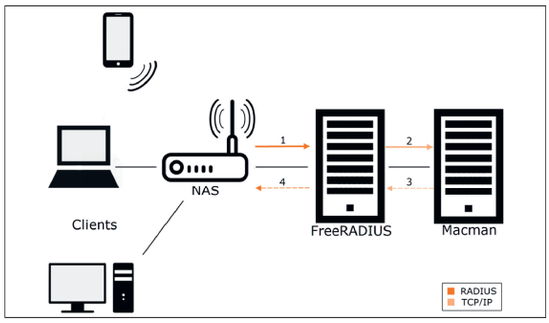
Filippo Pitrella

Michael Schefer

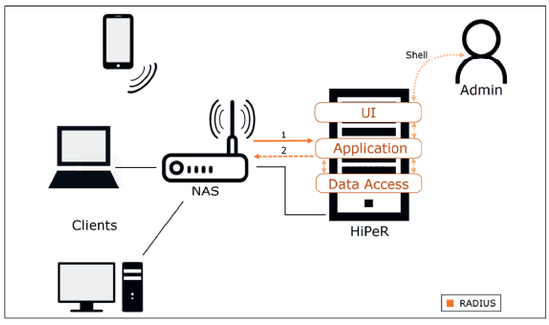
Diplomanden	Filippo Pitrella, Michael Schefer
Examinator	Prof. Beat Stettler
Experte	Rolf Schärer, Cisco
Themengebiet	Sicherheit
Projektpartner	CloudGuard Software AG, Zürich, ZH

HiPeR

High Performance RADIUS Server



Systemübersicht bisherige Lösung



Systemübersicht neu entwickelte Lösung

Projektpartner CloudGuard Software AG

Ausgangslage: Sicherheit ist ein zentrales Thema in Netzwerken. Um sich gegen unerlaubte Zugriffe zu schützen, wird von Firmen häufig ein RADIUS Server eingesetzt. Benutzer müssen sich damit vor dem Zugriff auf das Netzwerk authentisieren. Die zurzeit von der Firma CloudGuard eingesetzte Lösung setzt sich aus den zwei Produkten Macman und FreeRADIUS zusammen. Diese Kombination zweier Lösungen verursacht zusätzliche Kommunikation, was die Performance beeinträchtigt. Deshalb soll mit dieser Arbeit die Grundlage für einen RADIUS Server geschaffen werden, der die Funktionalität beider Produkte in sich vereint und die Performance steigert.

Vorgehen/Technologien: Die Entwicklung wird in drei Phasen aufgeteilt, die sich an den primären Aufgaben des Servers orientieren. In einem ersten Schritt müssen Benutzer in der Lage sein, sich am Netzwerk anzumelden. Anschliessend muss die Nutzungsstatistik eines Benutzers erfasst werden können. Die letzte Phase betrifft schliesslich die Trennung des Benutzers vom Netzwerk. Damit HiPeR auf allen Betriebssystemen eingesetzt werden kann, wird als Programmiersprache Java (Version 8) verwendet. Die Grundlage für die Implementation bildet das Netzwerk Framework Netty. Dieses erlaubt die asynchrone Bearbeitung von Anfragen und ermöglicht eine hohe Performance. Die Bedienung der Applikation erfolgt über eine Eingabeaufforderung, die auf der Shell des Spring Frameworks basiert.

Ergebnis: Die entstandene Applikation ist in der Lage, bis zu 95000 Anfragen pro Sekunde zu bearbeiten. Sie erlaubt die Authentifizierung von Linux- und Mac-Clients sowie von Android-Smartphones und iPhones durch das Protected Extensible Authentification Protocol (PEAP). Geräte, welche dieses Protokoll nicht unterstützen, können anhand ihrer MAC-Adresse authentifiziert werden. Sobald ein Gerät verbunden ist, werden im Hintergrund laufend Nutzungsstatistiken erfasst, um zum Beispiel Verrechnungen von bezogenen Leistungen zu ermöglichen. Sollte ein verbundener Benutzer nicht mehr für das Netzwerk zugelassen sein, besteht die Möglichkeit, diesen über die Eingabeauforderung vom Netzwerk zu trennen.