JISSec 4(2) 2008

Journal of Information System Security

www.jissec.org

Editorial

This issue of the Journal of Information System Security presents three very interesting papers. The first paper is entitled 'Vulnerabilities and Patches of Open Source Software: An Empirical Study' and has been written by Kemal Altinkemer from the Krannert Graduate School of Management, Purdue University, Jackie Rees from the Krannert Graduate School of Management, Center for Education and Research in Information Assurance and Security (CERIAS) Purdue University and Sanjay Sridhar, Merrill Lynch, Merrill Lynch Financial Center. The authors discuss in the paper how they investigate specific security characteristics of open source and proprietary operating system software. Their analysis consists of several years' worth of collated data regarding software vulnerability. This was performed in order to determine if significant differences exist in terms of inter-arrival times of published vulnerabilities, mean time to release patches, type of vulnerability reported and respective severity of the vulnerabilities. The results demonstrate that open source and proprietary operating system software are each likely to report similar vulnerabilities and that open source providers are marginally quicker in releasing patches for problems identified in their software.

The second paper entitled 'MILD DSS - Conceptual Architecture, Validation and Representation' is written by Khalid Abdullah Fakeeh from the Department of Computer Science, King Abdul Aziz University, Jeddah, Saudi Arabia and Sohail Asghar from the Clayton School of Information Technology, Monash University, Melbourne, Australia. The authors tackle the subject of Disaster Management, which can be described as a complex and highly multi-disciplinary area. Their concept involves the MILD DSS; which stands for 'A MultI-Layered Architecture for Disaster Management Decision Support Systems'. The goal of the MILD DSS is to produce an integrated model based on a disaster scenario. The necessity of decision-making in disaster management often requires a decision support system to fulfill dynamic and rapidly changing decision needs. The MILD DSS is dedicated to supporting decision-making in disaster management and is designed for such applications. The authors propose that the design of the MILD DSS improves the efficiency and

reusability of decision support systems for disaster management by considering the commonalities of decision support needs and the environmental as an essential and common factor with the ability to change the severity of a disaster.

The third paper is entitled 'Just Trying to Be Friendly: A Case Study in Social Engineering', and is written by Doug White from the Roger Williams University and Alan Rea from the Western Michigan University. The authors evaluate a case that can be used in networking or general security courses. They propose how security policies and organizational procedures that do not take into account socio-technical approaches will ultimately not protect organizational systems in today's Digital Economy. The case examines this scenario and focuses on how a security consultant tries to determine a technical solution only to find that the answer is in the social engineering realm. This case focuses on developing techniques to determine, evaluate, and then thwart social engineering mechanisms through the use of user education and socio-technical security policies and procedures.

These three papers provide valuable information regarding Information System Security and can provide some insight and knowledge into this rapidly expanding field of research.

Gurpreet Dhillon
Editor-in-Chief