Bachelorthesis-Aufgabe

Automatisierte Anomalie Detektion in der Memory Forensik

ID	IBTE1-1-13
Studierende	Ramona Cioccarelli Benjamin Urech
Betreuer	Dr. Endre Bangerter
Experten	Dr. Federico Flueckiger
Aufgabe	Die "Memoryforensik", also die Analyse von Abbildern des RAM Speichers ist eine Schlüsseltechnik für die Detektion und Analyse von Malware und vielen Hackingangriffen. Die Idee ist, dass Angreifer unvermeidliche Spuren im Speicher hinterlassen. Dies sind beispielsweise unbekannte Prozesse, oder subtile Systemmodifikationen. Die Memoryforensik erlaubt diese Spuren, bei denen es sich letztlich um Anomalien handelt, zu finden, somit Angriffe zu detektieren und (zumindest teilweise) zu verstehen. Die Schwierigkeit hierbei ist, dass oft tief reichende System- und Malware-Kenntnisse von Nöten sind, und solche Analysen nur wenigen Spezialisten zugänglich sind. Das Ziel dieser Bachelorarbeit ist es diese Problematik zu entschärfen, in dem die Detektion von Anomalien im Speicher, zumindest teilweise, automatisiert wird. Die Automatisierung soll erreicht werden in dem die Charakteristiken von Speicherbildern unversehrter Systemen untersucht und ausgewertet werden, um Regeln und Heuristiken zur Detektion zu gewinnen. Das resultierende System soll in Praxistests systematisch evaluiert werden.