World Academy of Science, Engineering and Technology
International Journal of Electrical and Information Engineering
Vol:8, No:03, 2014

Software Vulnerability Markets: Discoverers and Buyers

Authors : Abdullah M. Algarni, Yashwant K. Malaiya

Abstract : Some of the key aspects of vulnerability-discovery, dissemination, and disclosure-have received some attention recently. However, the role of interaction among the vulnerability discoverers and vulnerability acquirers has not yet been adequately addressed. Our study suggests that a major percentage of discoverers, a majority in some cases, are unaffiliated with the software developers and thus are free to disseminate the vulnerabilities they discover in any way they like. As a result, multiple vulnerability markets have emerged. In some of these markets, the exchange is regulated, but in others, there is little or no regulation. In recent vulnerability discovery literature, the vulnerability discoverers have remained anonymous individuals. Although there has been an attempt to model the level of their efforts, information regarding their identities, modes of operation, and what they are doing with the discovered vulnerabilities has not been explored. Reports of buying and selling of the vulnerabilities are now appearing in the press; however, the existence of such markets requires validation, and the natures of the markets need to be analysed. To address this need, we have attempted to collect detailed information. We have identified the most prolific vulnerability discoverers throughout the past decade and examined their motivation and methods. A large percentage of these discoverers are located in Eastern and Western Europe and in the Far East. We have contacted several of them in order to collect first-hand information regarding their techniques, motivations, and involvement in the vulnerability markets. We examine why many of the discoverers appear to retire after a highly successful vulnerability-finding career. The paper identifies the actual vulnerability markets, rather than the hypothetical ideal markets that are often examined. The emergence of worldwide government agencies as vulnerability buyers has significant implications. We discuss potential factors that can impact the risk to society and the need for detailed exploration.

Keywords : risk management, software security, vulnerability discoverers, vulnerability markets
Conference Title : ICISS 2014 : International Conference on Information Systems Security
Conference Location : Madrid, Spain
Conference Dates : March 27-28, 2014