INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,
Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],
Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 2980 Cities in 165 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. COVERING LETTER FOR SUBMISSION:

DATED: _____________

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF** .

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

NOTES:
a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mentionthe following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. MANUSCRIPT TITLE: The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. AUTHOR NAME (S) & AFFILIATIONS: The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. ABSTRACT: Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS**: Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT**: Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS**: All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS**: All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT**: The main text should follow the following sequence:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESES

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

SCOPE FOR FURTHER RESEARCH

ACKNOWLEDGMENTS

REFERENCES

APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **FIGURES &TABLES**: These should be simple, crystal clear, centered, separately numbered &self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS**:These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES**: The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.
- ONLINE RESOURCES
- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

SPIRAL SECURITY MODEL TO COUNTER THE THREATS DUE TO HUMAN FACTORS IN WEB APPLICATIONS

BISWAJIT TRIPATHY
ASSOCIATE PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
SYNERGY INSTITUTE OF ENGINEERING & TECHNOLOGY
DHENKANAL

JIBITESH MISHRA
HEAD
DEPARTMENT OF INFORMATION TECHNOLOGY
COLLEGE OF ENGINEERING & TECHNOLOGY
BIJU PATNAIK UNIVERSITY OF TECHNOLOGY
GHATIKIA

ABSTRACT

Last few years, the security of web has taken a different turn. More and more attacks are done on applications. Also the severe lack of employee awareness is making security breaches particularly due to their weak operational practices. To make the task of the attackers easier, many a times the back-end systems are tied into the front-end ones. Due to the emergence of e-commerce systems, the integration of extranet has made the task of the security managers more complicated. The client side can be classified into external clients and internal employees. The social engineering practices employed by organizations may not be adequate for both categories of clients. We propose a spiral security model that includes the conventional planning phases to monitoring phases that takes the help of various technical components of web applications to counter the threats due to human factors. Though application firewall is a easier threat protection measure, but we propose a model that takes into account some corrective as well as preventive measures from the human perspective based on some technical components.

KEYWORDS

e- Commerce, Spiral Security, Human Factors, Corrective & Preventive.

1. INTRODUCTION

With the growth of e-commerce more and more web based applications are integrated to have intranet & extranet systems in place. India, an emerging economy, has witnessed unprecedented levels of economic expansion, along with countries like China, Russia, Mexico and Brazil. India, being a cost effective and labor intensive economy, has benefited immensely from outsourcing of work from developed countries, and a strong manufacturing and export oriented industrial framework. In 2009 out of $161.3 billion most of the FDI went to the IT and ITeS sector. Experts expect the Indian economy to be the world's biggest economy by 2040.

Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users .

In a nutshell, the perception of cyber-threats therefore has two main aspects: On one side A new kind of vulnerability due to modern society's dependency on inherently insecure information systems, and the expansion of the threat spectrum, especially in terms of malicious actors and their capabilities, on the other side[12].

Attackers have changed trends to attack more on the application than the traditional attacks. Most of these attacks take a social approach [1,2] than the technical approach. Security processes need to be kept in all places keeping the attackers mentality in view. Particularly as the clients are used by the attackers through social practices, new social engineering methodologies should be kept in place involving the clients. We have proposed a spiral security model involving both corrective & preventive actions to counter the threats from the human factors. This paper consists of the following sections. Section 2 describes the existing security measures against application threats in the e-commerce systems. The vulnerabilities on web based systems due to the social factors and the protective measures are discussed in Section 3.

We have proposed a new security model called as spiral security model for the web based applications to counter the threats due to human factors in section 4. Section 5 gives the conclusion and final remarks.

2. EXISTING SECURITY MEASURES FOR E-COMMERCE APPLICATIONS THREATS

The major security issues are confidentiality, integrity and availability. Of late privacy and non-repudiation are added to the security of e-commerce systems. However, authentication, authorization and auditing are the three major factors for the security of applications. There are many recorded application vulnerabilities and their counter measures in the web application threat model [3]. In this section, we will categories of web application vulnerabilities and their countermeasures.

2.1. KEY APPLICATIONS THREATS

The key points for web applications are already identified as following.

- Input and data validation
- Authentication
- Authorization
- Configuration management
- Sensitive data
- Session management
- Cryptography
- Parameter manipulation
- Exception management
- Auditing and logging

The threats that can arise due to these key points are shown in the table below.

TABLE 1: KEY APPLICATION AREAS

Key Points	Description
Input and data validation	Input validation refers to validation of input by the application filters before additional processing.
Authentication	Authentication is the process where an entity proves the identity of another entity, typically through credentials, such as a user name and password.
Authorization	Authorization is to check how the application provides access controls for resources and operations.
Configuration management	Configuration management refers to the handling operational issues of the application. It includes questions like as to how the application is administered, which databases it connects to and how these settings are secured.
Sensitive data	Sensitive data refers to how your application handles any data that must be protected either in memory, over the wire or in persistent stores.
Session management	A session refers to a series of related interactions between a user and the web application. Session management refers to how the application handles and protects these interactions.
Cryptography	Cryptography refers to how the web application enforces confidentiality and integrity. It includes questions like how secured and tamperproof the data or libraries are? How strong are the seeds for random values that must be cryptographically strong?
Parameter manipulation	Parameter manipulation refers to safeguards of parameters and how the application processes input parameters.
Exception Management	It is the management of failure of application. It includes questions like does the application fails gracefully or does it return friendly error information to end users?
Auditing and logging	Auditing and logging checks as to how the application records security related events i.e. who did what and when?

The threats related to the key points can be shown in the following table.

TABLE 2: KEY APPLICATION THREATS

Key Points	Threats
Input and data validation	Buffer overflow, cross-site scripting, SQL injection
Authentication	Network eavesdropping, brute force attacks, dictionary attacks, cookie replay, credential theft
Authorization	Elevation of privilege, disclosure of confidential data, data tampering, luring attacks
Configuration management	Unauthorized access to administration interfaces, unauthorized access to configuration stores, retrieval of clear text configuration data, lack of individual accountability, over privileged process and service accounts
Sensitive data	Access sensitive data in storage, network eavesdropping, data tampering
Session management	Session hijacking, session replay, man in the middle
Cryptography	Poor key generation or key management, weak or custom encryption
Parameter manipulation	Query string manipulation, form field manipulation, cookie manipulation, HTTP header manipulation
Exception management	Information disclosure, denial of service
Auditing and logging	User denies performing an operation, attacker exploits an application without trace, attacker covers his or her tracks

2.2. SECURITY MEASURES AGAINST THE APPLICATIONS THREATS

The countermeasures for the traditional security threats are already given by many authors from time to time. For instance, in the SQL injection under the input validation, the countermeasure can be as follows:

- A thorough input validation should be performed. The application should validate its input prior to sending a request to the database.
- Parameterized stored procedures for database access should be used to ensure that input strings are not treated as executable statements. If stored procedures can't be used, SQL parameters can be used to build SQL commands.
- Least privileged accounts should be used to connect to the database.

Similarly, countermeasures to prevent cookies replay under authentication can include the following:

- An encrypted communication channel provided by SSL should be used whenever an authentication cookie is transmitted.
- A cookie timeout to a value should be used that forces authentication after a relatively short time interval. Although this doesn't prevent replay attacks, it reduces the time interval in which the attacker can replay a request without being forced to re-authenticate as the session has timed out.

Also, countermeasures for unauthorized access to administration interfaces under the configuration management can include the following:

- The number of administration interfaces should be minimized.
- Strong authentication e.g. using digital certificates should be done.
- Strong authorization with multiple gatekeepers should be done.
- Local administration should only be done. If remote administration is absolutely essential, encrypted channels such as VPN technology or SSL should only be used. In order to further reduce the risk, IPSec policies should be used to limit remote administration to computers on the internal network.

3. THREATS ON E-COMMERCE APPLICATIONS COMPONENTS DUE TO SOCIAL FACTORS

The major components of e-commerce applications are front-end web server, middle-tier application server and the back-end database server. Some of the counter measures of the key security issues as discussed earlier e.g. secured configuration, validating inputs, exception handling and authorizing users can be applied to the web server in order to protect it. The application server needs to apply the counter measures for authentications and authorization. The auditing and logging activities on transactions need to be employed in the application server as well. The database server needs to be protected by the usage of hashing techniques as sensitive data are available there. The various social factors that can cause threats to these components are discussed below.

3.1. KEY SOCIAL FACTORS ENABLING APPLICATION THREATS

The key social factor for gaining access to e-commerce applications is to get acquaintance of the system. Social engineering is the practice of obtaining confidential information by manipulation of legitimate users. Some of the key issues that can create threats to the e-commerce application is given below:

- Gathering information about employees through mailers e.g. survey etc.
- Gathering information about employees by developing relationships
- Forensic analysis of the hard drives, memory sticks etc.
- Pretending to be a senior manager or helpless user
- Pretending to be a technical support engineer
- Disgruntled employees

The threats that can arise due to these key points are mainly accessibility to the various resources of the e-commerce system. The CISCO 2008 annual report tells that human nature, in the forms of insider threats, susceptibility to social engineering and carelessness that leads to inadvertent data loss, continues to be a major factor in numerous security incidents [4].

3.2. COUNTER MEASURES FOR THE SOCIAL FACTORS

There are well defined counter measures for the security threats due to the social factors.
Some of them are given below.

- A well documented Security Policy accessible to employees & training provided to the employees
- Awareness of threats and impact of social engineering on the company
- Implementation of proper security audit
- Proper Identity Management policy for authentication
- Clear cut operating policies & procedures to limit vulnerabilities.
- Use of advanced physical solutions such as intelligent revolving doors, biometric systems, etc. to eliminate or reduce unauthorized physical access

Some of the hacker tactics and the combat strategy [5] from the social engineering aspect are listed. However, a more generic well-documented Security Policy and associated standards and guidelines can form the foundation of a good security strategy. The policy should clearly document in ordinary terms so that the ordinary user i.e. the employee will understand. Also along with each policy, the standards and guidelines to be followed should be clearly explained. Some of the broad outlines of this policy should include the following:

- Computer system usage: Monitoring the usage of the use of non-company standard mails or activity.
- Proper Information classification and handling: Confidential information should be properly classified and should not be available to everybody.
- Personnel security: Proper screening new employees and other visitors to ensure that they do not pose a security threat.
- Physical security: Proper authentication process for allowing employees to secure portions inside the company e.g. sign in procedures through electronic and biometric security devices etc.
- Information access: Password usage and guidelines for generating secure passwords, access authorization.
- Protection from viruses: Working policies for protection of the systems from viruses and other threats.
- Security awareness training: This ensures that employees are kept informedof threats and counter measures.
- Compliance monitoring: This ensures that the security policy is being complied with.
- Documentation destruction: All information should be disposed of by shredding not by discarding in the trash or recycle bins.

4. SECURITY MODEL FOR E-COMMERCE APPLICATIONS

As far as design of e-commerce applications are concerned, the counter measures of the key security issues on its major components are discussed earlier e.g. secured configuration, validating inputs, exception handling and authorizing users for web servers, authentications, authorization, auditing and logging activities for the application server, etc. In order to counter the vulnerabilities in the e-commerce application design, there are secured design considerations. For example, under input validation, constraining input is one of the preferred approach. This is about allowing good data. The idea here is to define a filter of acceptable input by using type, length, format and range. Use cases should be written and the acceptable input for the application fields should be written.

Similar to the input validation techniques, strong authentication techniques mainly in terms of passwords policies should be prepared. Strong passwords, password expiry period and account lockout policies can safeguard the servers. However, the concern is not in the design issues rather in the human issues. In this section, we propose some corrective & preventive measures from the human perspective.

4.1. DATA LEVEL VALIDATION

Though the design consideration makes input validation in a proper manner, what about the disgruntled employees who makes some changes in the data layer that can create chaos in the e-commerce system. For example, in a shopping cart example, if an accounting operator is given privilege of changing the rate of certain items as there is a change in the rates and he changes the rates of some other items whose rates are not changed, this is an issue of data integrity. Here there are two counter measures that can be offered as given below.

1. Allowing item wise privileges to the employee to change data.
2. Counter authorizing the changes by the account manager.

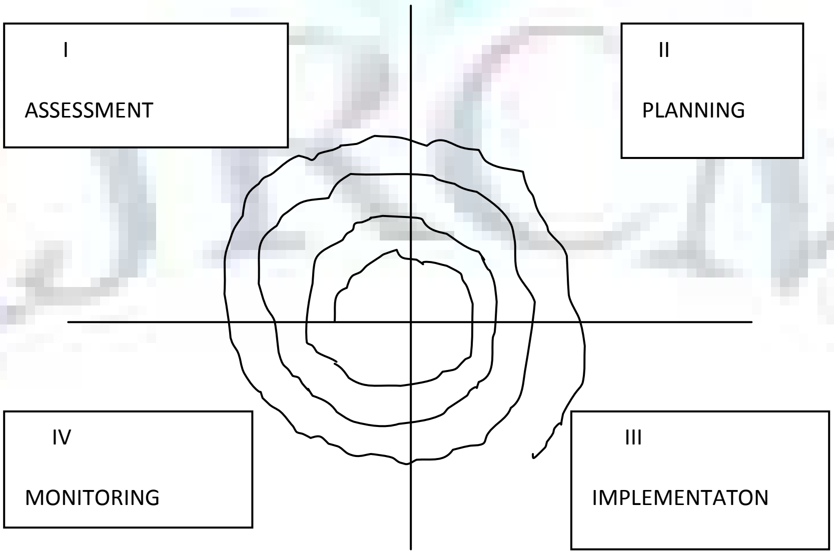
However, there is still human factor for both these cases. In the first case, many a times even though item wise privileges are given to the particular employee, he can mention certain problem in the system and get the general privilege from the system administrator.

With regard to the second case he might have obtained the password of his manager by some means. Therefore, even if a threat tree [6] will be drawn and both these threats due to human factors can be made "AND", still there is always a chance of malicious intent.

This type of threat can only be detected if the a data layer audit is made and its cycle should be short depending on the number of e-commerce transactions in the system.

Therefore, a continuous monitoring is required as may be seen in the proposed spiral model in figure 1 below:

FIGURE 1: SPIRAL MODEL FOR E-COMMERCE SECURITY



4.2. SYSTEM LEVEL AUTHORIZATION

When the design of application is made, minimum access to the system level recourses should given. In fact, restrictions should be placed on the application in terms of which system-level resources it can access. This risk mitigation strategy can limit damage to the Assessment Planning Monitoring Implementation application.

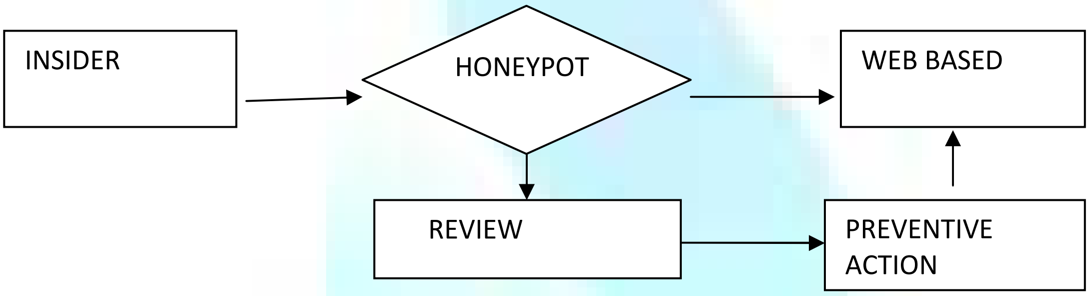
This code access security is a resource constraint model that can prevent code and Web applications from accessing specific types of system-level resources. When code access security is used, it inevitably influences the application design. Also, the application design should identify all of the identities that the application uses, including the process identity and any impersonated identities, including anonymous Internet user accounts and service identities. The design should also indicate to which resources these identities require access. At deployment time, the appropriate access control list can be configured on system-level resources to ensure that the identities of the application only have access to the resources they require. However, the insider threat research indicates that 57% of the insiders were granted access to system administrator's password upon hire and another 33% of the insiders were hired as privileged uses [7].

One of the major preventive method for insider threat is proper screening of employees. However, as prevention of insider threat is the costliest and can make much damage, some preventive actions can be made as given below:

- Conducting careful background checks.
- Clearly documenting insider threat controls.
- Enforcing separation of duties and least privilege.
- Implementing strict password and account management policies and practices.
- Monitoring and auditing every employee's online actions.
- Monitoring and responding to suspicious or disruptive behavior.
- Making usage of additional controls for system administrators and privileged users.
- Layered defense against remote attacks should be made.
- Following termination of employee immediately deactivate access.
- Collection of employee data for investigations, if required.
- Implement secure backup and recovery processes.

Also a better option can used to spot the disgruntled employees is implementation of a honeypot [8,9]. These honey pots can provide valuable information on the patterns used by insiders. We have suggested to use a honeypot as shown in figure 2 to identify the employees usage pattern and accordingly take preventive action.

FIGURE 2: A PREVENTIVE HONEYPOT MODEL FOR INSIDERS



In fact, both the data layer audit for a corrective action and the insiders usage patterns for a preventive action can be monitored regularly using the spiral model and fresh assessment about the security of the e-commerce application can be made. This Insiders System Review Honeypot assessment needs proper planning for final implementation. As this process is an ongoing one, we have proposed this spiral model for the security of web applications.

5. CONCLUSION

Though the design considerations from the security perspective for web applications are clearly stated in many of the research papers, the security issues from the human perspective is hardly considered from the technical perspective. Only some counter measures for social factors as discussed in section 3.2 are suggested by researchers from time to time. Even Intrusion Detection Systems (IDS) are not able to track insider attacks [8] and the complexity of using a combination of IDS systems [10] may not be adequate.

Therefore, we have proposed a spiral model that takes into account a data layer audit for corrective action and finding the insiders usage pattern from a honeypot application for preventive action, those work in conjunction with each other to make an effective web based security model from the human perspective.

REFERENCES

1. About.com. (2008). Social Engineering: Testing the Human Factor of Security. Retrieved February 27, 2013, from http://bizsecurity.about.com/od/personneltesting/a/soceng.htm.
2. Granger, S. (2001). Social Engineering Fundamentals, Part I: Hacker Tactics. Retrieved February 28, 2009, from http://www.securityfocus.com/infocus/1527.
3. Meier, J. D., Mackman, A. and Wastell, B. (2005). Threat Modeling Web Applications. Retrieved February 9, 2013, from http://msdn.microsoft.com/enus/library/ms978516.aspx.
4. CISCO. (2008). Cisco 2008 Annual Security Report. Retrieved February , 2009, from http://www.ironport.com/report/.
5. Granger, S. (2002). Social Engineering Fundamentals, Part II: Combat Strategies. Retrieved February 28, 2009, from http://www.securityfocus.com/infocus/1533.
6. Fredsson, J. and Olandersson, S. (2001). Threats in Information Security: Beyond technical solutions – using threat tree analysis. Bachelor's Thesis, Bleking Institute of Technology. Retrieved February 11, 2013, from www.bth.se/fou/cuppsats.nsf/all/f1761c2bccc7e25bc1256a6c004defe5/$file/Thesis.pdf
7. Michalle Kenny, J.D., Kowalski, E., Cappeli, D., Moore, A., Shimeall, T. and Rogers, S. (2005). Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. Retrieved February 23, 2013, from http://www.cert.org/archive/pdf/insidercross051105.pdf
8. Martin, W. W. (2001). Honey Pots and Honey Nets - Security through Deception.Retrieved February 23, 2013, from http://www.sans.org/reading_room/whitepapers/attacking/honey_pots_and_honey_nets_security_through_deception_41?show=41.php&cat=attacking
9. Mokube, I. and Adams, M. (2007). Honeypots: concepts, approaches and challenges. Proceedings of the ACM 45th annual southeast regional conference. Pages 321-326.
10. Einwechter, N. (2002). Preventing and Detecting Insider Attacks using IDS. Retrieved February 23, 2013, from http://www.securityfocus.com/infocus/1558.
11. Stahl B C: Privacy and Security as Ideology by IEEE Technology & Society Magazine, SPRING,IEEE page:35-45(2007)
12. Myriam Dunn: A comparative analysis of cyber security initiatives worldwide international telecommunication union, WSIS Thematic Meeting on Cyber security, Geneva, Center for Security Studies, Swiss Federal Institute of Technology (ETH Zurich) for the WSIS Thematic Meeting on Cyber security.(2005)

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you tosupply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail**infoijrcm@gmail.com** for further improvements in the interest of research.

If youhave any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

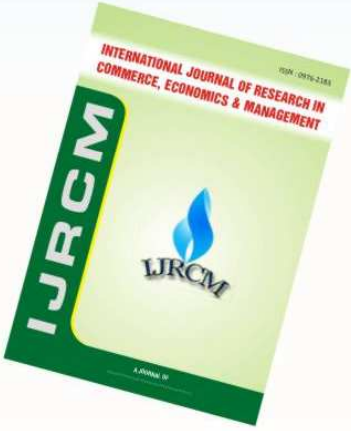
DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, nor its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal is exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals



ISSN : 0976-2183

INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, ECONOMICS & MANAGEMENT

IJRCM

IJRCM

A JOURNAL OF

ISSN : 0976-2183

INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT

IJRCM

IJRCM

A JOURNAL OF

ISSN : 0976-2183

INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE & MANAGEMENT

IJRCM

IJRCM

A JOURNAL OF