Abstract

Software vulnerability detection is an active area of research in the software engineering domain. This is partly due to the continuous disclosure of security vulnerabilities. Although previous studies demonstrate the usefulness of employing several detection techniques, models, tools in detecting software vulnerabilities, the improvement of effectiveness of these detection models and tools is still a major challenge to researchers and practitioners. Cascaded Refinement Network (CRN) is novel model that has been successfully applied in several domains of studies such as image analysis, however its application to the field of vulnerability analysis has not been investigated. Motivated by the model effectiveness in these fields of studies, we investigate its feasibility within the domain of vulnerability detection using a theoretical framework. The analysis involves first presenting a general overview of the static
analysis tools, and then an overview of the theoretical framework for vulnerability detection based on the CRN. The preliminary findings show that the concept is feasible within the domain of vulnerability detection.

References

17. N. Ayewah, D. Hovemeyer, J. D. Morgensthaler, J. Penix, and W. Pugh, "Using static


Index Terms

Computer Science Software Engineering

Keywords

Software Vulnerability; Static Analysis; Cascaded Refinement Network