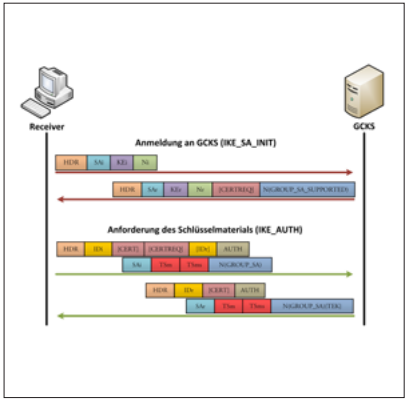
Cornel
Eberle

Roman
Federer

Multicast Security using IPsec

A lightweight solution based on IKEv2

Diplomanden	Cornel Eberle, Roman Federer
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere AG, Zürich
Themengebiet	Sicherheit
Projektpartner	Institut für Internet-Technologien und -Anwendungen ITA , HSR, Rapperswil-Jona SG



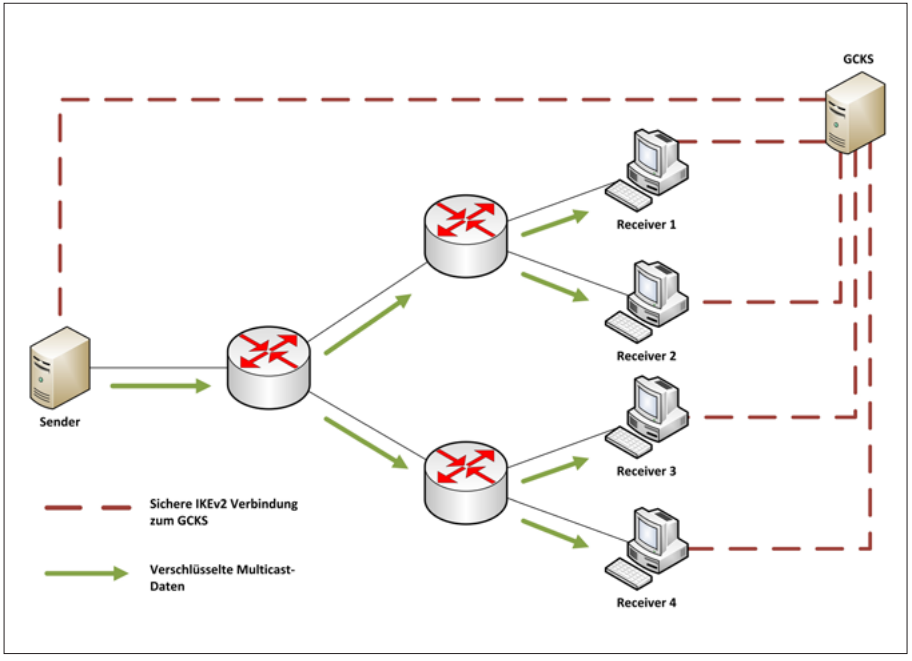
Nachrichten bei der Schlüsselanforderung

Ausgangslage: IPsec ist ein verbreitetes Protokoll zur Absicherung der Netzwerkkommunikation auf dem Network-Layer. Dabei werden Vertraulichkeit, Authentizität und Integrität der Daten gewährleistet. Das Internet-Key-Exchange-Protokoll in Version 2 (IKEv2) wird für den Austausch der Schlüssel verwendet.

Bis heute existiert im IPsec-Standard keine Lösung für die Absicherung von IP-Multicast-Verkehr. Da es sich bei Multicast um Kommunikation zwischen mehr als zwei Teilnehmern handelt, muss ein gemeinsamer Schlüssel verteilt werden.

Einige Ansätze einer IPsec-Multicast-Lösung wurden bereits entwickelt und im Internet publiziert. Diese sind jedoch entweder zu umfangreich, zu kompliziert in der Realisierung oder enthalten Schwachstellen.

Aufgabenstellung: Das Ziel dieses Projekts war die Entwicklung eines IPsec-Multicast-Protokolls, welches auf IKEv2 aufbaut. Die Lösung soll möglichst leichtgewichtig sein und so viel wie möglich vom Standard übernehmen. Zudem soll die Realisierung eines High-Level-Protokollsimulators in der Programmiersprache C# die Funktionsweise des



Komponenten einer IPsec-Multicast-Umgebung

Protokolls anhand einer praktischen Umsetzung überprüfen.

Lösung: Für die Verwaltung der IPsec-Multicast-Gruppen wurde ein Group Controller and Key Server GCKS erstellt. Ein neuer Teilnehmer meldet sich beim GCKS an, um das Schlüsselmaterial für eine Multicast-Gruppe zu erhalten. Dazu sind zwei Nachrichtenpaare nötig, welche, leicht abgeändert, dem IKEv2-Standard entsprechen.

Der Schlüssel für eine IPsec-Multicast-Gruppe wird in bestimmten Zeitintervallen erneuert. Dieser als Rekeying bezeichnete Vorgang wird auch durchgeführt, wenn ein neuer Teilnehmer zur Gruppe hinzukommt oder ein Teilnehmer die Gruppe verlässt. Durch diese Strategie kann sichergestellt werden, dass nur aktive Teilnehmer der Gruppe den Verkehr entschlüsseln können.