Comprehensive Analysis on Secure Software Development Practices

Zaki Ahmad Rathore
Computer Science
University of Central Florida
Orlando, Florida, United States
za535945@ucf.edu

Shishir Singh
Computer Science
University of Central Florida
Orlando, Florida, United States
Shishir.singh@ucf.edu

Vigneshwar Sundararajan
Cybersecurity and Privacy
University of Central Florida
Orlando, Florida, United States
vi126747@ucf.edu

PROPOSAL

In today's interconnected world, where digital systems underpin almost every aspect of our lives, the security of software has never been more critical.

Data leaks, financial losses, and even threats to national security can result from software flaws. The techniques used by bad actors to exploit vulnerabilities evolve along with technology. Organizations must establish and continuously enhance safe software development processes to combat this changing threat landscape. In this proposal, a thorough study effort that will survey, examine, and improve secure software development processes across several businesses is described.

PROBLEM STATEMENT

Despite the growing significance of secure software development, we still lack a thorough knowledge of how these approaches can be used in actual situations. Many businesses find it difficult to stay on top of new dangers and developing best practices. This study tackles the urgent need to evaluate the state of current safe software development techniques, pinpoint weaknesses, and offer suggestions for advancement.

GOALS

1. Evaluating the adoption and implementation of secure coding standards in software development processes.
2. Analyze how security controls are incorporated throughout the entire process of developing software, from design and coding to testing and deployment.
3. Determine prevalent security weaknesses and evaluate the efficiency of businesses' use of mitigation techniques.
4. Examine how security awareness and training programs affect the number of security incidents and the overall level of software security.

LITERATURE REVIEW

A thorough analysis of the existing literature demonstrates the crucial role that secure software development approaches play in defending against online threats. Best practices, frameworks, and recommendations have all been put out. However, there is a lack of research that provides a thorough survey and analysis of how these methods are being used across a range of businesses. By offering practical information about the state of secure software development, this study seeks to close that gap.

METHODOLOGY

A mixed-methods strategy will be used to collect data for this study, integrating quantitative and qualitative methods:

QUANTITATIVE DATA COLLECTION

Surveys: To ensure participation from different firm sizes and areas, a survey will be developed and disseminated to software development teams across broad industries. The poll will ask questions regarding secure coding techniques, security integration into development workflows, and training initiatives.

Sampling: Organizations of all sizes and sectors will be sought out **to** obtain a representative sample.

QUALITATIVE DATA COLLECTION

Semi-Structured Interviews: For semi-structured interviews, about 3 business professionals will be chosen using purposive sampling. These interviews will provide further light on the difficulties and achievements of developing secure software.

DATA ANALYSIS

Using statistical software, quantitative survey data will be examined for trends, correlations, and patterns in the responses. Thematic analysis will be used to find recurrent themes and insights in qualitative data from interviews. To guarantee data veracity, results from both methodologies will be triangulated.

RESEARCH DESIGN

This study uses a cross-sectional research design and gathers data over a six-month period. It is critical to recognize any drawbacks, such as the potential for self-reporting biases in survey replies and the study's emphasis on medium- to large-sized businesses.

CONCLUSION

This research project is poised to make significant contributions to the field of secure software development practices. By offering a real-world assessment of the current state of these practices across industries, it aims to pinpoint areas in need of improvement and

provide actionable recommendations. Ultimately, the findings will enhance the security posture of organizations and contribute to the broader cybersecurity landscape as we strive to create a safer digital world.

REFERENCES

.

[1] Lt. Dr. P. C. Behera and C. Dash, An approach for secure software development life cycle in small software firms, https://www.researchgate.net/publication/353306538_An_Approach_for_Secure_Software_Development_Life_Cycle_in_Small_Software_Firms.

[2] W. Umeugo, Secure Software Development Lifecycle: A case for adoption in software smes, https://www.researchgate.net/publication/368737283_SECURE_SOFTWARE_DEVELOPMENT_LIFECYCLE_A_CASE_FOR_ADOPTION_IN_SOFTWARE_SMES.

[3] H. Assal and S. Chiasson, Security in the Software Development Lifecycle - USENIX, https://www.usenix.org/system/files/conference/soups2018/soups2018-assal.pdf.