

Understanding Security Challenges Across Software Development Environments

Houda Naji

December 3, 2025

Securing the software development lifecycle is increasingly critical, as vulnerabilities can cause substantial financial, operational, and reputational damage. Beyond technical challenges, security is shaped by organizational processes, collaboration, and role responsibilities. This dissertation investigates how security is understood, prioritized, and enacted across diverse roles, development practices, and technological contexts, focusing on agile software development and disruptive technologies such as blockchain ecosystems. Drawing on three empirical studies combining qualitative and quantitative methods, including interviews, requirement-writing exercises, developer code reviews, and large-scale analyses, the research examines collaboration between developers and security experts, the role of product managers in shaping security requirements, and security practices in high-stakes blockchain environments such as Solana.

Across these studies, recurring patterns emerge. Security is often deprioritized, responsibilities are diffused, and collaboration barriers amplify risks. Teams frequently adopt reactive approaches, and organizational structures strongly influence security integration. The findings highlight the systemic nature of secure software development, emphasizing the need for clear accountability, cross-role collaboration, and structural support to embed security as a shared priority. By clarifying how roles, organizational processes, and technological contexts affect security practices, this dissertation provides actionable insights for designing frameworks and tools that proactively enhance security across both traditional and emerging software development environments.

Sicherheitsherausforderungen in verschiedenen Softwareentwicklungsumgebungen verstehen

Houda Naji

December 3, 2025

Die Absicherung des Softwareentwicklungszyklus wird zunehmend entscheidend, da Schwachstellen erhebliche finanzielle, operative und reputationsbezogene Schäden verursachen können. Sicherheit stellt dabei nicht nur eine technische Herausforderung dar, sondern wird stark von organisatorischen Prozessen, Zusammenarbeit und Rollenverantwortlichkeiten geprägt. Diese Dissertation untersucht, wie Sicherheit in verschiedenen Rollen, Entwicklungspraktiken und technologischen Kontexten verstanden, priorisiert und umgesetzt wird, mit Schwerpunkt auf agiler Softwareentwicklung und disruptiven Technologien wie Blockchain-Systemen. Auf Basis von drei empirischen Studien mit qualitativen und quantitativen Methoden, darunter Interviews, Aufgaben zur Anforderungserstellung, Code-Reviews durch Entwicklerinnen und Entwickler sowie groß angelegte Analysen, wird die Zusammenarbeit zwischen Entwicklern und Sicherheitsexperten, die Rolle von Product Managern bei der Definition von Sicherheitsanforderungen und Sicherheitspraktiken in risikobehafteten Blockchain-Umgebungen wie Solana untersucht.

In allen Studien zeigen sich wiederkehrende Muster. Sicherheit wird häufig nachrangig behandelt, Verantwortlichkeiten sind diffus verteilt und Barrieren in der Zusammenarbeit verstärken Risiken. Teams verfolgen oft reaktive Ansätze, während organisatorische Strukturen die Integration von Sicherheit stark beeinflussen. Die Ergebnisse verdeutlichen die systemische Natur sicherer Softwareentwicklung und unterstreichen die Notwendigkeit klarer Verantwortlichkeiten, bereichsübergreifender Zusammenarbeit und struktureller Unterstützung, um Sicherheit als gemeinsame Priorität zu verankern. Durch die Analyse von Rollen, organisatorischen Prozessen und technologischen Kontexten liefert diese Dissertation praxisnahe Erkenntnisse für die Gestaltung von Rahmenwerken und Werkzeugen, die Sicherheit proaktiv in traditionelle und neue Entwicklungsumgebungen integrieren.