Vulnerability Perceptions and Practices in Software Development Teams

Arpita Ghosh
University of North Carolina at Charlotte

Lipsarani Sahoo
University of North Carolina at Charlotte

Heather Richter Lipford
University of North Carolina at Charlotte

Abstract

In today's software development landscape, ensuring robust security practices is crucial due to the high risk of security incidents resulting from software vulnerabilities. Researchers and industry practitioners have recommended a greater organizational focus on security, regular security testing, and other vulnerability mitigation practices. Many organizations do now have a robust secure software development life cycle. We seek to extend prior research by examining the practices and perceptions of teams that are in organizations with standard vulnerability management practices. We seek to identify common perceptions, practices and challenges of teams where security is already considered an important component of software development, as well as where and how teams vary in their practices. Our results will provide evidence of where teams are still struggling with vulnerability prevention and mitigation to provide recommendations to further reduce security risks.

1 Introduction and Background

Software vulnerabilities are a continued concern in software development, as they are the root cause of many security breaches and attacks. For example, the U.S. Department of Homeland Security estimates that 90% of security incidents result from exploits against defects in software, with a significant proportion of both in-house and vendor software failing to meet critical security standards like the OWASP Top 10 [3]. Security is still often overshadowed by functional requirements, thus increasing vulnerability risks [1, 2, 4]. Previous research in software security has focused on two sets of factors that are related to vulnerabilities in applications. First, are factors inherent to the software itself, with studies exploring how the number of security vulnerabilities can be correlated to an application's size, age, language, and platform for example [6]. Other research has examined factors related to developer and organizational perceptions and practices, such as security training, vulnerability handling, and team dynamics.

The outcomes of much of this research are a set of recommended software security practices, including organizations emphasizing software security, regular use of vulnerability detection tools, and integration of security champions into development teams. Yet even with these practices, teams may still fail to adequately prevent and detect software vulnerabilities. This may be due to individual perceptions and knowledge, team dynamics and culture, a lack of organizational incentives towards security, or other factors. Thus, in this research, we seek to deepen our understanding of how software development teams perceive and practice software security by focusing specifically on organizations with a strong security focus and standard security procedures. By identifying continued challenges we seek to further help organizations and teams improve their vulnerability management practices, lowering the likelihood of security flaws in their code.

2 Methodology

This qualitative, interview study explores the vulnerability perceptions and practices of members of software development teams. Our recruitment process focused on software developers from organizations with a strong security focus, such as those with vulnerability management teams, and standard security procedures and training. We focus on financial organizations and large enterprises in particular, as they are typically more focused on security, often being early adopters of the latest security tools and practices. These companies are frequently targeted by attackers due to the sensitive nature of their data and operations. For example, a recent report by

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

IBM (2023) highlighted that the financial sector experienced the highest average cost of a data breach, amounting to $5.97 million per incident [5]. This makes them an ideal subject for studying the effectiveness and perceptions of security practices within security-conscious environments.

We recruited participants via our professional and personal networks, word of mouth, and snowball sampling. To date, we have interviewed 34 software developers. Most work as a software developer in an Agile type process, with titles such as Frontend Software Developer or Full Stack Developer. A few had other roles in teams, including a project manager, team lead, and development support. Their experience ranged from 1 years to 15 years.

Interviews were conducted via Zoom to gain insights into software security practices, including secure development, code review, security training, and team dynamics. Each interview lasted about 45 minutes, and participants received a $50 gift card. The interviews were recorded, transcribed, and anonymized for analysis. A qualitative thematic analysis, following a grounded theory approach, was used to identify themes. The ongoing analysis has yielded the preliminary results summarized below.

3 Results

Our analysis has focused on the common practices and perceptions of software development teams, along with variations between teams that indicate better, or worse, security practices. Key themes include:

3.0.1 SDLC Practices

The significance of incorporating security throughout the Software Development Life Cycle (SDLC), including routine testing and monitoring, was emphasized by our participants' beliefs and practices. Static and dynamic scanning are common practices, yet many teams limited these scans to code check-in or in response to an incident. Participants reported being overwhelmed by false positives in the scan reports, and with prioritizing mitigation. They also focused heavily on functional testing with little attention on additional security-related testing. However, teams that were more proactive conducted regular vulnerability scans, and had immediate response mechanisms in place with an individual designated to review scanning and testing results.

Most teams reported that peer code reviews were standard. Again, however, these reviews tended to focus on functionality with limited attention to application security. A few teams reported that they employ more rigorous processes, adhering to updated coding standards and utilizing comprehensive checklists to ensure a consistent focus on security and enforcement of standards.

3.0.2 Security Training

Security training is a standard component of large organizations, typically conducted at an organizational or enterprise level rather than being specific to individual projects, programming languages, or offensive/defensive strategies. Some participants mentioned that their teams have developed their own security training sessions, such as knowledge transfer (KT) sessions. Additionally, some individuals noted that their proactive and self-motivated nature drives them to participate in these trainings. It is important to note, however, that these training sessions are generally theoretical and not hands-on.

3.0.3 Team Dynamics and Incentives

Cohesive team dynamics were critical for maintaining a strong security posture. Teams with stable compositions, strong interpersonal relationships, and active managerial involvement felt that they were more effective in implementing security practices. In contrast, teams experiencing high turnover and disengaged management reported that they struggled with maintaining consistent security practices, leading to fragmented approaches to security. Aligning incentives with security objectives was also recognized as an effective way to motivate developers. A few teams explicitly recognized and rewarded security efforts, such as a shout-out in a team call, creating a culture that valued security. In other teams, greater emphasis was placed on functionality and speed over security, resulting in less motivation for developers to invest time in security practices.

Cohesive team dynamics were critical for maintaining a strong security posture. Teams with stable compositions, strong interpersonal relationships, and active managerial involvement felt that they were more effective in implementing security practices. In contrast, teams experiencing high turnover and disengaged management reported that they struggled with maintaining consistent security practices, leading to fragmented approaches to security. This aligns with the observations of Haney et al. [4], who found that security practices are often influenced by team dynamics and individual perceptions.

4 Implications and Conclusion

Our preliminary analysis indicates that even in organizations with standard procedures for vulnerability management, practices can vary, potentially leading to greater security risks. Our results can provide guidance for improving application security, by identifying practices that organizations can be monitor and implement, such as more hands-on training relevant to the particular application, checklists for peer review, and recognition for developers who prevent vulnerabilities.

References

[1] Latifa Alzahrani and Kavita Panwar Seth. The impact of organizational practices on the information security management performance. *Information*, 12(10):398, 2021.

[2] Larissa Braz and Alberto Bacchelli. Software security during modern code review: The developer's perspective. In *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*, pages 810–821, 2022.

[3] Cybersecurity and Infrastructure Security Agency (CISA). Software assurance information sheet, n.d. Accessed: 2024-05-22.

[4] Julie M Haney and Wayne G Lutters. " it's {Scary... It's}{Confusing... It's} dull": How cybersecurity advocates overcome negative perceptions of security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 411–425, 2018.

[5] IBM. Half of breached organizations unwilling to increase security spend despite soaring breach costs, 2024. IBM Report.

[6] Yuancheng Li, Longqiang Ma, Liang Shen, Junfeng Lv, and Pan Zhang. Open source software security vulnerability detection based on dynamic behavior features. *Plos one*, 14(8):e0221530, 2019.