Multicast Security Group Key Management Architecture (MSEC GKMArch)

draft-ietf-msec-gkmarch-07.txt

Internet Security

Tobias Engelbrecht

Einführung

Bei diversen Internetanwendungen, wie zum Beispiel Telefonkonferenzen (mit mehreren Teilnehmern) oder Video Übertragungen, müssen immer wieder dieselben Pakete von einem Sender an mehrere Empfänger übertragen werden. Um hierbei die Netzlast gering zu halten, wird IP Multicasting angewendet. Bei dieser Technik sendet der Sender nur ein Paket an alle angemeldeten Empfänger. Die Duplizierung und Verteilung des Pakets übernehmen dabei die Router zwischen dem Sender und den Empfängern.
Einige Anwendungen, z.B. Telefonkonferenzen zwischen Geschäftspartnern, erfordern hierbei einen sicheren Datenverkehr zwischen dem Sender und den Empfängern. Dieser „Draft“ beschäftigt sich mit der Verteilung der Schlüssel für den sicheren Datenverkehr zwischen Sender und Empfängern.

Anforderungen an ein „Group Key Management Protocol“

Die Teilnehmer an einer Multicast Kommunikation werden in eine sichere Gruppe zusammengefasst. In dieser kann jeder Sender oder Empfänger bzw. beides sein. Das „Group Key Management Protocol“ unterstützt die sichere Kommunikation innerhalb dieser Gruppe. Außerdem stellt es sicher, dass nur berechtigte Mitglieder zugriff zu den Gruppen Schlüsseln haben.
Wichtig ist es, dass das Protokoll die folgenden, von Multicast Anwendungen geforderten, Anforderungen erfüllt:

- alle Gruppenmitglieder erhalten die „Security Assocations“
- die Schlüssel werden aktualisiert
- die Schlüssel werden sicher, unversehrt und verifizierbar geliefert
- das Protocol soll sicher gegen „replay attacks“ und „denial of service attacks“ sein
- das Protocol soll es ermöglichen, dass neue Mitglieder keinen Zugriff auf alte Schlüssel bekommen und das ehemalige Mitglieder keinen Zugriff mehr auf aktuelle Schlüssel besitzen
- usw.

Konzeption der „Group Key Management Architecture“

Das Ziel der “Group Key Management Architecture” ist die sichere Kommunikation zwischen ihren Mitgliedern. Hierfür muss das „Group Key Management Protocol“ jedem Mitglied die aktuelle „Data Security Association“ bereitstellen. Die „Data Security Association“ sichert die Verbindung von Sender zu Empfängern über das „Data Security Protocol“.

Um den Mitgliedern einer sicheren Gruppe die Informationen für die „Data Security Association“ bereitzustellen, wird das „Registration Protocol“ und das „Rekey Protocol“ benötigt. Die beiden Protokolle müssen jeweils wieder mit einer „Security Assocation“ abgesichert werden.

Die „Registration“ und „Rekey“ Nachrichten, die die Schlüssel und die Informationen für die jeweilige „Security Association“ („Registration“, „Rekey“, „Data“) enthalten, werden von dem „Group Controller / Key Server“ gesendet.

Die drei „Security Associations“, „Data“, „Registration“ und “Rekey”, bilden die “Group Security Association”.

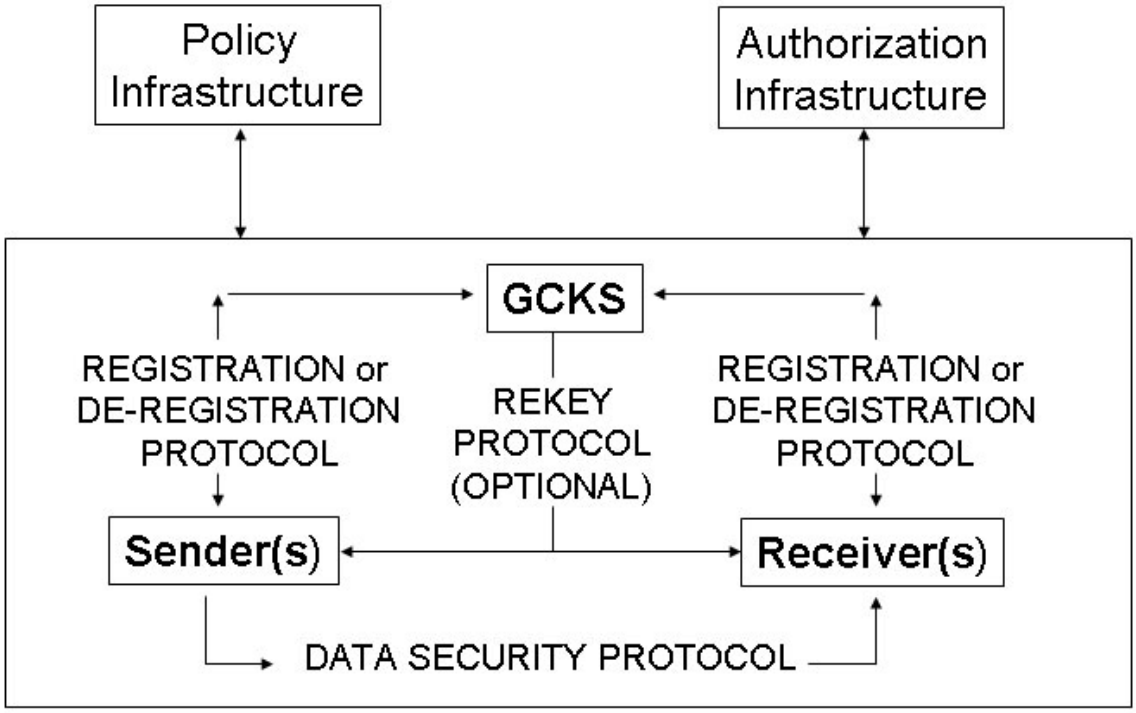

Abbildung 1: Group Security Association Model

Die Abbildung 1: Group Security Association Model zeigt die für eine „Group Security Associaton“ benötigten Protokolle und Mitglieder.

Group Controller / Key Server

Zentraler Punkt der „MSEC Group Key Management Architecture“ ist der „Group Controller / Key Server“. Er erstellt die für eine sichere Kommunikation notwendigen „key encryption keys“ (KEKs) und „traffic encrytption keys“ (TEKs) bereit und ist für deren Verteilung verantwortlich. Dazu hat er hauptsächlich das „Registration Protocol“ zur Verfügung. Das „Rekey Protocol“ aus Abbildung 1: Group Security Association Modelist optional aber wünschenswert. Weiterhin führt der „Group Controller / Key Server“ die Authentifizierung der einzelnen Mitglieder durch. Der Besitzer der Gruppe bestimmt den „Group Controller / Key Server“ und legt auch die Authentifizierungskriterien, sowie die Einstellungen für die verwendeten Protokolle fest. So entscheidet der Besitzer z. B. ob das „Rekey Protocol“ verwendet werden soll oder nicht.

Registration Protocol

Ein Mitglied, das an einer sicheren Gruppe teilnehmen will, muss sich an dieser zuerst anmelden. Hierfür wird das „Registration Protocol“ verwendet. Dabei authentifizieren sich hierbei zuerst der „Group Controller / Key Server“ und das neue Mitglied gegenseitig. Stellt der „Group Controller / Key Server“ fest, dass das Mitglied berechtigt ist zugriff zu erlangen, sendet er ihm, je nach Einstellungen in den Richtlinien, entweder die notwendigen Informationen („Rekey Security Association“) um eine sichere Verbindung über das „Rekey Protocol“ herzustellen oder Informationen („Data Security Association“) um eine sichere Verbindung zwischen den Mitgliedern herzustellen. Wichtig hierbei ist, dass der Datenverkehr in einer sicheren Art und Weise von statten geht.

Rekey Protocol

Wenn ein Mitglied die Gruppe verlässt, der Gruppenbesitzer die Richtlinien verändert oder die Schlüssel ablaufen, müssen die verbleibenden Mitglieder mit neuen Schlüsseln und / oder „Security Associations“ versorgt werden. Hierzu wird das „Rekey Protocol“ verwendet.
Geschützt wird das „Rekey Protocol“ durch die „Rekey Security Association“. Die hierfür notwendigen Informationen werden über das „Registration Protocol“ mitgeliefert.
Der Inhalt einer „Rekey Message“ können die Informationen für eine neue „Rekey Security Association“ und / oder für eine „Data Security Association“ sein.

Wünschenswert für das „Rekey Protocol“ wäre, wenn es sicherstellt, dass alle Mitglieder die „Rekey“ Nachrichten in einer gewissen Zeit bekommen.
Als Authentifizierung der „Rekey Message“ können zwei Verfahren eingesetzt werden: „Source Authentication“ und „Group Based Authentication“. Bei dem „Group Based Authentication“ Verfahren wird ein symmetrischer Schlüssel eingesetzt und ist deshalb nur zu empfehlen, wenn allen Mitgliedern der Gruppe vertraut werden kann.

Group Security Association (GSA)

Die „Group Security Association“ besteht aus der „Data Security Association“, der „Registration Security Association” und der optionalen “Rekey Security Association”.
Wie oben schon beschrieben, schützt die “Registration Security Association” das „Registration Protocol”.
Zusätzlich initialisiert das „Registriation Protocol“ auch die „Rekey Security Associaton“. Das „Rekey Protocol“ initialisiert dann die „Data Security Association“.
Verzichtet der Gruppenbesitzer auf den Einsatz der „Rekey Security Association“, wird die „Data Security Association“ bereits mit dem „Registration Protocol“ initialisiert.

Rekey Security Association

Die „Rekey Security Association“ enthält die kryptographischen Richtlinien, welche den „Group Key Management Algorithm“, den „KEK Encryption Algorithm“, den „Authentication Algorithm“, die „Control Group Adress“ und die „Rekey Server Adress“ festlegt. Außerdem sind in der „Rekey Security Association“ auch noch die „key encryption keys“, der Authentifizierungschlüssel, eine Information zu welcher Gruppe die „Security Association“ gehört, Informationen gegen „replay attacks“ und ein „security parameter index“.

Data Security Association

Die „Data Security Association“ schützt das „Data Security Protocol“. Das Protokoll wird für den sicheren Transport der Daten von Sender zu den Empfängern eingesetzt (siehe Abbildung 1: Group Security Association Model). IPsec zum Beispiel beinhaltet ein „Data Security Protocol“.

Die „Data Security Association“ beinhaltet Informationen zu welcher Gruppe sie gehört, die „traffic protection keys“ zum Verschlüsseln des Datenverkehrs, „sequence numbers“ für „replay protection“ und einen „security parameter index“ (SPI) sowie die Richtlinien für die „Data Security Association“.

Sicherheitsbetrachtungen

Die oben genannten Protokolle („Registration Protocol“, „Rekey Protocol“ und „Data Security Protocol“) müssen gegen verschiedene Angriffe geschützt werden.

So verringern Techniken zum „Authenticated Key Exchange“ die Auswirkung von „man-in-the-middle“ und „connection hijacking attacks“. Sequenz Nummern können erfolgreich gegen „replay attacks“ eingesetzt werden. Hierfür wird jedes Paket aufsteigend nummeriert. Wenn mehrere Sender an einer Kommunikation beteiligt sind, müssen diese die Sequenz Nummern untereinander synchronisieren. „Cookies“ bieten ein effizientes Mittel um den Effekt von „Denial of Service“ Angriffen einzugrenzen.

Das „Rekey Protocol“ ist neu und die Probleme die damit auftreten können, sind noch unbekannt. Die Verwendung von Multicast Kommunikation wirft neue zusätzliche Sicherheitsprobleme auf, z. B. „Implosion“ oder „Denial of Service Attacks“. Die „Rekey Protocol“ Spezifikation muss hier sichere Lösung für diese Probleme anbieten.