Jan Jürjens, Kurt Schneider (Hrsg.): Software Engineering 2017,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 57

"Jumping Through Hoops": Why do Java Developers Struggle With Cryptography APIs?

Sarah Nadi[1] Stefan Krüger[2] Mira Mezini[3] Eric Bodden[4]

Abstract: To protect sensitive data processed by current applications, developers, whether security experts or not, have to rely on cryptography. While cryptography algorithms have become increasingly advanced, many data breaches occur because developers do not correctly use the corresponding APIs. To guide future research into practical solutions to this problem, we perform an empirical investigation into the obstacles developers face while using the Java cryptography APIs, the tasks they use the APIs for, and the kind of (tool) support they desire. We triangulate data from four separate studies that include the analysis of 100 StackOverflow posts, 100 GitHub repositories, and survey input from 48 developers. We find that while developers find it difficult to use certain cryptographic algorithms correctly, they feel surprisingly confident in selecting the relevant cryptography concepts (e.g., encryption vs. signatures). We also find that the APIs are generally perceived to be too low-level and that developers prefer more task-based solutions.

Keywords: Cryptography, API misuse, empirical software engineering

[1] University of Alberta
[2] Paderborn University
[3] Technische Universität Darmstadt
[4] Heinz Nixdorf Institut, Paderborn University & Fraunhofer IEM