

Implementation eines Open-Source STRIDE Threat-Modelling-Tools

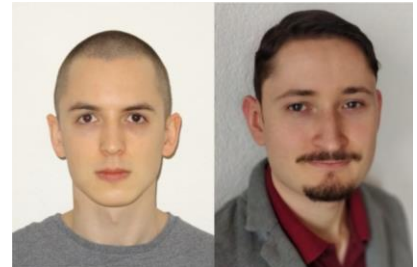
Kein Unternehmen will in den Schlagzeilen landen, weil ihm ungenügend gesicherte User-Daten gestohlen wurden. Um einem solchen Fall entgegenzuwirken, sollten Sicherheitsvorkehrungen bei der Softwareentwicklung getroffen werden. Doch wie weiss man, ob man die richtigen gewählt hat?

Eine mögliche Antwort ist Threat-Modeling. Dies hat Microsoft auch erkannt und bereits 2008 der Öffentlichkeit die erste Version des «Security Development Lifecycle Threat Modeling Tools» zur Verfügung gestellt. Dieses Tool bietet dem Anwender die Möglichkeit, mit einer Vielzahl von vordefinierten Schablonen ein Data-Flow-Diagramm zu erstellen, durch STRIDE mögliche Threats für dieses System zu identifizieren und das Diagramm zusammen mit den Threats als Bericht zu exportieren.

Das Tool von Microsoft funktioniert jedoch nur auf Windows, weshalb das Ziel dieser Bachelorarbeit war, eine ähnliche Desktopapplikation zu implementieren, welche Open Source ist und auf den Betriebssystemen Windows, Linux und macOS läuft. Konkret wurde geplant folgende Applikationskomponenten zu realisieren: ein Diagrammeditor für Data-Flow-Diagramme, ein automatisches Threat-Analyse-System und ein Threat-Report-Generator.

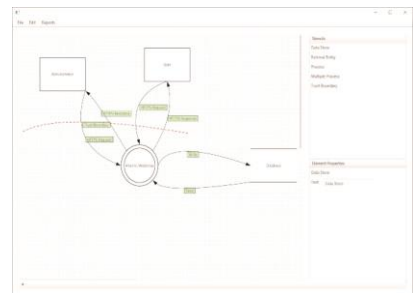
Um die Plattformunabhängigkeit zu ermöglichen, wurde die Applikation in Java entwickelt. Dazu wurde das JavaFX GUI-Toolkit und die Open Source Bibliothek «Graph Editor» verwendet.

Die geplanten drei Hauptfunktionen konnten umgesetzt werden und funktionieren ohne signifikante Probleme. Das aus der Arbeit resultierende «STRIDE Threat Modeling Tool» kann erfolgreich zum Threat-Modeling verwendet werden, wie wir im Resultate-Abschnitt dieses Berichts demonstrieren. Das finale Produkt ist dennoch nicht ohne gewisse Mängel bezüglich Benutzerfreundlichkeit und besitzt Ausbaupotenzial für zusätzliche Features.

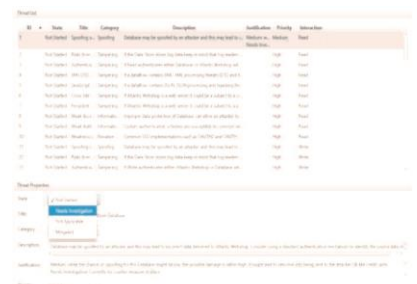


Diplomierende
Michael Schlaubit
Manuel Schreier

Dozent
Stephan Neuhaus



Screenshot des Diagrammeditors im
«STRIDE Threat Modeling Tool».



ID	Name	Severity	Category	Description	Qualifikation	Rating	Verantwortung
1	Verlust	Hoch	Verlust	Die Daten werden durch die Speicherung auf dem Server...	Verlust	Hoch	Verlust
2	Verlust	Hoch	Verlust	Die Daten werden durch die Speicherung auf dem Server...	Verlust	Hoch	Verlust
3	Verlust	Hoch	Verlust	Die Daten werden durch die Speicherung auf dem Server...	Verlust	Hoch	Verlust
4	Verlust	Hoch	Verlust	Die Daten werden durch die Speicherung auf dem Server...	Verlust	Hoch	Verlust
5	Verlust	Hoch	Verlust	Die Daten werden durch die Speicherung auf dem Server...	Verlust	Hoch	Verlust
6	Verlust	Hoch	Verlust	Die Daten werden durch die Speicherung auf dem Server...	Verlust	Hoch	Verlust
7	Verlust	Hoch	Verlust	Die Daten werden durch die Speicherung auf dem Server...	Verlust	Hoch	Verlust
8	Verlust	Hoch	Verlust	Die Daten werden durch die Speicherung auf dem Server...	Verlust	Hoch	Verlust
9	Verlust	Hoch	Verlust	Die Daten werden durch die Speicherung auf dem Server...	Verlust	Hoch	Verlust
10	Verlust	Hoch	Verlust	Die Daten werden durch die Speicherung auf dem Server...	Verlust	Hoch	Verlust

Screenshot einer Threat-Liste im
«STRIDE Threat Modeling Tool».