
Smita Srivastava1, Shweta Kurda2, Priya Dubey3
Information Technology
Dronacharya College of Engineering, Gurgaon

Abstract

Web Engineering has become one of the core disciplines for building Web-oriented applications. This paper proposes to reposition Web engineering to be more specific to what the Web is, by which we mean not only an interface technology, but an information system, into which Web-oriented applications have to be embedded. More traditional Web applications often are just user interfaces to data silos, whereas the last years have shown that well-designed Web-oriented applications can essentially start with no data, and derive all their value from being open and attracting users on a large scale. The paper reaches a conclusion that Web Engineering at this stage is a moving target since Web technologies are constantly evolving, making new types of applications possible, which in turn may require innovations in how they are built, deployed and maintained.

Key words: Web Engineering, Web-based Information Systems, Web application development, development methodologies

1. Introduction

The World Wide Web has become a major delivery platform for a variety of complex and sophisticated enterprise applications in several domains. In addition to their inherent multifaceted functionality, these Web applications exhibit complex behavior and place some unique demands on their usability, performance, security and ability to grow and evolve. However, a vast majority of these applications continue to be developed in an ad-hoc way, contributing to problems of usability, maintainability, quality and reliability. While Web development can benefit from established practices from other related disciplines, it has certain distinguishing characteristics that demand special considerations. In recent years, there have been developments towards addressing these considerations.

As an emerging discipline, Web engineering actively promotes systematic, disciplined and quantifiable approaches towards successful development of high-quality, ubiquitously usable Web-based systems and applications. In particular, Web engineering focuses on the methodologies, techniques and tools that are the foundation of Web application development and which support their design, development, evolution, and evaluation. Web application development has certain characteristics that make it different from traditional software, information system, or computer application development.

Web engineering is multidisciplinary and encompasses contributions from diverse areas: systems analysis and design, software engineering, hypermedia/hypertext engineering, requirements engineering, human-computer interaction, user interface, information engineering, information indexing and retrieval, testing, modelling and simulation, project management, and graphic design and presentation. Web engineering is neither a clone, nor a subset of software engineering, although both involve programming and software development. While Web Engineering uses software engineering principles, it encompasses new approaches, methodologies, tools, techniques, and guidelines to meet the unique requirements of Web-based applications.

2. Relevant Work

Proponents of Web engineering supported the establishment of Web engineering as a discipline at an early stage of Web. First Workshop on Web Engineering was held in...
conjunction with World Wide Web Conference held in Brisbane, Australia, in 1998. San Murugesan, Yogesh Deshpande, Steve Hansen and Athula Ginige, from University of Western Sydney, Australia formally promoted Web engineering as a new discipline in the first ICSE workshop on Web Engineering in 1999. Since then they published a series of papers in a number of journals, conferences and magazines to promote their view and got wide support. Major arguments for Web engineering as a new discipline are:

- Web-based Information Systems (WIS) development process is different and unique.
- Web engineering is multi-disciplinary; no single discipline (such as software engineering) can provide complete theory basis, body of knowledge and practices to guide WIS development.
- Issues of evolution and lifecycle management when compared to more 'traditional' applications.
- Web-based information systems and applications are pervasive and non-trivial. The prospect of Web as a platform will continue to grow and it is worth being treated specifically.

However, it has been controversial, especially for people in other traditional disciplines such as software engineering, to recognize Web engineering as a new field. The issue is how different and independent Web engineering is, compared with other disciplines.

3. Survey Analysis

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

3.1 Methodology

The Web survey was validated by two different individuals in the financial industry. The first individual is a technical lead for a major financial institution in the United States and the second individual is a Security Specialist for a financial institution in the United Kingdom.

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, Zelkowitz and Wallace categorized this approach as a historical “Lessons Learned” approach to software engineering experimentation. This historical “Lessons Learned” approach is used to identify trends. 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 comparable 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.

Even though the survey was carefully designed in the beginning with the majority of the questions having a specific answer[22], the sample size was relatively small, (fifty-three initial respondents) coupled with a high number of respondents who did not complete all of the sections (eighteen), 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 e-mail request was initiated through the British Computing Society in Glasgow. This request helped to target professionals in the industry. The balance, of the respondents, was acquired via communication with colleges, i.e., word of mouth. The reduced sample size in the various areas helped support the initial qualitative approach to the implementation of the survey instrument. Hence, the point of the survey was not to argue the validity of the sample size, the coverage area, or the incomplete survey responses. In academia, there has been a great deal of debate over the demographic groups that have access to the internet, why individuals do not complete surveys, and the best presentation design for web surveys.

This survey endeavored to determine the responder’s opinion and acquire practical information regarding his or her experience with security and development methodologies. The Web provided the vehicle with the broadest industrial coverage, with the least cost and risk to organizations while providing information on trends in the industry. Other approaches such as gathering log data will not indicate where security is in the development process and interviews are very time consuming and costly to all parties.
3.2 Demographics

The initial questions were used to determine the interviewee’s current role in the development process and to determine the overall size of the organization. The titles indicated that the interviewees were experienced IT professionals. Out of the initial fifty-three valid respondents who participated in the survey, forty-one of the respondents, to the web survey, were from the United Kingdom. The balance of the respondents consisted of seven from Jordan, one from France, one from Japan, and three from the United States. The options for the size of the respondent’s organization and their responses are detailed in Table 1. Fifty-three respondents participated in the survey; however, only thirty-five respondents provided input for all of the sections.

Table 1. Organization size

<table>
<thead>
<tr>
<th>Categories</th>
<th>Size</th>
<th>Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0 - 500</td>
<td>28</td>
</tr>
<tr>
<td>2</td>
<td>500 - 1,000</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>1,000 - 5,000</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>5,000 - 10,000</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>10,000 - 50,000</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>50,000 - 100,000</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>100,000 or More</td>
<td>2</td>
</tr>
</tbody>
</table>

Although the specific industry was not captured in the survey, this result in the first category supports the idea that a lot of web development companies are small companies.

3.3 Web Application Development Methodology

Before security can be addressed in an organization’s Web application development process, there needs to be an application development methodology in use within the organization. This methodology can be either implicit or explicit, though it is recommended that the development process be explicit. An explicit development methodology helps encourage understanding among existing employees and can be used to help foster new employee training. The point supported by the survey is that there needs to be a Web application development methodology within the organization, regardless of approach. A web development methodology also helps to provide structure to the complex, agile, time sensitive development environment. The survey responses indicated that there is the possibility that environments exist that claim to have a security process and no application development process.

This result initiates several queries. The natural questions include: was the survey too strict in asking for a defined documented process; are there organizations that do not have implicit or explicit development environment; and are there potential discrepancies on the definition of security among the participating parties? These concerns are valid observations to note and warrant a discussion in their own right. Regardless of the outcome of those discussions, security can not be implemented into a development environment that does not exist. Hence, the identification of the Web application development process (even if it is implicit) is a critical starting point when trying to integrate security into a development environment.

3.4 Web Security Development Process Definition

The discrepancy in the responses around the questions concerning a defined application development process and a defined application development internet security process indicates that there is possibly some confusion over the definition of an internet security process in the industry. In general, most of the respondents indicated that the phases of the security development process were present. This indication naturally leads one to suspect that the respondents could have simply added a security checklist to a small piece of a traditional process and called it a security development process.

This discrepancy naturally leads to a discussion about terminology. Terminology in various environments has the potential to have multiple meanings. As Anderson indicated, reality is a complex environment in the real world[1]. Different organizations will require “some combination of user authentication, transaction integrity and accountability, fault-tolerance, message secrecy and coverture”[1].

In order to cut down on possible confusion and to ensure that everyone is communicating properly, organizations should define:

① What security means to the business
② What it means to a web application
③ What it means in the development process
④ What a Web Engineering Security development process entails.
Defining this information naturally supports the Web engineering criteria for a usability focused design. For the purposes of this discussion, security should be defined in terms of Confidentiality, Integrity and Availability also know as the CIA[23]. Security, in terms of a web application, means that the information resources are suitably protected in terms of the CIA and that the level of protection is based on acceptable risk and appropriate end-user requirements. Security in the development process means integrating appropriate security measures into the existing development process in order to produce a more secure end-product. A Web Engineering Security process should include security information that is present in the Web Engineering Security (WES) Methodology[10]. Clearly defining the Web security development process will encourage clearer communication among employees and help with future employee training.

3.5 End-User Feedback

The survey noted that there was a lack of end-user feedback in the internet, intranet and extranet development processes. If a development process does not attempt to acquire feedback from the end users, this could signal potentially large problems with the development process alignment with the needs of the business. Strong support for end-user participation, in Web application development, has been previously indicated in a journal article by McDonald and Welland[17].

This lack of feedback has a direct impact on the potential effectiveness of a security solution. Actual end-users, not surrogate end-users, need to be used in the testing of the application. End-users will perform operations, submit data, and interpret instructions in ways that the development team, the business team or the technical staff within an organization could never dream! This is also true from a security perspective.

End-users should be observed and consulted for information on the effectiveness of the implemented security solution. Observing employees has the potential to reveal security issues and application problems that could be manipulated into contributing to a security breach.

It could be argued that employees are not always forth coming with information, especially if the lack of security or the potential security vulnerability either does not directly affect their duties or actually helps them to accomplish their assigned task. This indicates that “users often disable or ignore security to get their work done”[3]. The opposite could also be argued that employees may not be aware that they are creating security problems through a lack of knowledge, general education and training. Hence, a multiple stream approach consisting of end-user involvement in testing, end-user observation, and end-user consultation is recommended when working with end-users.

The concept of involving end-users in the security aspect of the application development process is not a new concept. Saltzer and Schroeder categorized “Psychological Acceptability” as one of eight “useful principles that can guide the design and contribute to an implementation without security flaws”. Seltzer’s and Schroeder’s viewpoint was from the perspective of minimizing mistakes through the human interface design which is a valid point, but it does not specifically address end-user involvement in testing or observation of the end-user during testing. Existing research coupled with the results of the survey discussed in this paper strengthens the case for an organization to seek end-user feedback from a security perspective.

3.6 Implement & Test Disaster Recovery Plans

Nineteen of the thirty-seven respondents indicated that they have a disaster recovery plan that includes the individual applications. When asked if the organization has tested the disaster recovery plan by execution within the past twelve months the number fell to ten. Testing the disaster recovery plan implies that the plan is relatively up-to-date and is functional as of the last execution. Hence, the survey is really saying that there were ten out of a potential thirty-seven organizations that have an upto-date, tested and functional disaster recovery plan.

This information concurs with an AT&T “survey of more than 1,200 businesses conducted from January to August, 2005; (where) nearly 40 percent stated that business continuity planning was not a priority”[2]. Security is really a risk management game in today’s society [30]. In today’s Web enabled environment disruptions are measured in minutes, not hours[14]. When it comes to risk, organizations have to make hard decisions on exactly how much risk it is willing to accept and
exactly how much money it is willing to spend to achieve the agreed upon level of security [8].

The logical progression, once the risk and cost decisions have been made, is to address the need for a disaster recovery plan. There are a multitude of reasons for developing and implementing a disaster recovery plan. These reasons not only include the obvious technical attacks on an organization’s Web site, as reported by The Open Web Application Security Project (OWASP) [28], but also natural disasters and terrorist attacks. These possibilities have been blatantly exhibited over the past year or so and include: The Asian Tsunami; Hurricane Katrina; Madrid Bombings[4]; Terrorist bombing in London; and The Hemel Hempstead Oil Depot Fire[15].

These events stress the need for organizations to have and test a disaster recovery plan. If the organization does not have a disaster recovery plan, then it is difficult to develop a cost effective secure design solution for a Web application.

3.7 Job Related Impact

The survey revealed that the majority of the organizations do not have a job related impact for not following the security development process. There needs to be a job related impact associated with security process compliancy. Employees need to understand that there is a job related impact for not following organizational processes. This becomes even more important when considering security.

One solution would be to provide positive and negative reinforcement. The idea is to reward individuals that adhere to the security process. An example would be to provide monetary rewards to programmers based on the amount of secure code they produce, not the total amount of code that they generate. On the other side of this issue, there needs to be repercussions for individuals who do not follow the organization’s security development process. Another idea that has surfaced is to tie security to the employees yearly evaluation [32].

Web application development takes place in a fast paced environment where business reputations, market shares, financial opportunities and losses are at risk daily. This increased performance pressure supports the business need for increased job related impact measures in secure Web application development.

5 Education and Training

The breakneck speed of technological breakthroughs and new types of applications plus the market volatility mean that education and training are now life-long issues for everyone. Web Engineering education and training programmes must therefore not only deal with the current Web technologies but also foster the pro-active approach and a spirit of experimentation and innovation.

Universities organise undergraduate and graduate courses in computing and Information Technology (IT) focussed on traditional disciplines such as Computer Science (CS), Software Engineering (SE), Information Systems (IS) and Computer Engineering and Networking. Web Engineering does not fit well within these boundaries and in fact is not on their radar yet.

Professional organisations such as the Association for Computing Machinery (ACM), the Institute for Electrical and Electronics Engineers Computer Society (IEEE-CS), the Association for Information Systems (AIS) and others reinforce the distinctions among these disciplines even as they have started to emphasise commonalities between them. The recent curricula recommendations include net-centric computing subjects at the undergraduate level[41]. However, their thrust is more in terms of technical computing.

On the other hand, there are hundreds of commercial institutions that deliver courses in Web technologies, some of them calling their courses as Web Engineering. They focus mostly on imparting specific skills required for the current technologies and commercial packages. Only infrequently do they prepare students to face a whole gamut of issues, life-long learning or to discharge their social, legal, ethical and professional responsibilities. These areas require a level of maturity, ability and willingness to think through and beyond the boundaries of traditional disciplines.

The School of Computing and IT in the University of Western Sydney introduced two subjects in Web development at undergraduate level in 1997 and a full one-year specialisation at graduate level in 1999. The undergraduate subjects have been very popular, reflecting the popularity of the Web itself. The graduate
course currently has about 50 students but there is always a question from practically everyone as to what this Web Engineering means. Web Engineering is also taught at University of Karlsruhe\textsuperscript{43} and has been proposed at University of California, Santa Cruz. See Whitehead\textsuperscript{44} for details of the latter course. At the Catholic University in Rio de Janeiro, Web Engineering has been taught, both at the undergraduate and graduate levels, since 1996, with emphasis on design methods. A future paper will carry out a comparative analysis and critique of these courses and other proposals.

We have found that the undergraduate students thought of Web development mainly in technical, computing or programming terms. For them, the new technology itself was fascinating and the rest either irrelevant or a waste of time. Questions of copyright, privacy laws, accessibility, document management, maintenance or how to deal with information explosion were not seen as part of the overall Web development nor were the students mentally quite ready to deal with or devise strategies for future developments. In pedagogical terms, the students are still learning the basics and are not in a position to synthesise that learning, let alone evaluate how they might utilise it.

At the masters level that students start to ask, and can be challenged on how to deal with, the difficult questions about what works in specific situations, what does not, why and what can be done about it. It is at that level, with a certain degree of maturity that they start to devise and systematically experiment with their own solutions.

The tentative conclusion is that Web Engineering is best taught in all its complexity at the graduate level.

4. Conclusion

The issues covered in this paper have been lightly discussed, in some form or variation, 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 additional research on common sense solutions in the area of Web Engineering security processes.

The results from the Web survey have identified five elements that should be examined prior to any Security Improvement Initiative (SII) being conducted. The basic principle is that there appears to be fundamental issues with industrial Web application development that need to be addressed. The survey indicates that the elements listed in section five appear to be problem areas and warrant additional research. 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 SII and/or provide a less resistant path to SII identified areas that need improvement. This information can also be used to identify problem areas in SII’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 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.

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. Additional areas of interest that the survey did not explore would include: any interdependencies between the essential elements and the actual and/or perceived Return on Investment (ROI) for the individual stages of the development life cycle and specific ROI for security within each stage of the life cycle.

5. References


