Citation:
S. Amft, S. Höltervennhoff, R. Panskus, K. Marky and S. Fahl, "Everyone for Themselves? A Qualitative Study about Individual Security Setups of Open Source Software Contributors," in 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2024 pp. 249-249.
doi: 10.1109/SP54263.2024.00182

Link:
https://www.computer.org/csdl/proceedings-article/sp/2024/313000a249/1WPcZ798V1K

Abstract:
To increase open-source software supply chain security, protecting the development environment of contributors against attacks is crucial. For example, contributors must protect authentication credentials for software repositories, code-signing keys, and their systems from malware. Previous incidents illustrated that open-source contributors struggle with protecting their development environment. In contrast to companies, open-source software projects cannot easily enforce security guidelines for development environments. Instead, contributors' security setups are likely heterogeneous regarding chosen technologies and strategies. To the best of our knowledge, we perform the first in-depth qualitative investigation of the security of open-source software contributors' individual security setups, their motivation, decision-making, and sentiments, and the potential impact on open-source software supply chain security. Therefore, we conduct 20 semi-structured interviews with a diverse set of experienced contributors to critical open-source software projects. Overall, we find that contributors have a generally high affinity for security. However, security practices are rarely discussed in the community or enforced by projects. Furthermore, we see a strong influence of social mechanisms, such as trust, respect, or politeness, further impeding the sharing of security knowledge and best practices. We conclude our work with a discussion of the impact of our findings on open-source software and supply chain security, and make recommendations for the open-source software community.