International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 3, Number 1 (2011), pp. 51-60

http://www.irphouse.com

Need of another Element for Security Improvement Approach in Web Application Development

Rajiv Mahajan[1] and Amarpreet Singh[2]

[1]Associate Prof. [2]Associate Prof.
ACET, Amritsar, Punjab, India
E-mail: rajiv_research_home@yahoo.com

Abstract

In high-speed and extremely complex environment Web enabled, information rich business needs Security. In Security Improvement Approach (SIA) understanding security, in relation to the business incentive is essential. This paper presents basic organizational elements that need to be identified, defined and addressed before examining a Web Engineering Development process for security. These elements are derived from empirical evidence based on a Web survey and supporting literature. This paper contribute Web Engineering specific elements that need to be acknowledged and resolved before examining a Web Engineering process from a security perspective and the elements can also be used in the assessment of a current application development process prior to an SIA.

Keywords: Security, Survey, Design, Academia, Web Engineering, Software Engineering, Development Process

Introduction

Sensitive elements of the web engineering development environment are multidisciplinary state of affairs [8]; a complex, agile, time sensitive development environment; a diverse end-user population and a usability focused design [18]. But now it should be assumed that the fifth element in today's Web engineering project environment is security. These can related with financial or Economic security. A large numbers of web sites publishing about the need of security. The United States Committee on Government Reform recently published information indicating that "the scores for the Departments of Defense, Homeland Security, Justice, State – the agencies on the front line in the war on terror - remained unacceptably low or dropped precipitously"[5]. It is also important to recognize that potential security breaches are

not limited to technical difficulties or process deficiencies. In order to improve human short comings, processes need to be developed so that they aid in the minimization in breaches due to human inadequacies. The story does not conclude with the obvious Web attacks and human blunders. Web technology is penetrating a multitude of other business applications. A successful attack via the RFID has a direct impact on the web channel. Hence, the long range implications for poorly designed and/or implemented Web interfaces, or middle ware applications that use Web protocols, potentially create a vast array of implications via the execution of SQL injections, buffer overflows, viruses etc.

These events drive the need to understand security based on the business incentive. Security needs to be integrated into the development process so that it provides an acceptable amount of risk mitigation, at an acceptable price, at a realistic user acceptance level while protecting the organizations information assets.

Relevant Work

Security is a hot and serious Problem in today's society and hence, quickly promoting an information rich research environment. Wang's article inspects risk at various levels in the application along with the effects on quality factors. However, the paper does not tackle organizational foundation issues that need to be addressed before security can be implemented successfully, effectively and continually. Yee's article scrutinizes issues that are relevant to security and usability but makes no reference to underlying corporate issues that drive variances between usability and security. Articles by Taylor and McGraw make excellent points about the need to improve code from a design and defense perspective. However, they provide generic information that is not specific to Web Engineering and they fail to address underlying organizational issues that affect the ability of an organization to efficiently and effectively implement security into the development process.

The Common Criteria (CC) attempts to fuse an assortment of international standards into a set of evaluation criteria to be utilized against information technology products.. The Common Criteria approach to implementing security has several problems that obstruct its acceptance in the area of Web Engineering.

The biggest obstacle is the fact that one of the defining characteristics of a Web Engineering process is short development life cycles. Another characteristic that is in conflict is the small development teams and the administrative resource intensive requirements for acquiring a certification. In addition to these issues, the certification process is expensive, there is a lack of method evaluation in the Common Criteria, and the "criteria are too focused on the technical aspects of design"[1].

Recent research produced the Security Criteria for Web Application Development which broadens the focus of the security examination specifically in the area of Web Engineering processes. SCWAD has been proposed to assess the security applicability of an existing Web engineering process and to provide guidance to Security Improvement Initiatives (SIA). SCWAD specifically recognizes six essential security criteria for evaluating web engineering methodologies. In this paper five essential security elements that need to be addressed prior to an SIA being conducted in an

Academic organization. These same elements can also be used in the assessment of a current application development process prior to an SIA.

Survey Analysis

The point of the survey was to attempt to determine how security is realistically perceived and implemented in industry during application development.

Methodology

The Web survey was validated by two different type of organization. The approach taken with the web survey was really more of a qualitative approach than a quantitative approach. Due to the fact that the survey was basically capturing current / past information, so it categorized this approach as a historical "Lessons Learned" approach to software engineering experimentation. The benefit to this approach is that it is a low cost solution to acquiring data. One of the drawbacks is that it "cannot be used for statistically validating the results". Another drawback is that it is difficult to replicate, with the same results, due to variances in the participants and mitigating issues that affect interviewee opinions. There is also a lack of control, in Web surveys, over the validity of the respondents and their answers.

In survey the sample size was relatively small,(fifty-three initial respondents) coupled with a high abandonment number (eighteen), in the application developing industry and IT expert academician (Programmer) which severely detracts from any statistical data that could be derived from the survey results. The majority of the respondents were acquired through e-mail request. The balance of the respondents was acquired via communication with colleges, i.e., word of mouth. In academia, there has been a great deal of debate over the demographic groups that have access to the internet, why individuals abandon surveys, and the best presentation design for web surveys. This survey endeavoured to determine the responder's opinion and acquire practical information regarding his or her experience with security and development methodologies.

Demographics

The initial questions were from experienced IT professionals to determine the interviewee's current role in the development process and to determine the overall size of the organization. Out of the initial sixty valid respondents who participated in the survey, forty-one of the respondents to the web survey were from different location. The options for the size of the respondent's organization are detailed in Table 1.

Organization Size Categories	Size	Response
1	0 - 500	26
2	500 - 1,000	12
3	1,000 - 5,000	10
4	5,000 - 10,000	7
5	10,000 - 50,000	5

6	50,000 - 100,000	4
7	100,000 or More	2

There were twenty-six respondents in the first category. Although the specific industry was not captured in the survey, this result supports the idea that a lot of web development companies are small companies. This makes up the majority of the respondents. The balance of the break-down is as follows: four respondents in the second category, nine respondents in the third category, three respondents in the fourth category, five respondents in the fifth category, two respondents in the sixth category and two respondents in the last category.

Results

As expected, the number of respondents decreased as the survey progressed from internet, to intranet to extranet questions. It should be noted that most of the respondents represent small businesses. The majority of the respondent's organizations have internet sites. The break down of the type of application development process implemented by the various organizations is shown in fig-1 Application Development Process.

The traditional systems development process appears to remain very prevalent in industry Web development. The industrial responses that included some form of the traditional development process appeared in five out of the thirteen responses for internet development and eight out of the thirteen for intranet development and four out of six responses for extranet development. In Case of Academician development the traditional development process appeared in four out of the thirteen responses for internet development and seven out of the thirteen for intranet development and three out of six responses for extranet development. Oddly enough, none of the respondents indicated that they use both agile and traditional processes depending on the nature of the project. Fig 1 – Application Development Process (a) Industry Response and (b) Academic Response

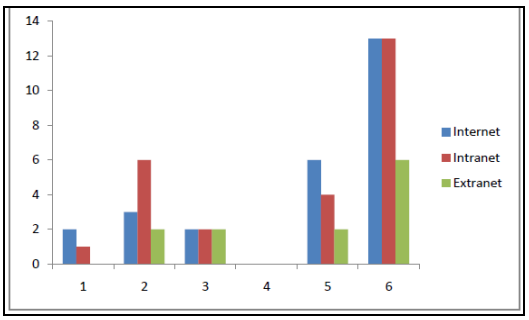


Fig 1 (a) Industry Response

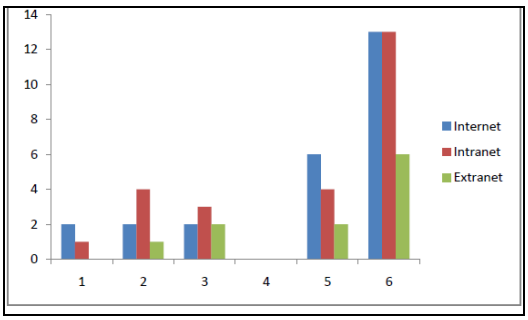


Fig -1(b) Academics Response

Fig 1 - Key X-axis

1. Agile Development Process (Extreme Programming, Dynamic Systems)
2. Traditional Systems Development Processes (Water Fall Approach, Spiral Model)
3. A process that is a combination of Traditional and Agile Development Processes
4. Use both Agile and Traditional process depending on the nature of the project.
5. In-House
6. Total Number of Respondents

This implies that the organizations involved in the survey are either all or nothing when implementing a development process. This result supports previous application development research findings where specific organizations have taken a "one size fits all approach"[24]. One of the development process response options was "In-House". In retrospect, it would have been interesting to have the individuals taking the survey explain their "In-House" approach at this point. This would have given some insight into the foundation of some of the customized development processes currently used in industry.

An interesting point is that the data did not totally reflect expectations where the methodology and the size of the company were considered in the internet development process. The expectation was that the small companies would be using agile approaches and large companies would be using some form of a traditional approach. There is a category six company using an agile approach, two companies in category one using a traditional approach and one using an in-house approach. As the survey progressed to the intranet development questions, the number of companies using a traditional systems approach doubles to six companies. Two of these companies are in category one, three are in category five and one is in category seven. There were no agile answers to the extranet development question. As expected, there were no companies in category one that responded to having an extranet.

It is encouraging that seventeen of the respondents indicated that they have a defined application internet development process; however, nineteen out of thirty-six respondents indicated that they did not. One issue that did surface through analysis is the question of a defined vs. implicit development process. An alternative set of questions would have been to ask if participants had an implicit development process and to have expanded on exactly what that entailed.

It is worth noting that there were more positive answers to the question asking about the existence of a defined application development process for intranet and extranet applications. The same question, posed about the internet, yielded more negative responses. It should be noted that out of the six respondents who have a defined extranet application development process, five of the respondents have all three forms of Web application development processes defined.

The number of positive responses for organizations in category one having a defined application development internet process fell from six in the internet, to four in the intranet and zero in the extranet categories. Hence, the trend indicates that organizations with a defined extranet process are more likely to have defined

processes for internets and intranets. The high-level application development process results are summarized in Fig 2 – Defined Application Development Process.

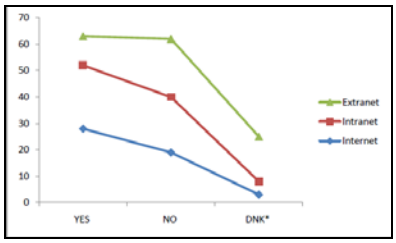
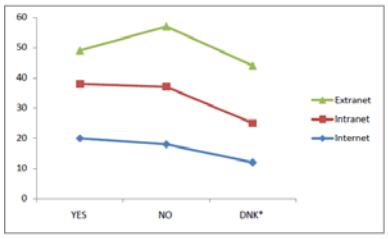


Fig 2 (a) Industry Response



*DNK: Do Not Know

Fig -2 (b) Academics Response

There were thirty-five responses to a question about the organization having a defined application development internet security process. Out of the thirty-five responses, seventeen indicated that they have an internet application development security process, while fourteen indicated that they did not and four indicated that they "Do Not Know".

The expectation was that there would have been more responses that had a defined internet application development process than a defined internet security process. On that same line of thought, another expectation also would have been for the respondents who answered positively to the defined application development process question to be the same as the respondents in the defined application development security process question.

In other words, the organizations that have an application development process would have been expected to have a security development process. A detailed examination reveals that there were seven responders who confirmed having a defined security development process but who also did not indicate positively that they have a defined application development process. This result, however, was neither logical nor expected from the survey. The organizational demographics for the ten respondents who have a security process and do not have a defined development process indicates that these respondents are from relatively small organizations both for industry and Academic organizations each. The data are summarized in fig 3 – Security Process & No Defined Application Development Process.

Fig 3 – Security Process & No Defined Application Development Process

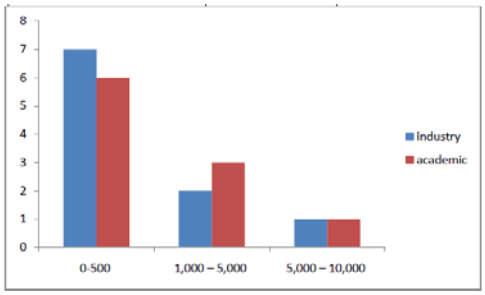


Fig 3

The results of the organizational demographics of the ten respondents that had both a defined application development process and an internet security process were as expected. The results were spread out across the respondent categories industry and Academic organizations each. This information is summarized in fig 4 – Security Process & A Defined Application Development Process fig 4 – Security Process & A Defined Application Development Process

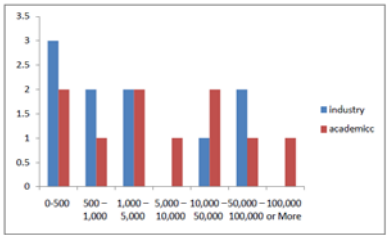


Fig 4

The survey did indicate that security is being substantially recognized "During the initial design phase" for internet, intranet, and extranet development. This is an excellent indicator that security is starting to be included at the beginning of the development process. To what depth security is being addressed in the design phase is still open to investigation.

The survey then attempted to determine the phases that were included in the security process, whether there is an individual responsible for ensuring that the security process is followed and if there is any job related impact for not following the security process. The specifics that the survey revealed, in reference to the organizations that claimed to have defined application development security processes, are summarized in Table 6 – Security Process Information. There were a total of twenty internet respondents, fifteen intranet respondents, and five extranet respondents industry and Academic organizations each.

The table reveals that, out of the respondents having a defined application development security process, the weakest phase is the feedback phase. Most of the organizations that responded indicated there was an individual on the team who is responsible for insuring that the intranet security process is followed, but there was a drop in positive responses to the question inquiring about a job related impact for not following the intranet security process.

Fig 5– Security Process Information

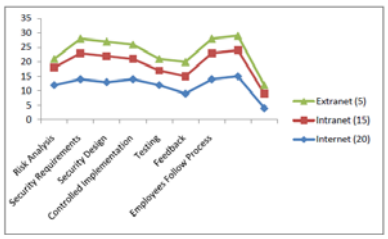


Fig 5 (a) Industry Response

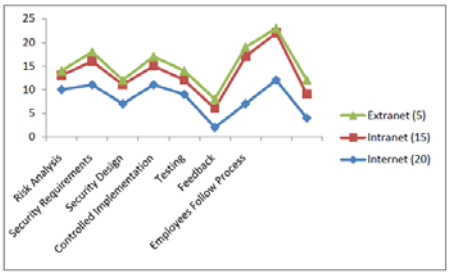


Fig 5 (b) Academics Response

It is also worth noting that a majority of the respondents felt that their organizations considered security to be "Very Important" in its internet, intranet, and extranet applications. However, the number of "Very Important" responses fell to sixteen when asked how important security is within the development process.

Organizations appear to be contributing to the security education of their employees. The survey did not attempt to define this information to determine the type of security education that was being distributed in organizations. However, there still appears to be a gap between understanding security and actually doing something about security.

Only nineteen (one more than half of the respondents) gave a positive answer to the question of the organization having a disaster recovery plan that includes the applications in the security design requirements. Only half of the nineteen responses indicated that the organization had tested the disaster recovery plan through execution.

Conclusion

Security continues to be an issue that demands attention in the business environment. All of these issues have been lightly discussed, in some form or fashion, as solitary issues of importance during application development; however, they have never been viewed as a group of criteria for secure Web application development. Realistically, the outcome of this survey presents the foundations for common sense solutions in the area of Web Engineering security processes.

Security is an important topic in today's business environment that needs to be addressed through improved processes and initiatives. Typically, security has been generally addressed in papers examining technical solutions to security, examining specific types of attacks like SQL injections, and examining specific papers on the need for organizations to conduct specific projects on risk analysis in order to understand organizational threats.

The results from the Web survey have identified five elements that should be examined prior to any Security Initiative Approach (SIA) being conducted. These elements include:

1. Application Development Methodology
2. Web Security Development Process Definition

3. End Users Feed Back
4. Implement & Test Disaster Recovery Plans
5. Job Related Impact

This does not mean that the list is exhaustive or conclusive or that these elements are mandatory for an organization to function. However, their presence will potentially improve the results of the SIA and/or provide a less resistant path to SIA identified areas that need improvement. This information can also be used to identify problem areas in SIA's that are currently under construction.

An interesting topic to examine after conducting any survey is lessons learned. More specifically, if you could repeat the survey, would you repeat the survey in the same manner? The answer to that question for this specific survey is "No". The survey should be divided into three separate surveys, one survey each for the internet, intranet and extranet. The restructure is based on the fact that several participants dropped out of the survey and that participants who did not pay close attention to the questions thought they were answering the same questions repeatedly. When in reality they were answering the same types of questions for the various forms of the net. The restructure would shorten the survey and make it more concise in respect to participant relevance.

Future work in this area should include an attempt to drill down into the various interpretations of the definition of security among an assortment of organizations. It should also attempt to acquire more detailed information on an organization's in-house development process approaches to security and examine implicit approaches to security and their effectiveness in 'real-world' environments.

References

[1] Anderson, R., Security Engineering: A Guide to Builidng Dependable Distributed Systems. 2001, New York: John Wiley & Sons, Inc.

[2] AT&T, AT&T Study Finds U.S. Businesses Unprepared For Disaster. June 6. http://www.att.com/news/2005/09/12-2

[3] Balfanz, D., Durfee, G., Smetters, D. K. and Grinter, R. E., In search of usable security: five lessons from the field. Security & Privacy Magazine, IEEE, 2004. 2(5): p. 19-24.

[4] CNN, Massacer in Madrid, Madrid bombings:One Year on. 08/05. http://www.cnn.com/SPECIALS/2004/madrid.bombing/

[5] Committee on Government Reform, "No Computer System Left Behind: A Review of the 2005 Federal Computer Security Scorecards". March 23, 2006. http://reform.house.gov/GovReform/News/DocumentSingle.aspx?DocumentID=40762

[6] Deloitte, 2004 Global Security Survey. 2004, Deloitte Touché Tohmatsu:: London. p. 1-36.

[7] Deloitte, 2005 Global Security Survey. 2005, Deloitte Touché Tohmatsu: London. p. 1-44.

[8] Deshpande, Y. and Hansen, S., Web Engineering: Creating a Discipline among Disciplines. Multimedia, IEEE, 2001. 8(2): p. 82-87.
[9] EPCglobal, The Application Level Events (ALE) Specification, Version 1.0. March 21, 2006. http://www.epcglobalinc.org/standards_technology/specifications.html
[10] Evers, J., Auditor loses McAfee employee data. March 13. http://news.zdnet.com/2100-1009_22-6042544.html
[11] Glisson, W. B. and Welland, R. Web Development Evolution: The Assimilation of Web Engineering Security. in 3rd Latin American Web Congress. 2005. Buenos Aires - Argentina: IEEE CS Press.
[12] Glisson, W. B., Glisson, L. M. and Welland, R. Web Development Evolution: The Business Perspective on Security. in Thirty-Fifth Annual Western Decision Sciences Institute. 2006. Hawaii: Western Decision Sciences Institute.
[13] Glisson, W. B., McDonald, A. and Welland, R. Web Engineering Security: A Practitioner's Perspective. in International Conference on Web Engineering. 2006. Palo Alto, California: Springer.
[14] Glisson, W. B. and Welland, R., Web Survey Technical Report. 2006.
[15] Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Richardson, R., 2004 CSI/FBI Computer Crime Security Survey. 2004, Computer Security Institute. p. 2-18.
[16] Gordon, L. A., Loeb, M. P., Lucyshyn, W. and Richardson, R., 2005 CSI/FBIComputer Crime Survey, in Tenth Annual. 2005, Computer Security Institute. p. 1-25.
[17] Gunn, H., Web-based Surveys: Changing the Survey Process. 17/11/2005. http://www.firstmonday.org/issues/issue7_12/gunn/#author
[18] Horn, P., It's Time to Arrest Cyber Crime. February 13. http://www.businessweek.com/technology/content/feb2006/tc20060202_832554.htm
[19] IBM Global Services, Business Continuity: New risks, new imperatives and a new approach. June 6. http://www-1.ibm.com/services/continuity/recover1.nsf/files/Downloads/$file/buscont.pdf
[20] Jones, T. and Holden, J., Disaster recovery: no more excuses. March 19, 2006. http://www.computerbusinessreview.com/article_feature.asp?guid=D82839BB-8BD7-4C94-B06E-BF0B27968B6A