
-Masterarbeit-

IF-MAP Entwicklung in Testbed mit Logreplay

Motivation

Der Betrieb von IT Infrastrukturen führt zu einer Vielzahl von Ereignissen wie das Hinzufügen von Geräten, Anmelden von Benutzern aber auch dem Ausfall von Geräten oder Ergebnissen von Intrusion Detection Systemen. Hinzu kommen Ereignisse, die sich aus dem eigentlichen Anwendungsfall der Infrastruktur ergeben. Diese Ereignisse sind abhängig von den Prozessen die auf Basis der Infrastruktur durchgeführt werden, so dass sich verschiedene Klassen von Ereignissen ergeben.

Ereignisse beeinflussen die eigentlichen Prozesse auf unterschiedliche Weise. Ein einheitliches Erfassen und Darstellen dieser Ereignisse stellt eine zentrale Fähigkeit für verschiedene Infrastrukturen dar, um das Bereitstellen eines verlässlichen QoS zu gewährleisten. Hierbei bestehen in der Industrie verschiedene Initiativen zur Vereinheitlichung der Protokolle und Methoden zur Verarbeitung von Ereignissen. IF-MAP stellt hierbei einen interessanten Vertreter dar, der sich zur Zeit in der Standardisierung befindet.

Basierend auf einer Testumgebung gilt es die möglichen Ereignisse zu bestimmen und deren Abhängigkeiten zu spezifizieren. Ziel der Arbeit ist es hierbei ein Modell auf Basis eines Beispielszenarios zu entwickeln und dieses Modell danach in einem praktischen Beispiel auf Basis von IF-MAP zu realisieren. Um die unterschiedlichen, sicherheitsspezifischen Informationen aus dem Testbed sammeln und verarbeiten zu können, sind verschiedene MAP-Clients zu entwickeln.

Aufgaben

- Identifikation und Implementierung der Eventquellen in Testumgebung
- Ein erstes Modell einer Teilmenge der Eventinformationen
- Anbindung der Metadaten an einen MAP Server

Anforderungen

- Bereitschaft sich in neue Themenbereiche selbständig einzuarbeiten
- Gute Programmierkenntnisse
- Gutes technisches Verständnis von verteilten Systemen (client-server)
- Gute analytische Fähigkeiten
- Gute englische Sprachkenntnisse (Arbeit auf Deutsch oder Englisch)

Beginn

Ab sofort möglich

Kontakt

Nicolai Kuntze & Timo Winkelvos
nicolai.kuntze@sit.fraunhofer.de, timo.winkelvos@sit.fraunhofer.de
Fraunhofer Institute for Secure Information Technology (SIT)
Rheinstraße 75
64295 Darmstadt