

Security-Analyse von Lastenheften bei Bosch Infotainment

Hintergrund

Lastenhefte sind oft sehr umfangreich, besonders auch im Infotainmentbereich. Auch in diesem Bereich wird die Sicherheit gegen Angriffe immer wichtiger. Es gibt aber oft nicht genug Security-Experten, um alle Lastenhefte im Detail auf Security zu prüfen. Am FG Software Engineering wurde im Rahmen des SecVolution-Projekts ein Ansatz entwickelt, natürlichsprachliche Dokumente wie Lastenhefte mit Hilfe einer zweistufigen Ontologie aus allg. Security-Konzepten und Anwendungskonzepten zu analysieren. Dieser Ansatz war ursprünglich auf Informationssysteme zugeschnitten.

Aufgabe

In dieser Masterarbeit soll die Werkzeugkette des Ansatzes funktionsfähig aufgebaut und auf den neuen Anwendungsbereich von Bosch Car Infotainment angewendet werden:

- Zunächst ist eine Einarbeitung in den existierenden NLP (natural language processing)-Ansatz von SecVolution erforderlich. Dann können die darin verwendeten Werkzeuge besorgt und in eine Toolkette eingefügt werden.
- Parallel kann eine Analyse möglicher Bedrohungen und Security-Begriffe bei Bosch in Hildesheim erfolgen. Befragung dortiger Fachexperten und die Analyse von Dokumenten führen zu einer speziellen Ontologie dieses Bereichs, die mit der allgemeinen Ontologie von Security-Konzepten verbunden wird. Eine Ontologie ist ein Begriffs- und Konzeptschema, das wie eine Datenbank mit zusätzlichen Analysefunktionen genutzt werden kann.
- Danach müssen noch semantische Muster (Frames) für die Situation bei Bosch aufgebaut werden, die auf verdächtige Konstellationen in den Lastenheften aufmerksam machen. Dann ist der Ansatz anwendbar.
- Nun wird die aufgebaute Werkzeugkette und die zweistufige Ontologie auf andere, neue Lastenhefte angewendet, um die Wirksamkeit des Ansatzes zu evaluieren und iterativ zu verbessern. Dazu werden u.a. Frames so weiterentwickelt, dass man weitere verdächtige Ausdrücke erkennen kann.
- Das Ergebnis ist die Toolkette mit Beschreibung und zweistufiger Ontologie, sowie eine Dokumentation der Evaluierungsschritte und daraus abgeleiteter Verbesserungsmaßnahmen. Zum Abschluss wird das Potenzial des Verfahrens abgeschätzt.

Die Ausarbeitung dokumentiert die obigen Schritte und Konzepte und enthält zusätzlich eine Sammlung von aufgetretenen Problemen und Lösungen dazu. Diese Sammlung soll dazu dienen, den Ansatz in anderen Bereichen noch schneller aufsetzen und anpassen zu können.

Organisatorisches

- Betreuer:** M.Sc. Fabien Viertel
Prüfer: Prof. Kurt Schneider
Beginn: frühestens ab 1.4.2017