153.

[4]Sangita Roy Avinash Kumar Singh and Ashok Singh Sairam Senior Member IACSIT, *A Novel Approach to Prevent SQL Injection Attack Using URL Filter*, International Journal of Innovation, Management and Technology, Vol. 3, No. 5, October 2012.

[5] S. FouzulHidhaya and Angelina Geetha, Department of Computer science and Engineering B.S. AbdurRahman University Chennai Tamilnadu India., *Intrusion Protection against SQL Injection Attacks Using a Reverse Proxy*,

[6] Benjamin Livshits and Monica S. Lam, *Finding Security Vulnerabilities in Java Applications with Static Analysis*, Computer Science Department Stanford University, September 25, 2005.

[7]Vibhakti Mate Milind Tote, *implementation approach for secure web application by different prevention strategy*, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 11, November 2014.

[8]OWASP plans to release the final public release of the OWASP Top 10 - 2010 during the first quarter of 2010 after a final, one-month public comment period ending December 31, 2009.

[9]Department of Computer Applications SRM University Chennai India S.AnjugamA.Murugan, *Efficient Method for Preventing SQL Injection Attacks on Web Applications Using Encryption and Tokenization*, Volume 4, Issue 4, April 201.

[10]SrinivasAvireddyVaralakshmiPerumal Narayan Gowraj…, *Random4: An Application Specific Randomized Encryption Algorithm to prevent SQLInjection*, 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[11] TayoubWalid, *Implementation of Public-Key Cryptosystems on Android Mobiles*, unpublished Master, M'Sila University, Computer Science department 2012/2013.

[12]Santa Clara, *An Introduction to Cryptography, Network Associates, Inc. and its Affiliated Companies,*(1990-1999), pp.11, 15.

[13]*Cryptography and data Security*, by Addison-Wesley Publishing Company, *Reading Massachusetts Menlo Park California London Amsterdam Don Mills, Ontario Sydney*,1982.

[14]*Technopidian.http//www.technopidian.com/definition14516/ hashing.*

[15]A.J.Menezes, P. van Oorschot and S.A. Vanstone.*The Handbook of Applied Cryptography, Cryptography an Introduction (3rd Edition)*, Nigel Smart, 1997, University of Bristol.

[16]*The Mathematics of the RSA Public-Key Cryptosystem*, Dr Burt Kaliski RSA Laboratories, 1989.

[17]*Elliptic curve cryptosystem*, Naoya Torii Kazuhiro Yokoyama, June 6-2000, UDC -681,8.

[18]*Elliptic Curve Cryptography, An Implementation Guide Anoop MS*available at:*http://www.infosecwriters.com/text_resources/pdf/Elliptic_Curve_AnnopMS.pdf.*

[19]*http//www. Security innovations.com/products/encryption-liberaries/ntru-crypto.*

[20] Professor Kris Gaj, *The NTRU Cryptosystem Implementation and Comparative Analysis,* Rodney D'Souza, George Mason University, ECE 646, Fall 2001.

[21]*Analytical study of implementation issues of NTRU*, Gauravaram, Praveen, Narumanchi, Harika, Emmadi, NiteshThis, 2014. File downloadedfrom:
http: //www.eprints.qut.edu.au./83615/.

[22]*The ElGamal Cryptosystem*, Andreas V. Meier, June 8, 2005.

[23]Shafi Goldwasser Mihir Bellare, *Lecture Notes on Cryptography*, (MIT July 2008).

[24]Joseph Sterling Grah, *HASH FUNCTIONS IN CRYPTOGRAPHY*,Master of science thesis, Universitet i Bergen, June 1, 2008.

[25] A.J.Menezes, P. van Oorschot and S.A. Vanstone.*The Handbook of Applied Cryptography, Cryptography An Introduction* (3rd Edition), Nigel Smart, 1997, University of Bristol.

[26]William Stallings, *Basics of Cryptography, Network Security Essentials, Applications and Standards*, 2nd edition. Chapter2. Give the year and place of publication.

[27] Yogesh Bansal, Jin H. Park, *Multi-hashing for Protecting Web Applications from SQL Injection Attacks*, computer science californiastate university,Volume 4, Number 3, May 2015.

[28] DepavathHarinath, M V Ramana Murthy, B Chitra, *Cryptographic Methods and Performance Analysis of Data Encryption Algorithms in Network Security*, International

Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 7, July 2015, Available online at: www.ijarcsse.com.

[29]Stackoverflowhttp://stackoverflow.com/questions/6870473/comparison-of-performance-difference-between-rsa-managedrijndael-managed-aes.

[30] A. P Shaikh, V. kaul, *Enhanced Security Algorithm using Hybrid Encryption and ECC*, I.T, Thakur College of Engineering & Technology /Mumbai University, India, May-Jun. 2014, Available online at: www.iosrjournals.org.

[31] Rounak Sinha, Hemant Kumar Srivastava, Sumita Gupta, *Performance Based Comparison Study of RSA and Elliptic Curve Cryptography*, International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013, ISSN 2229-5518, Available online at : http://www.ijser.org.

[32] http://www.ntchosting.com/encyclopedia/databases/mysql/phpmyadmin consulted in (10-04-2016).

[33] http://www.ibm.com/devloperworks/java/tutorials/j-introjsp/j-introjsp-html.consultedin (10-04-2016).

[34]Technopediahttp://www.technopedia.com/definition/jsps consulted in (10-04-2016)..

[35]Technopedia http://www.technopedia.com/definition/24735/netbeans consulted in (10-04-2016)..

[36]http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/advantages-and disadvantages.htm consulted in (10-04-2016).

الملخص

مع تزايد خدمات وحجم استعمال الانترنت في العالم تزايدت معه التهديدات و الخروقات الأمنية بشكل كبير،من بين نقاط ضعف تطبيقات الويب والأكثر خطورة هي حقن SQL الخبيثة حيث بمجرد إدخال هذه التعليمات الخبيثة تتسبب في استعراض شامل لبيانات سرية.

لذا فان الهدف من هده المذكرة هو إيجاد الطريقة المثلى لحماية تطبيقات الويب والبيانات الحساسة من المهاجمين والخروقات الأمنية عن طريق استخدام أنظمة التشفير الفعالة التي توفر بدورها درجة حماية كبيرة لتطبيقات الويب حيث قمنا بدراسة شاملة حول مختلف الاستراتيجيات التي تعتمد على التشفير في مضمونها وأمثلها كما تطرقنا إلى ما يسمى بالإمضاء الالكتروني ودوره الفعال في حماية البيانات حيث طبقنا بعض خوارزميات التشفير مثل RSA ECC,أيضا شرح بعض التقنيات المستخدمة لحماية ومنع الاستفسارات الملوثة التي يتم إدخالها من طرف المهاجم .

كلمات دلائلية:ECC،RSA، SQL، SQLI، NTRU، Elgmal، PHPMyadmin

Abstract

With the spread of Internet use in the world, security threats in the Internet increased dramatically. Among the vulnerabilities of the web application is SQL injection, which is based on the insertion of malicious requests to the DBMS, which executes these requests denier allowing access to sensitive and confidentiel data.

The purpose of this research paper is to find the best way to protect Web applications and sensitive data against hackers and security breaches through the use of effective encryption systems which, in turn, provide a significant degree of protection for Web applications. We made a thorough study of the different optimal strategies based on encryption in their content. We dealt with the e-Signature and its effective role in the protection of data. We applied encryption algorithms such as ECC, NTRUand of some of the techniques used to protect and prevent contaminated queries that are entered by the attacker.

Keys words:ECC, RSA, SQL, SQLI, NTRU, Elgmal, PHPMyadmin.

Résumé

Avec l'augmentation et la propagation de l'utilisation de l'internet dans le monde, les menaces de sécurité dans d'Internet ont augmenté de façon spectaculaire. Parmi les points vulnérables de ces applications web c'est l'injection SQL, qui se base sur l'insertion des requêtes malveillantes vers SGBD.Ce denier exécute ces requêtes ce qui lui permet d'accéder à des données sensibles et confidentielles.

Le but de ce mémoire est de trouver la meilleure façon de protéger les applications Web et les données sensibles contre les pirates et les failles de sécurité par l'utilisation des systèmes de cryptage efficaces qui, à leur tour, offrent un degré important de protection pour les applications Web. Nous avons fait une étude approfondie sur les différentesstratégies optimales qui se basent sur le chiffrement dans leur contenu.Nous avons mentionné l'e-Signature et son rôle efficace dans la protection des données. Nous avonségalement appliqué des algorithmes de chiffrement tels que ECC, RSAnous avons aussi expliqué quelques techniques utilisées pour protéger et prévenir les contaminées qui ont été entrées parattaquant.

Mottes clés: ECC, RSA, SQL, SQLI, NTRU, Elgmal, PHPMyadmin.