

Formale Spezifikation von Sicherheitsanforderungen auf Basis von Common Criteria Schutzprofilen

Masterarbeit

Zertifizierungen von IT-Produkten nach *Common Criteria* erfordern ab der Prüftiefe EAL 6 eine Modellierung der Sicherheitsanforderungen mithilfe *formaler Spezifikationssprachen*, z. B. endlichen Automaten (Beuster & Greimel, 2012). Da in der Industrie häufig *Schutzprofile* für die Anforderungsspezifikation genutzt und diese vollständige Anforderungen für eine Produktkategorie beinhalten, sollen diese Anforderungen als *wiederverwendbare, formale Spezifikationen* modelliert werden.

Ziele

- Literaturrecherche und -aufarbeitung
- Entwicklung von formal spezifizierten Mustern für Common Criteria Sicherheitsanforderungen (Security Functional Requirements)
- Demonstration anhand eines konkreten Common Criteria Schutzprofils und eines zugehörigen Security Targets

Literaturrecherche

- Welche formalen Spezifikationssprachen wurden bisher im Kontext der IT-Sicherheit verwendet?

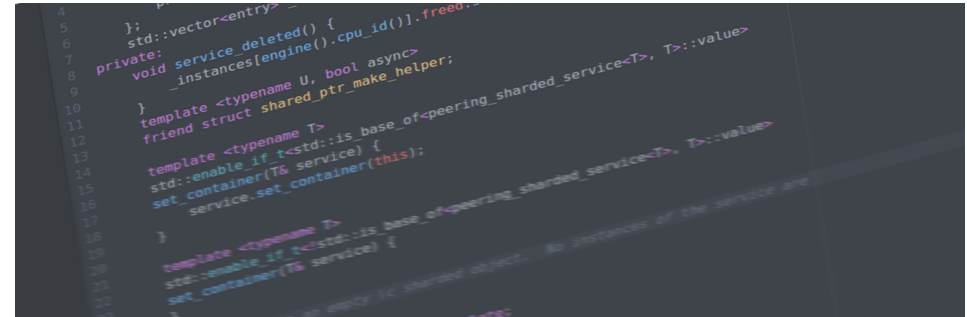


Foto von Sarah Meilwes erstellt

- Welche formalen Spezifikationssprachen wurden bisher im Rahmen von Common Criteria Zertifizierungen verwendet?
- Welche musterbasierten Ansätze für formale Spezifikation gibt es?
- Einordnung der selbst entwickelten Muster im Rahmen der Literaturrecherche

Initiale Literatur

Beuster, G., & Greimel, K. (2012). Formal Security Policy Models for Smart Card Evaluations. *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, 1640–1642.

<https://www.commoncriteriaportal.org/> (28.08.2023)

https://www.bsi.bund.de/DE/Themen/StandardsKriterien/FormaleMethoden/formalemethoden_node.html (28.08.2023)

https://www.bsi.bund.de/DE/Publikationen/Studien/Formal_Methods_Study_875/study_875.html (28.08.2023)

Prof. Dr. Holger Schmidt

Professur für IT-Sicherheit, Informatik

Kontakt: holger.schmidt004@fh-dortmund.de

**Fachhochschule
Dortmund**

University of Applied Sciences and Arts