Volume 3, No. 1, January 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

SECURITY ASSURANCE THROUGH EFFICIENT EVENT LOG AND AUDIT TRIALS

S. K. Pandey[1*], K. Mustafa [2]
[1]Department of Information Technology, Board of Studies the Institute of Chartered Accountants of India (Set up by an Act of Parliament), Noida- 201 309, INDIA
santo.panday@yahoo.co.in
[2]Department of Computer Science Jamia Millia Islamia (A Central University), New Delhi-110 025, INDIA
kmfaruki@yahoo.com

Abstract- In current digital era, business organizations are using Information and Communications Technologies (ICT) for better support of their goals. There is no doubt to say that every function of the business modules is either dependent or going to be reliant on IT related tools and techniques. This facilitates organizations on one side but at the same time, it has some big challenges also from the security perspective. Insecure software is already proving to be a threat to the financial, defense, energy, and other critical important applications, which are increasing risk in direct or indirect way. To overcome these issues, a variety of methodologies have been deployed for developing secure software, but, on the other hand, attackers are continuously exploiting vulnerabilities to compromise security. Research studies reveal that security cannot be added in developed software rather it should be introduced *right from the beginning* in the Software Development Life Cycle (SDLC). To achieve this objective, security measures must be embedded throughout the SDLC phases and starting from the requirements phase itself. 'Event Log and Audit Trails' is globally accepted as one of the prominent security requirements. Appropriate level of this requirement may well enforce security features and hence, ensure security for deployed software. The paper proposes a checklist, which may enable the assessment of the appropriateness of 'Event Log and Audit Trails' and lead to counter/additional measures for security assurance.

Keywords- Software Security, Security Assurance, Event Log and Audit Trials, Event Log and Audit Trials Checklist.

INTRODUCTION

The core objective of software security is to imagine about the attacker and to foresee attacker's motive and perception. Generally, software development is termed as 'building software that works under normal terms and conditions'. But, if the security aspect is clubbed with software development, the developers' focal point of concentration becomes attacker's perspective i.e. 'how they can become a threat to the software'. After due analysis, various mechanisms for dealing with those threats have been devised. One of the globally accepted mechanisms is that security can be ensured inside the software by integrating it in each of the generic phases of the development life cycle (Allen et al., 2008).

In recent years, a number of approaches, techniques and frameworks have been evolved over the time to address the aforementioned approach for designing, developing and deploying (relatively) secure software applications. It is also observed by the experts that requirements phase has proved to be the major bottleneck, but at the same time, this phase is the least technical and addressed among the other phases. As the vulnerabilities of software increases, system needs additional requirements for security aspects, which protects the software from vulnerabilities and makes the software more reliable. The requirements team's overall perspective of security goals, challenges, and plans need to be incorporated in the SRS that is shaped during the requirement's phase. Security requirements can be incorporated along with functional requirements in the SRS, which will in turn provide an advanced planning to conquer security related issues for later stages. After a thorough exploration of the related literature, following major security requirements have been collected (Peltier, 2002), which are needed to be addressed appropriately:

a. Authentication,
b. Access Controls and Rights,
c. Confidentiality,
d. Non-Repudiation,
e. Event Log and Audit Trails,
f. Data Classification Procedures,
g. Business Continuity and Disaster Recovery,
h. Virus Protection,
i. Backup & Recovery, and
j. Incident Management, Intrusion Detection and Forensic Analysis.

In our previous work, prescriptive techniques for the assurance of first four security requirements have been covered up to some extent (Mustafa et al., 2008, 2009) (Pandey & Mustafa, 2010, 2011). To extend this series one step further, in this paper, we highlight 'Event Log and Audit Trials'. 'Event Log and Audit Trials' specifies systems and procedures, which must be developed and implemented to monitor the activities related to the use of the Information System resources and services in order to safeguard information and computing resources from various business and environmental threats (National Thermal Power Corporation Ltd., 2006). A checklist is proposed for the verification of the major facts related with 'Event Log and Audit Trials' in the subsequent section.

Beyond this introduction on the background details, the remainder of this paper is organized as follows. Section II describes 'Event Log and Audit Trials'. The 'Checklist Approach' is discussed in Section III, while a Checklist for 'Event Log and Audit Trials' is proposed in Section IV.

'Implementation Mechanism' of the checklist is given in Section V. 'Tryout Results and Discussion' is provided in Section VI and 'Conclusions and Future Works' are given in Section VII. Finally, References are given in Section VIII.

EVENT LOG AND AUDIT TRAILS

In current interconnected but vulnerable world, there are numerous threats to the software systems and their allies. To safeguard information and computing resources from these threats, there must be efficient systems as well as procedures, which should be deployed to monitor the activities related to the use of the Information System resources and services (National Thermal Power Corporation Ltd., 2006). It is very imperative to ensure that the information on these systems is not revealed to unauthorized individuals, and that the integrity of the data is restored. In order to address all these pertinent issues, one of the major security requirements, namely, 'Event Log and Audit Trials' can be incorporated. To implement this security requirement, in every software system, there must be some procedures for maintaining the event logs and audit trails, which will in turn prevent and detect any unwanted tampering and use of its IT resources.

The users of IT resources should make sure the security of their respective software and should report any violations or breaches and any other unhealthy events without any delay to the concerned and competent authority. They have to be very alert and careful to catch up the suspected threats so that immediate action could be taken, accordingly. Detailed analysis of these logs may be done to conclude the results, if any on a periodical basis. Normally, event logs and audit trails are maintained for:

a. monitoring the appropriate usage of the IT resources;
b. detecting unwanted and malicious activity with the IT resources;
c. associating particular events with users; and
d. reporting on the effectiveness and compliance with security policies.

THE CHECKLIST APPROACH

Proposal of any methodology is quite appreciable but researchers should try to shape the steps very simple and ready to use directly by following the famous axiom 'simplicity is the power'. Any proposal is only used by the personnel of related community if they find its steps user-friendly and directly to use without a lengthy reading and understanding at their end. Unfortunately, it is observed that most of the methodologies do not fulfill these criterions and normally, not popularized among its targeted audience. To address this usability issue, one of the feasible solutions seems to be a checklist, which may ensure better process. Atomic checklists are generally used and have been found to be handy and quite fruitful (Pandey & Mustafa, 2010) in this concern.

Further, addressing the 'Event Log and Audit Trials', it becomes evident through the explanation of the researchers that a little work has been reported in the area; hence, it is viable to have a checklist for the same. But, as we said earlier, the checklist should be atomic in nature and can be easily usable by the community for secure software development. Taking into account the need and significance of 'Event Log and Audit Trials' checklist for building secure software, an integrated and prescriptive checklist is hereby proposed. Items of the checklist have been derived from the reported and well-verified practices of the literature and software industry, as evident from the item-wise references in most of the checkpoints.

AN EVENT LOG AND AUDIT TRAILS CHECKLIST

The distinctive objective of 'Event Log and Audit Trials' requirement is to maintain the logs of each activity related to the information resources and their periodical assessment and detailed analysis. Here, a checklist for 'Event Log and Audit Trials' is proposed based on the existing literature and the best practices used by the software industry. 'Event Log and Audit Trials' can be well implemented, which should have approved solution and may meet all or most of the following checklist items:

Table: 1

S. No.	Attribute	Check point Description	Status (Y/N/NA)
1.	Employees Accountability	Are all the employees responsible for maintaining a familiarity with the IT Security Policies and Procedures, Standards and Guidelines which are responsible for reporting any suspected activities, security breaches or violations (Tufts University, 2003)?	
2.	Security Breaches Reporting	Are employees, who suspect a security breach or violation communicating their concerns to their immediate supervisor (Chamoun & Hsu, 2002)? /* This individual must then evaluate the reported exceptions and refer all violations to the concerned Security Administrator. */	
3.	IT Resource Sabotage	Is there any IT resource misuse or suspected attempts to defeat IT resource safeguards, or attempts to gain unauthorized access to a resource (AT&T Laboratories, 2001)?	
4.	Compliance Monitoring	Is there any monitoring to ensure conformity to logical access policies and procedures (New Jersey State Legislature, 2002)? /* This is necessary to determine the effectiveness of measures adopted and to ensure conformity to logical access policies and procedures. */	
5.	Record Keeping of Audit Trails	Are audit trails recording exceptions and other security-related events kept for at least six months to assist in future investigations and access control monitoring (Sistem et al., 2006)?	
6.	Systems Monitoring	Are systems (used) monitored to ensure that users are only performing processes that have been explicitly authorized (UCISA, 2007)?	

		/* The level of monitoring required for individual systems should be determined by a separate risk assessment. */	
7.	Security Log Reports	Are security log reports generated for applications that have been determined to contain confidential/essential information (Sunset advisory Commission, 2009) (Darton College, 2005)?	
8.	Firewall Activation	Are auditing and logging enabled on the firewall to provide information about the activities through the firewall (Nelson David, 2007)? /* Because a large volume of data passes through the firewall, significant amount of hard drive space may be required to take the best advantage. This should be made available at all times. */	
9.	Internet Connection Periodic Review	Is there any periodic review of the Internet connection audit reports created on the firewall for any unusual/suspicious activities (National Thermal Power Corporation Ltd., 2006)?	
10.	Intrusion Detection Systems	Are intrusion detection systems deployed to perform real-time analysis of network traffic patterns to detect attempted attacks wherever technically feasible (National Thermal Power Corporation Ltd., 2006)? /* Without intrusion detection software/hardware, it becomes more difficult to detect attempts to breach security, as well as certain types of sophisticated attacks, thus increasing the likelihood of undetected compromise of system integrity and confidentiality. */	
11.	System Monitoring Tools	Are publicly accessible systems (e.g. external web sites) utilizing system monitoring tools that provide real-time alerts whenever suspicious user activity is detected (Peltier, 2002)?	
12.	Critical Data	Is host based IDS replaced on or close to systems where critical data is residing (National Thermal Power Corporation Ltd., 2006)?	
13.	Security Environment Periodic Review	Is there any periodic review of security environment for compliance with published Information Technology Security Policies and Procedures (National Thermal Power Corporation Ltd., 2006)? /* This must include an assessment of user practices, operations, and systems configurations. */	
14.	IT Users Practice Monitoring	Is there any proper monitoring of the practices of the IT users and third parties present at the company to ensure that a high level of compliance is maintained with published Information Technology Security Policies and Procedures, Standards and Guidelines (Peltier, 2010)?	

Based on these checkpoints, their corresponding attribute have been identified, which are given in the second column of the above checklist. A pictorial representation of the same is given as follows:

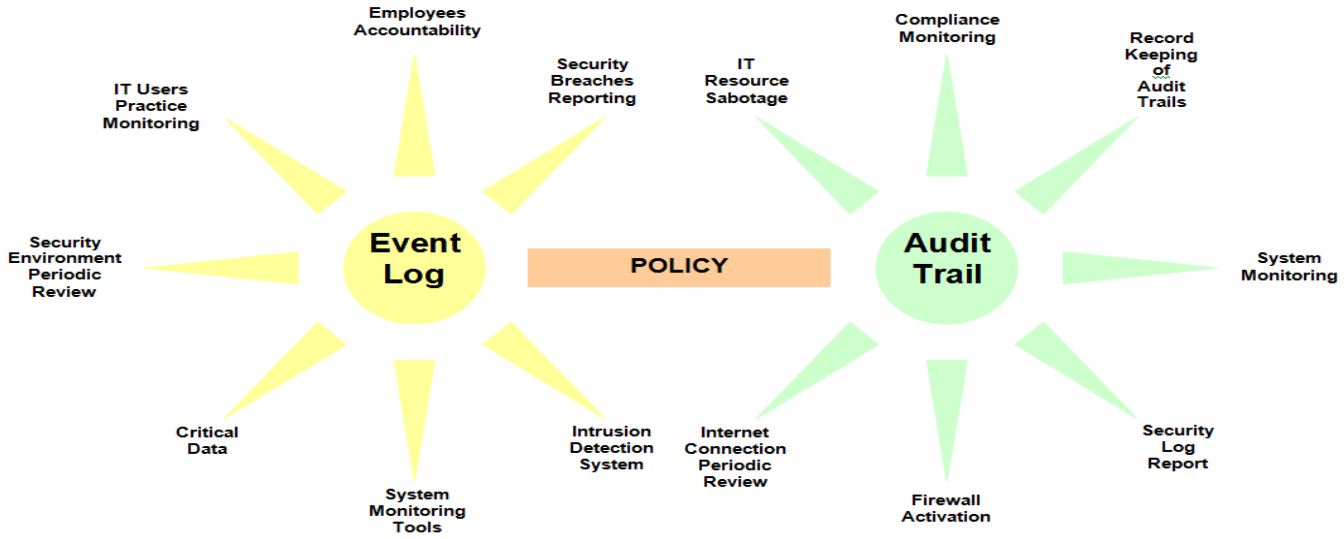

Figure 4.1: Attributes of Event Log and Audit Trail

IMPLEMENTATION MECHANISM

Following are the guidelines/steps for implementation of the proposed checklist:

a. First step will be the structured walkthrough by checklist filtering of the SRS, in which various checkpoints are provided for verification of the Event Log and Audit Trail requirement.
b. If any checkpoint is not pertinent to the project, it may be identified as 'NA'. This will not be taken into consideration.
c. For all the applicable checkpoints, requirement engineers may assess the compliance/ noncompliance of the checkpoints.
d. Further, compute the overall compliance status of the checklist in % with the help of all the compliance/non-compliance checkpoints. This will provide the exact status of the incorporation of the Event Log and Audit Trail requirement.
e. Based on the project need and other relevant factors like cost, effort etc., further course of action may be decided by the competent authorities.

TRYOUT RESULTS AND DISCUSSION

Proposal of any process/methodology is subject to the experimental validation and analysis of the results. There must be some experimental data, which should show the utility of the proposal. Keeping in mind the above fact, proposed checklist was applied to a real life project obtained from a software development company (on the request of the company, identity is concealed), and the final result of checklist assessment is computed on the basis of the total compliant, non-compliant and 'N/A' checkpoints as per prescribed implementation mechanism given in the above section. The assessment results are given as follows:

Table 6.1: Assessment Results

Total Checkpoints	Not Applicable (NA) Checkpoints	Total Available Checkpoints	Non-Compliant Checkpoints	Compliant Checkpoints	Overall Compliance Status
14	0	14	8	6	**42.86 %**

For the comparison of results, we demanded the results from the SRS provider. But as we know that in industry, this is highly informal; they were unable to provide such type of details. They could only provide a general opinion as saying that '*we are of the opinion that some significant points and procedures related to event log and audit trails are still missing and required to be incorporated'*. Their informal revelation about the final result confirms our formal results. From these evidences, the utility of the checklist is automatically ascertained up to some extent. However, it may not be sufficient to conclude so strongly about the effectiveness of the proposal but undoubtedly, up to some extent.

CONCLUSION AND FUTURE WORKS

The major contribution of this paper is the proposal of a checklist for the implementation of the 'Event Log and Audit Trials' requirements. The system will be stronger if it satisfies all or most of the checklist items given in the checklist. A detailed discussion of 'Event Log and Audit Trials' is given for the security assurance of the software. Being prescriptive in nature, the checklist can be easily implemented and it may reassure the integration of the security in the software from inception itself.

Future work may include the standardization of the results by strong validation of the proposed checklist on a large sample size. In addition, the weights of each attribute given in the checklist may also be computed to provide more accurate results. In future, we are also planning to develop some more checklists for the implementation of the other security requirements, based on the same pattern. This will help software developers and security experts for building secure software through easily implemental guidelines.

REFERENCES

[1]. Allen Julia H., Barnum Sean, Ellison Robert J., McGraw Gary, Mead Nancy R. (2008). Software security engineering: A guide for project managers. (pp. 6-8). Addison Wesley Professional.

[2]. AT&T Laboratories. (2001, April). Simple mail transfer protocol. Retrieved February 23, 2009 from http://www.ietf.org/rfc/rfc2821.txt

[3]. Chamoun Paula & Hsu Jennifer. (2002, March). Price water house coopers: Security services. Information Security Awareness Seminar for End Users. Dubai.

[4]. Darton College. (2005, December). Institutional security plan & report. Retrieved June 12, 2008, http://www.darton.edu/resources/pdfs/DC_Information_ Systems_ Use _Policies.pdf

[5]. Mustafa K., Pandey S. K., Rehman S. (2008, September). Security assurance by efficient access control and rights. CSI Communication, 32(6), 29-33.

[6]. Mustafa K., Rehman S., Pandey S. K. (2009, March): Confidentiality related security assessments. IEEE International Advance Computing Conference. Patiala.

[7]. National Thermal Power Corporation Ltd. (2006, July). Information security policies & procedures. [Technical report] Final V. 1.0.

[8]. Nelson David. (2007, February). Firewall information for windows media services 9 series. Retrieved July 7, 2008 from http://www.microsoft.com/win dows/windowsmedia/ forpros/serve/firewall.aspx

[9]. New Jersey State Legislature. (2002, May 20). Audit report of the office of information technology, e-government services. Retrieved June 12, 2008 from http://www.njleg.state.nj.us/legislativepub/auditor/99321.pdf

[10]. Pandey S. K. & Mustafa K. (2010, July-Aug). Security Assurance: An Authentication Initiative by Checklist. International Journal of Advanced Research in Computer Science. 1(2), 110-113.

[11]. Pandey S. K., Mustafa K. (2011, December). Security assurance by efficient non-repudiation requirements. International Conference on Communication Security and Information Assurance, New Delhi, India. (communicated)

[12]. Peltier Thomas R. (2002). Information security policies, procedures, and standards. CRC Press.

[13]. Peltier Thomas R. (2010). Information security risk analysis. CRC Press, Third Edition.

[14]. Sistem Perakaunan, Berkomputer Standard, Untuk Kerajaan Negeri. (2006, March). Information security policies and standards. SPEKS-POLSTD-01, Version 1.0.

[15]. Tufts University. (2003, January). Information technology resources security policy. Retrieved June 23, 2009 from http://uit.tufts.edu/?pid=431&c=105

[16]. UCISA. (2007, July 16). Information security toolkit. Retrieved February 12, 2008 from http://www.ucisa.ac.uk/publications/toolkit.aspx

