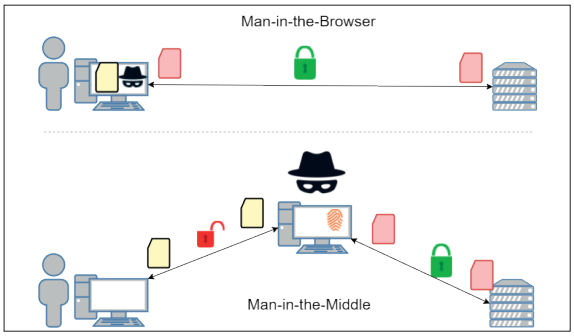
Matthias Gabriel

Philip Schmid

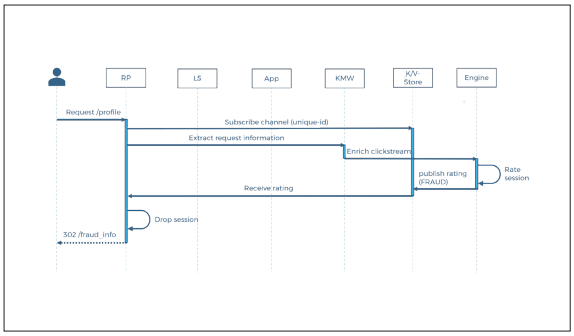
Diplomanden	Matthias Gabriel, Philip Schmid
Examinator	Ivan Bütler
Experte	Dr. Benjamin Fehrensen, UBS
Themengebiet	Sicherheit

Man in the Browser Detection

MarkovShield



Man-in-the-Browser vs Man-in-the-Middle

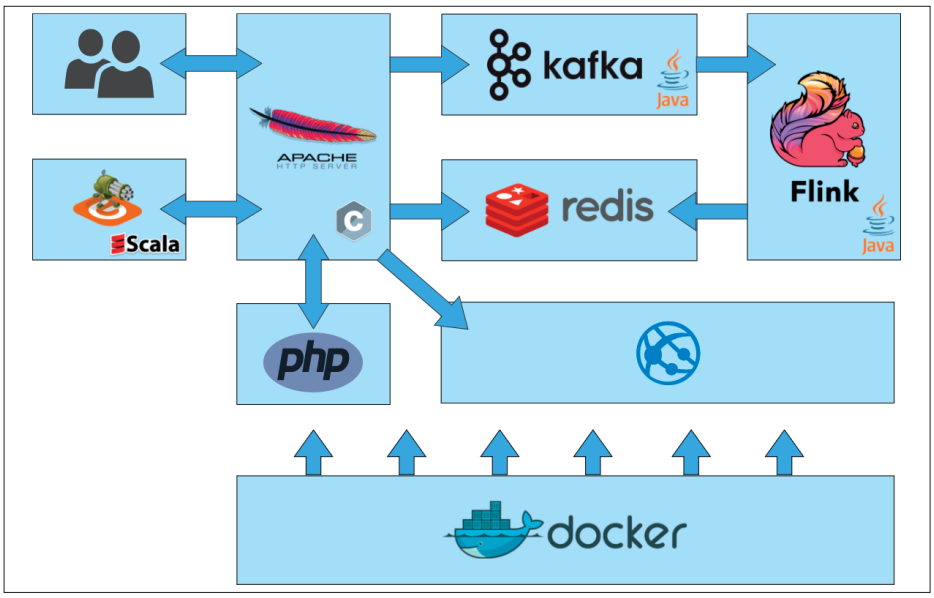


Ablaufdiagramm im Falle einer detektierten Anomalie

Ausgangslage: Sicherheit ist in der IT eine Thematik, die in den letzten Jahren immer wichtiger wurde. Zugleich wird jedoch auch mehr kriminelle Energie aufgewendet, und es werden immer wieder neue Angriffsvektoren auf die Systeme und deren Benutzer entdeckt. Eine Attacke, die auf solchen neuen Angriffsvektoren basiert, wird «Man-in-the-Browser» genannt. Kurzgefasst wird dabei der Datenaustausch zwischen dem Browser des Benutzers und der Webapplikation direkt im Browser des Benutzers manipuliert. Bestehende Sicherheitsmassnahmen werden dadurch ausgehebelt. Die neu entwickelte Security-Lösung soll anhand von historischen und zugleich computerunabhängigen Session-Daten Anomalien detektieren und entsprechende Gegenmassnahmen treffen.

Vorgehen/Technologien: In einer Masterarbeit wurden verschiedene Algorithmen analysiert und zu jedem wurden entsprechende Empfehlungen abgegeben und ein Post-Processing-Prototyp erstellt. Basierend darauf wurden die zusätzlichen Anforderungen für eine Realtime-Lösung evaluiert und in eine entsprechende Architektur überführt. Es stellte eine besondere Herausforderung dar, Technologien zu finden, die die Realtime-Anforderung erfüllen und wie diese zu einer performanten Architektur zusammengesetzt werden können.

Ergebnis: Als Resultat dieser Arbeit wurde die Security-Lösung MarkovShield entwickelt, die in der Lage ist, in Realtime Zugriffe auf eine Webapplikation zu bewerten, bevor diese den Webserver erreichen. Wird ein Zugriff als verdächtig erkannt, so werden entsprechende Gegenmassnahmen getroffen. Bei der Auswahl der Technologien wurde sichergestellt, dass beim Einsatz in einer produktiven Umgebung die einzelnen Komponenten gut skaliert werden können.



Architekturübersicht von MarkovShield