

Software Security during Modern Code Review: The Developer's Perspective

Larissa Braz, Alberto Bacchelli

30th ACM Joint European Software Engineering Conference and Symposium on the
Foundations of Software Engineering (ESEC/FSE 2021)

発表者：松尾 和輝

背景

- ソフトウェアの脆弱性
 - ソフトウェアコードに見られるセキュリティ上の欠陥, 不具合, 弱点のこと
 - 攻撃者^[23]によって悪用され, ソフトウェアシステムの利害関係者に損害を与える可能性がある^[28]
- 脆弱性を回避するために, 組織はソフトウェア開発の初期段階 (コードレビュー等) で発見するようになってきている^[1]
- コードレビューは, 脆弱性を早期に発見し, 修正するための重要な手法である ^[41, 67]

[1] 2020. GitLab: Mapping the DevSecOps Landscape - 2020 Survey. <https://about.gitlab.com/developer-survey>.

[23] K. Dempsey, P. Eavy, and G. Moore. 2017. Automation Support for Security Control Assessments. Technical Report. Technical Report NISTIR 8011, National Institute of Standards and Technology.

[28] The OWASP Foundation. Last accessed March 2022. OWASP Foundation. <https://owasp.org/>

[41] G. McGraw. 2004. Software security. IEEE Security Privacy 2, 2 (2004), 80–83.

[67] C. Thompson and D. Wagner. 2017. A Large-Scale Study of Modern Code Review and Security in Open Source Projects. In Proceedings of the International Conference on Predictive Models and Data Analytics in Software Engineering. 83–92.

背景

- 以前の研究[49, 73, 76, 77]では、安全な開発の採用が限られていることを報告、調査し、セキュリティに対する開発者の視点を調査している
- コードレビューにおけるセキュリティについては不明である
 - 脆弱性を回避するために、なぜ組織はソフトウェア開発の初期段階で発見するようになってきたのかがわからない

[49] A. Poller, L. Kocksch, S. Trpe, F. Epp, and K. Kinder-Kurlanda. 2017. Can security become a routine? A study of organizational change in an agile software development group. In Proceedings of the conference on computer supported cooperative work and social computing. 2489–2503.

[73] I. Woon and A. Kankanhalli. 2007. Investigation of IS professionals' intention to practise secure development of applications. International Journal of HumanComputer Studies 65, 1 (2007), 29–41.

[76] S. Xiao, J. Witschey, and E. Murphy-Hill. 2014. Social influences on secure development tool adoption: why security tools spread. In Proceedings of the Conference on Computer supported cooperative work and social computing. 1095– 1106.

[77] J. Xie, H. Lipford, and B. Chu. 2011. Why do programmers make security errors?. In Proceedings of the Symposium on Visual Languages and Human-Centric Computing. 161–164.

目的とアプローチ

- 目的

- コードレビュー時のソフトウェアセキュリティの評価に関する開発者の視点と、このプロセスに対して企業やプロジェクトが提供する支援について理解すること

- アプローチ

- 半構造化インタビューと、アンケートを実施
- それらの結果をもとに分析

※セキュリティを確保すること = 脆弱性に対処すること と定義 [51]

半構造化インタビュー

- 経験豊富なプロのソフトウェア開発者10人に対して、インタビューを実施
- 質問の流れ
 - (1)導入と背景の説明, 人口統計に関する質問
 - (2)コードレビューの質問

なぜコードレビューを行うのか, レビューの際にどのような問題を探すのか等
 - (3)セキュリティに関する質問

「ソフトウェアの脆弱性」という言葉を知っているか, コードをレビューするときにセキュリティを考慮するか等
 - (4)締め

アンケート

- 329名の方がアンケートに回答
 - 自由形式, 多肢選択式, 単一選択式, リッカード尺度など
 - 有効な回答が得られた182名の結果をもとに分析
- アンケートの内容
 - (1) ウェルカムページ
 - (2) 資格に関する質問
 - (3) コードレビューの経験と実践
 - (4) コードレビューにおけるセキュリティに関する知識と実践
 - (5) 人口統計
 - (6) フィードバックとクロージング

リサーチクエスチョン

RQ1.コードレビューにおけるソフトウェアセキュリティの確保について、現在の開発者の考えはどのようなものか？

RQ2.企業やプロジェクトは、コードレビュー時のセキュリティ評価をどの程度サポートしているか？

RQ3.最新のコードレビューにおいて、セキュリティを確保するために経験する主な課題は何か？

RQ1 | 結果

RQ1. セキュリティの確保に関する開発者の考え

- アンケート結果

Q.コードレビュー時に何を重視するか

- セキュリティに言及したのは9人のみ
- 一方で、コードの他の非機能的な品質が頻繁に言及された

Q.コードレビュー時に脆弱性を考慮しているか

- 111人の回答者がレビュー時に常に考慮していると回答

- インタビューでも同様の傾向が見られた

コードレビューにおいてセキュリティを確保することの重要性を認識しているが、
セキュリティが主要な優先事項の1つではない

RQ1 | 結果

RQ1. セキュリティの確保に関する開発者の考え

- インタビュー結果

- Q.責任の所在について

- 7人が、チームの責任であると想定

- 「他の人が対処しているから問題なし」

- 「セキュリティを考慮するのはバックエンドの開発者だろう」

- 「セキュリティを考慮するのはフロントエンドの開発者だろう」

- 「コードは外に出ないから問題なし」

- アンケートでは、ほとんどの人が自分の責任であると回答

開発するアプリケーションのセキュリティに対する思い込みから、
コードレビューの際にセキュリティが無視されやすい

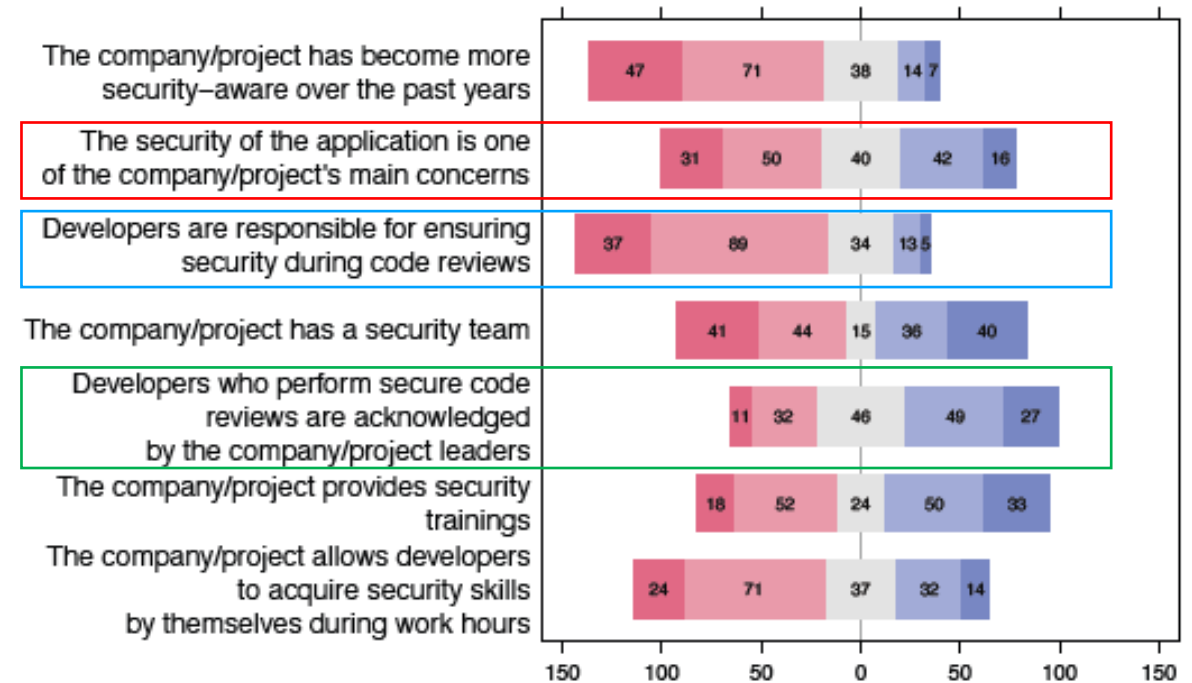
RQ2 | 結果

RQ2. セキュリティの確保に関する企業の考え

アンケート結果

- 企業やプロジェクトがセキュリティを主な関心事として考えていると回答した人は**45%**
- 開発者は自分の会社/プロジェクトでコードレビュー時にセキュリティを確保する責任があると回答した人は**69%**
- 企業やプロジェクトリーダーは、安全なコードレビューを行う開発者を認めているように感じている人は**24%**

(2) Please rate the following statements about the company/project you mainly develop for:



コードレビューの際にセキュリティを確保することを期待されているが、それを実行しても、企業/プロジェクトリーダーから認められていない

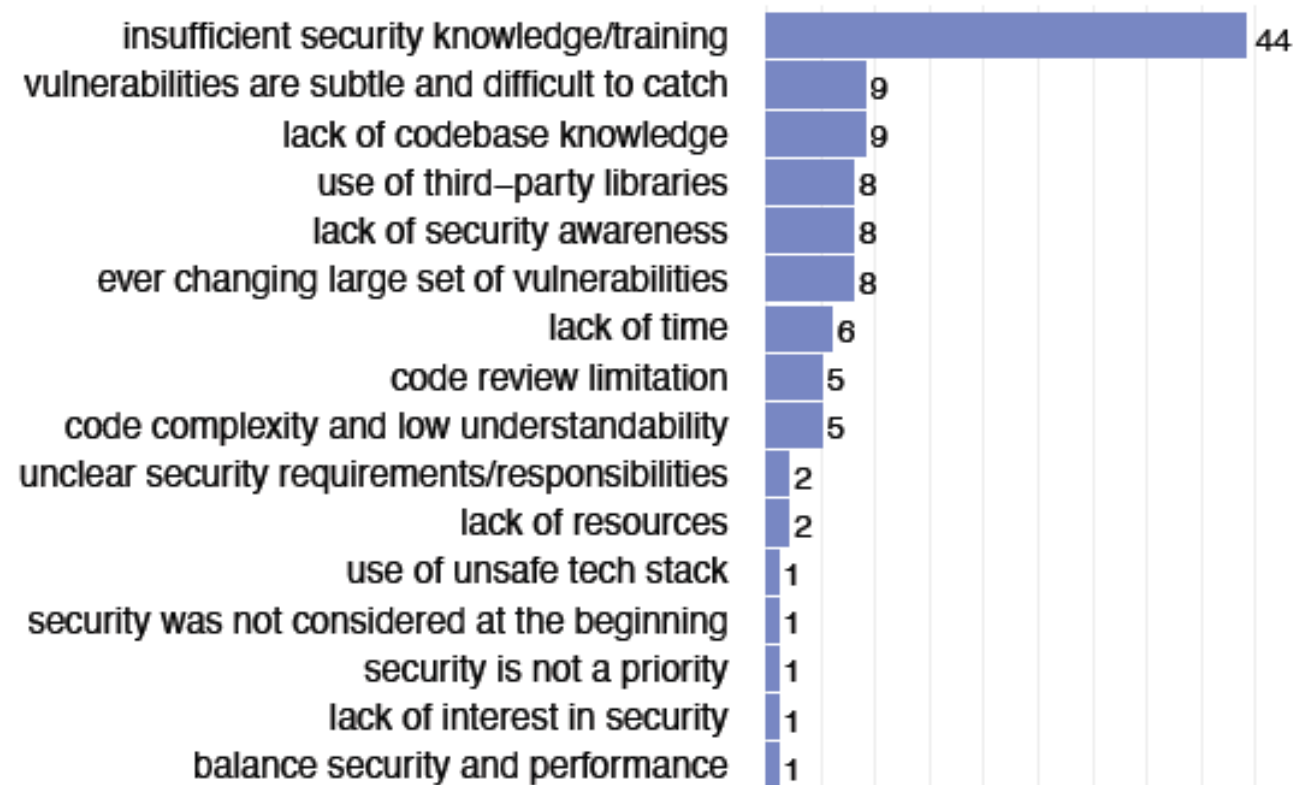
RQ3 | 結果

RQ3. セキュリティを確保するための課題

Q.コードレビュー時にセキュリティを確保することは難しいか

- 7人のインタビュー参加者が同意
 - アンケートでは, 51%が同意
- 知識不足, 想定される脆弱性や攻撃パターンの多さ, 時間的制約, 人的要因などが主な課題として挙げられた

コードレビュー時に開発者が直面する
セキュリティに関する課題



知識不足のためにセキュリティを確保することが難しい

まとめ

- 目的

- コードレビュー時のセキュリティに関する開発者や企業の意識調査

- 結果

- セキュリティを確保することの重要性を認識しているが、セキュリティは主要な優先事項の1つではない
- 企業は、セキュリティを確保することをあまり評価していない
- 知識不足がセキュリティを確保することを困難としている

所感

- 企業は、セキュリティを確保することをあまり評価していないのは意外だった
 - セキュリティを確保することは当たり前だと思われる？
 - 経営者と技術者との認識の間にギャップがある？
 - セキュリティに関する知識を得ることは困難であるにもかかわらず、当然のように求められる
 - 企業側が、セキュリティの確保をサポートするように移行するか、できるうちにセキュリティに関する知識を獲得することが重要だと思った

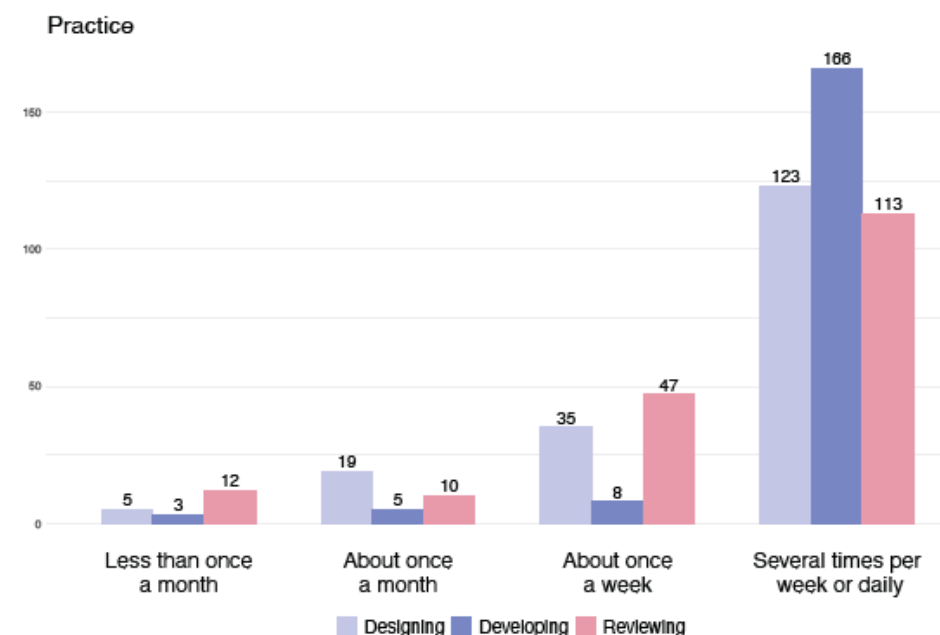
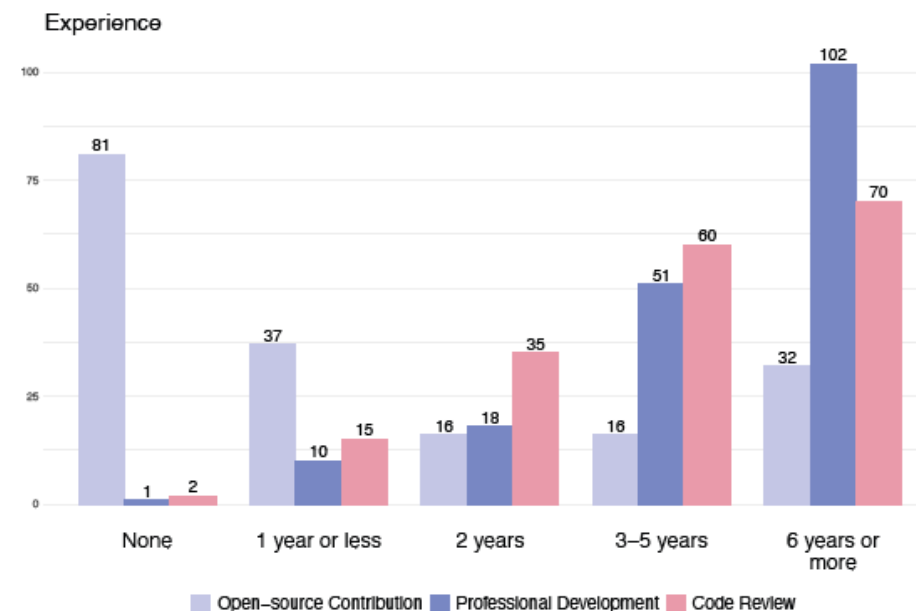
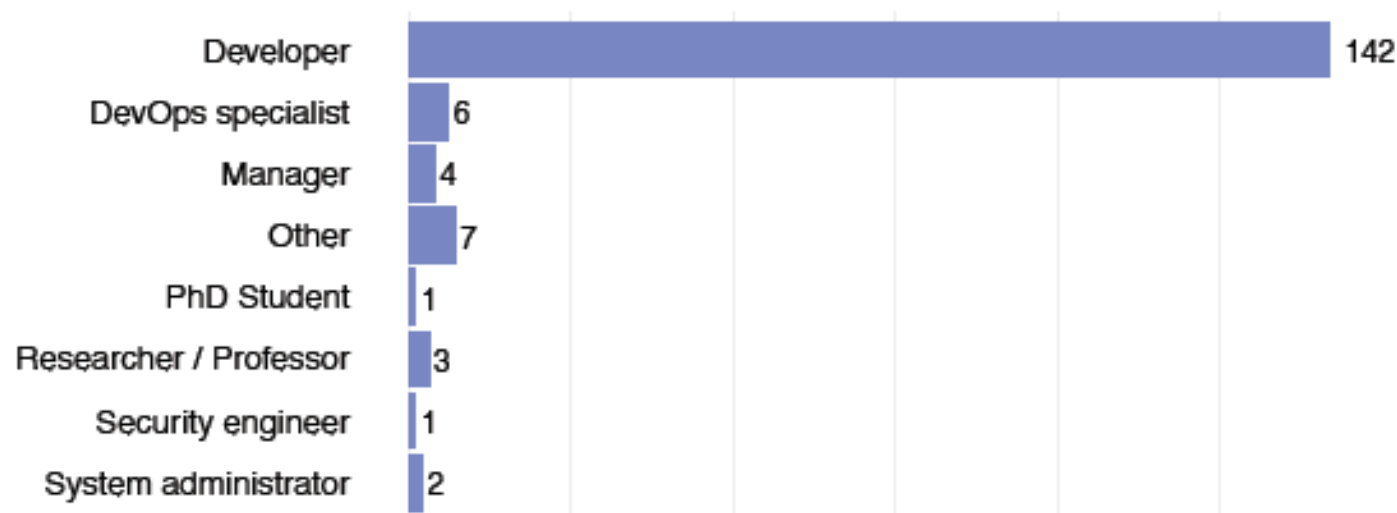
補足資料

インタビュー参加者に関する情報

ID	Domain	Company/ Project	Experience (in years)	Security Expert
<i>I1</i>	Indust./OSS	Mid SW Comp.	9	✓
<i>I2</i>	Industry	Startup	1	
<i>I3</i>	Industry	Large SW Comp.	1	
<i>I4</i>	Industry	Large SW Comp.	11	
<i>I5</i>	Industry	Startup	1	
<i>I6</i>	Industry	Large SW Comp.	13	
<i>I7</i>	Industry	Mid SW Comp.	6	
<i>I8</i>	Industry	Mid SW Comp.	7	
<i>I9</i>	Industry	Startup	2	
<i>I10</i>	Industry	Large SW Comp.	8	

アンケート回答者の人口統計

- アンケート回答者の役職（左） および経験（右上）と実務（右下）を表した図



インタビュー内容

