Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

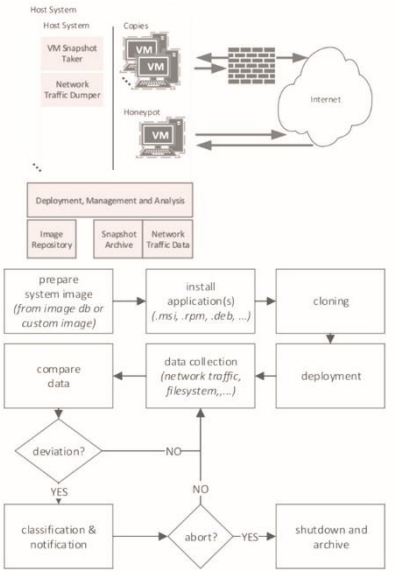
InIT Institut für angewandte
Informationstechnologie

Honey-Copy - Methoden zur Reduktion von False Positives

Diplomierende
Michael Hoessly
Dominik Stillhard

Dozent
Bernhard Tellenbach

In der vorhergehenden Forschungsarbeit wurde am Institut für Angewandte Informationstechnologie der ZHAW ein generisches High-Interaction-Server-Honeypot-System, Honey-Copy, entwickelt. Dieses verfolgt im Vergleich zu existierenden Produkten einen neuartigen Ansatz. Dieser basiert auf dem parallelen Betrieb von identischen, virtuellen Maschinen, von welchen nur eine (der Honeypot) exponiert ist. Zur Angriffserkennung wird diese regelmässig mit den anderen, nicht exponierten virtuellen Maschinen, verglichen. Da der Vergleich ausserhalb der VMs geschieht, kann die Erkennung des Honeypots als solchen vermindert werden.
Der Prototyp von Honey-Copy verursachte jedoch zu viele False Positives. Die vorliegende Arbeit geht den Ursachen hierfür auf den Grund und macht Vorschläge, wie False Positives behoben werden können. Dazu wurden verschiedene Honeypot-Konfigurationen über einen längeren Zeitraum betrieben. Für die Wahl der Konfigurationen wurden Marktanalysen bezüglich Attraktivität als Angriffsziel sowie bezüglich Verbreitungsgrad von beliebten Server-Konfigurationen durchgeführt. Aufgrund dieser wurden dann fünf Konfigurationen ausgewählt und entsprechende Virtuelle Maschinen erstellt. Aus den dabei anfallenden Daten konnten Konzepte zur Reduktion von False Positives, z.B. für False Positives, die aufgrund des Vergleichs des Netzwerkverkehrs entstehen, abgeleitet und teilweise implementiert werden.
Weiter wurde ein Algorithmus entwickelt, welcher in der Lage ist, bei Filesystem-Vergleichen entstandene False Positives zu reduzieren. Eine Integration dieses Algorithmus fehlt, jedoch bildet er eine gute Grundlage für eine Implementation. Die Arbeit macht zudem Vorschläge, wie Honey-Copy bezüglich Deployment weiter optimiert werden kann. Hier steht eine direkte Steuerung mittels Apache CloudStack im Fokus. Hinzu kommen diverse Verbesserungs-vorschläge, wie das System bezüglich Benutzerfreundlichkeit, Fehleranfälligkeit, Funktionalität und Performance optimiert werden kann.



Architektur und grundlegende Arbeitsweise von Honey-Copy