Systematisches Testen beim Einsatz kryptographischer Verfahren in der Entwicklung sicherer Software

Bachelorarbeit ggf. mit **Bachelor Projektarbeit**
Masterarbeit ggf. mit **Master Projektarbeit**

Verwundbarkeiten entstehen bei der Entwicklung von Software häufig durch einen *inkorrekten Einsatz kryptographischer Verfahren* (Nadi et al., 2016). Testen in diesem Kontext findet bis dato wenig Beachtung - sowohl in der Forschung als auch in der industriellen Praxis. Dabei ist *systematisches Testen* notwendig, welches sich typischer Fehler z. B. bei der Erzeugung von kryptographischen Schlüsseln, der Nutzung von APIs und der Einhaltung regulatorischer und gesetzlicher Anforderungen, widmet. Die Arbeit soll einerseits den Stand der Technik und Forschung im Rahmen einer Literaturrecherche erheben, und andererseits das Thema weiter motivieren. Neuartige Testansätze, z. B. ein System von musterhaften Tests gruppiert als Testsuites für verschiedene Themenfelder, sollen konzipiert und umgesetzt werden. Eine Evaluation der neuen Ansätze, z. B. anhand von Fallstudien, soll durchgeführt werden.

Ziele

- Literaturrecherche und -aufarbeitung
- Konzeption und Umsetzung neuer Testansätze
- Evaluation der neuen Ansätze

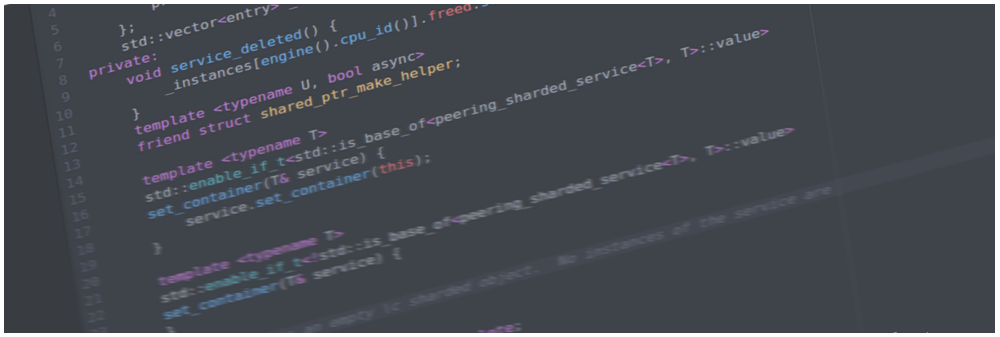

Foto von Sarah Meilwes erstellt

Literaturrecherche

- Verwundbarkeiten entstanden durch inkorrekt eingesetzte kryptographische Verfahren, z. B. ausgehend von Nadi et al., 2016
- Testansätze mit entsprechendem Fokus

Initiale Literatur

Nadi, S., Krüger, S., Mezini, M., & Bodden, E. (2016). Jumping Through Hoops: Why do Java Developers Struggle With Cryptography APIs? *Proceedings of the International Conference for Software Engineering (ICSE)*, 935–946.

Prof. Dr. Holger Schmidt
Professur für IT-Sicherheit, Informatik
Kontakt: holger.schmidt004[at]fh-dortmund.de

Fachhochschule Dortmund
University of Applied Sciences and Arts