UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

User Behaviour Modeling in Web Application Security Monitoring

A Case for a University Student and Staff Web Portal Andrew

Mwaura Kahonge December

2013

A thesis submitted in fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Computer Science

Abstract

ts in security monitoring and auditability in the web environment and proposes a solution that allows holistic collection and consolidation of audit trail information. When an application is breached, audit trails provide important evidence about user actions and have remained an invaluable part of system security especially when performing security audits and forensic analysis. However, due to the nature of the web architecture, a single web application will have several sub-systems that generate their own distinct log records, which are later difficult to consolidate accurately. Further, the log records themselves may not contain all evidence necessary as a result of not integrating audit requirements into the log generation process.

As much as preventive measures such as intrusion detection systems are advancing, they still do not guarantee secure systems. Routine log reviews and analysis are helpful in continuous monitoring and also in identifying security incidents shortly after they have occurred. However, analyzing distinct log files from the separate subsystems in the web environment can only assist in measuring limited user activity as opposed to a broader or holistic perspective across the entire application. Previous efforts have focused on observing traffic between separate servers at the network level with the aim of reconstructing web and database protocol strings from network packets as well as through the use of parameterized views so that database servers get extra information from the web server.

The research questions in this thesis ask about the role of audit planning in context-action logging, how this influences auditability of the resultant audit trail and subsequently, whether there is an effect on security assurance. Additionally, they ask how to practically log and consolidate context and action as well as how to model user behaviour from a security perspective.

This thesis makes a number of c~ntributions. Continuous User Behaviour Monitoring Model (CUBMM) is the main contribution and it introduces the idea of integrating audit requirements of a web application into the processes of log generation, log consolidation, log analysis and behaviour modeling. CUBMM is formulated based on a conceptual framework that we build from theory. Additionally, we implement a server side logging tool (COGNITO) that is able to perform context-action

Further, we create a novel Behaviour Graph notation pecific user activity.

By following the experimental design as the overall research design, we apply CUBMM in our research process and embed COGNITO on a live web environment where it collects audit trail records for a number of days. To test auditability of the collected logs, we sample a set of system controls in the Web Portal and conduct a security audit with the help of several information security experts. The audit is guided by a questionnaire designed to test a set of hypotheses based on the conceptual framework. We then use our Behaviour Graph notation (BG) on the context-based log data gathered by COGNITO to describe activity in the system from a security perspective.

Overall, results obtained indicate increased levels of confidence of audit conclusions when the context-based log data is used as compared to traditional log data. Additionally, with the new logs it was possible to perform fine grained auditing where respondents could accurately determine the identity of users as well as other web context information for database transactions.

This thesis concludes that integration of audit requirements to the generation and consolidation of logs will increase auditability and subsequently improve security assurance and enhance behaviour monitoring in a web application.

Key words: *Auditability, Context, Action, Log Analysis and Consolidation, Behaviour Modeling, Security Assurance, Audit, Monitoring.*