Kryptologie

IP Multicast

Philipp Kleinhenz, 67992, HTWK Leipzig

Julian Götz, 68549, HTWK Leipzig

10. Januar 2019

Problemstellung Multicast

IP-Multicast bezeichnet eine Technik zum effizienten Senden von Nachrichten an mehrere Teilnehmer unter Ausnutzung von hierarchischen Netzwerkstrukturen. Bei IP-Unicast wird jede Nachricht gesondert an jeden Teilnehmer gesendet. Im Gegensatz dazu wird bei IP-Multicast die Nachricht von weiterleitenden Routern nach Bedarf dupliziert und jeweils an die Unterknoten gesendet, bis sie bei den Nachricht anfordernden Teilnehmern ankommt.

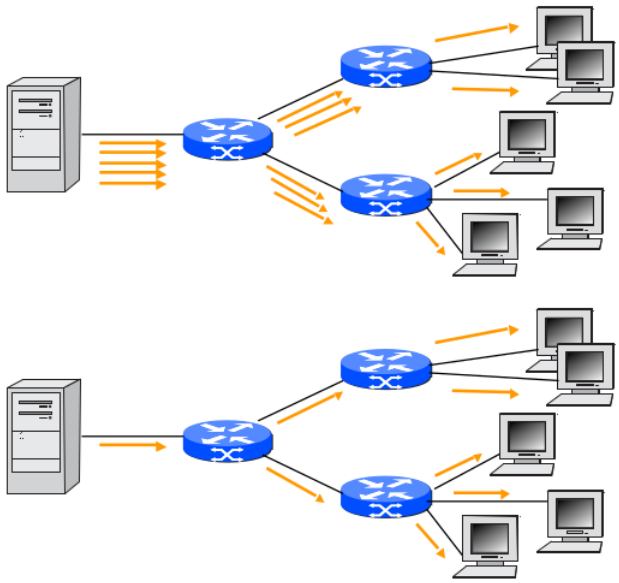

Abbildung 1: Senden von Nachrichten unter Nutzung von IP-Unicast (oben) und IP-Multicast (unten), jeder Pfeil stellt eine einzelne Nachricht dar [2]

Der einzige Unterschied eines IP-Multicast Pakets, zu einem normalen IP-Paket, besteht in seiner Zieladresse. Für IP-Multicast sind spezielle IP-Adressbereiche festgelegt, von $224.0.0.0$ bis $239.255.255.255$ Diese Bereiche repräsentieren Gruppen von Teilnehmern.

Den Inhalt eines IP-Multicast-Pakets lässt sich mit bekannten Methoden verschlüsseln. Das Problem liegt allerdings bei der Vereinbarung von gemeinsamen Schlüsseln. Da der *Diffie-Hellman-Schlüsselaustausch* nur bei zwei Teilnehmern funktioniert, wurden verschiedene Herangehensweisen zu dessen Verallgemeinerung entwickelt.

(Hinweis: "Die modulo p-Reduktionen wurden der leichteren Lesbarkeit halber weggelassen, sind aber in jedem Rechenschritt vorzunehmen."[2])

Zentralisierte Schlüsselvereinbarung

In der zentralisierten Schlüsselvereinbarung ist der sogenannte *Group Controller and Key Server (GCKS)* dafür zuständig, an alle Teilnehmer einer Gruppe Schlüssel zu senden. Außerdem besitzt er das exklusive Recht Teilnehmer aufzunehmen und auszuschließen.

Conditional Access System

Conditional Access Systeme sollen als Beispiel für eine zentralisierte Schlüsselvereinbarung dienen. Diese werden beispielsweise von Pay-TV-Anbietern genutzt. Nur ihre zahlenden Kunden dürfen ihr gesendetes Programm empfangen.

Hierzu werden Video- und Audiodaten mit einem *Control Word* verschlüsselt. Das *Control Word* wird zusammen mit zu prüfenden Bedingungen, beispielsweise Altersanforderungen, in einer *Entitlement Control Message (ECM)* übertragen. Diese *ECM* wird wiederum mit einem *Service Key (SK)* verschlüsselt und authentisiert.

Der *SK* befindet sich in modernen Pay-TV-Systemen auf einer Chipkarte. Nachdem die Chipkarte erfolgreich die Bedingungen der *ECM* geprüft und das *Control Word* entschlüsselt hat, beginnt das Dekodieren der Videodaten.

Schlüsselhierarchien

In *Conditional Access Systemen* werden Schlüsselhierarchien genutzt, um effizient *Service Keys* an Kunden zu versenden. Hierzu werden Chipkarten mit Kartennummer i mit individuellen Schlüsseln PK_i ausgestattet. Dann werden mehrere Kunden zu Gruppen j zusammengefasst, denen Gruppenschlüssel GK_j zugeordnet werden. Die *ECM* wird dann nur noch mit Gruppenschlüsseln verschlüsselt, was die Anzahl zu sendender Nachrichten verringert. Ein Gruppenschlüssel muss somit nur geändert werden, sollte ein Kunde sein Abonnement kündigen.

Dezentralisierte Schlüsselvereinbarung (Diffie-Hellman)

Konferenzschlüsselsystem von Ingemarsson, Tang und Wong (1982)

Das Konferenzschlüsselsystem stellt eine Verallgemeinerung des Diffie-Hellman-Schlüsselaustauschs für mehr als zwei Teilnehmer dar. Im DHS werden die Schlüssel im Exponenten miteinander multipliziert, wobei die Multiplikation eine symmetrische Funktion darstellt. Die Reihenfolge der Parameter ändert nichts am Ergebnis:

$$g^{f(a,b)} = g^{a \cdot b} = g^{b \cdot a} = g^{f(b,a)}$$

Die Funktion (in diesem Fall Multiplikation) lässt sich auch auf eine beliebige Anzahl Teilnehmer verallgemeinern, da sie symmetrisch ist.

Im Konferenzschlüsselsystem verschlüsselt jeder Teilnehmer die gemeinsame Zahl g mit seinem privaten Schlüssel und sendet dies als Nachricht an seinen Nachfolger. Im nächsten Schritt wird die soeben erhaltene Zahl mit wiederum dem eigenen privaten Schlüssel verschlüsselt. Dies wird soweit fortgesetzt, bis g mit dem privaten Schlüssel jedes Teilnehmers verschlüsselt wurde. Somit ist nach $n-1$ Runden jeder Teilnehmer im Besitz des Gruppenschlüssels k:

$$k = g^{a_n \cdot a_{n-1} \cdot \ldots \cdot a_1}$$

Burmester-Desmedt-Protokoll

Das Burmester-Desmedt-Protokoll verallgemeinert wie Ingemarsson et al. den Diffie-Hellman-Schlüsselaustausch auf eine beliebige Anzahl Teilnehmer. Jedoch werden nur zwei Runden an Nachrichtenaustausch benötigt und ist dadurch im Gegensatz zu Ingemarsson et al. praktikabel und skalierbar.

Es wird die Eigenschaft der Zyklizität der Multiplikation genutzt. Eine dreistellige Funktion ist zyklisch, wenn gilt:

$$f(a,b,c) = f(c,a,b) = f(b,c,a) = f(a,b,c)$$

Teilnehmer mit zugehörigen Geheimnins i haben jeweils einen Vorgänger und Nachfolger und durchlaufen folgende Runden:

1. Runde: Teilnehmer I sendet $z_I = g^i$ an Nachfolger und Vorgänger
2. Runde: Teilnehmer I sendet $X_I = (z_{I+1}/z_{I-1})^i$ an Nachfolger und Vorgänger

Der Gruppenschlüssel K berechnet sich wie folgt:

$$K_I = z_{I-1}^{n \cdot i} \cdot X_I^{n-1} \cdot X_{I+1}^{n-2} \cdot \ \ldots \ \cdot X_{I-2}^{1}$$

Aufnahme und Ausschluss von Mitgliedern

Unterscheidung zwischen Aufbau einer neuen Gruppe und Änderung einer bestehenden Gruppe im Jahr 1998 von Steiner, Waidner, Tsudik. Bei dem *Initial Key Agreement (IKA)*, der Schlüsselaustausch bei Aufbau einer neuen Kommunikationsgruppe, wird erstmalig ein Gruppenschlüssel erzeugt. Im Gegensatz dazu wird bei Veränderung des Gruppenschlüssels das *Auxiliary Key Agreement (AKA)* genutzt, welches zur effizienteren Berechnung eines Gruppenschlüssels dient und bereits vorhandene Informationen nutzt. Darunter fällt:

- Aufnahme neuer Teilnehmer
- Ausschluss alter Teilnehmer
- Vereinigen und Teilen von Gruppen

Für das *IKA* werden zuvor genannte Verfahren eingesetzt.

Bei der Aufnahme eines neuen Teilnehmers D im *AKA* lässt sich das Burmester-Desmedt-Protokoll effizient einsetzen. Insgesamt sind zur Aufnahme nur folgende vier Nachrichten notwendig:

1. Neuer Teilnehmer D an alle: $z_D = g^d$,
2. Neuer Teilnehmer D an alle: $X_D = (g^a / g^c)^d$
3. Nachbar A an alle: $X'_A = (g^b / g^d)^a$
4. Nachbar C an alle: $X'_B = (g^d / g^b)^c$

Ein Teilnehmer fungiert als *Group Controller* und hat bereits beim *IKA* die X_I Werte aller Teilnehmer gesammelt. Dieser überträgt nun diese, dem neuen Teilnehmer nicht bekannten Werte, an diesen. Da nun der neue Teilnehmer als einziger über alle Werte verfügt, übernimmt dieser die Rolle des *Group Controllers*.[1]

Iterierter Diffie-Hellman

Eine weitere Variante zur dynamischen Gruppenverwaltung bietet das iterierte Diffie-Hellman-Verfahren. Hierbei wird zur Gruppenbildung die Hierarchie eines Binärbaums ausgenutzt.

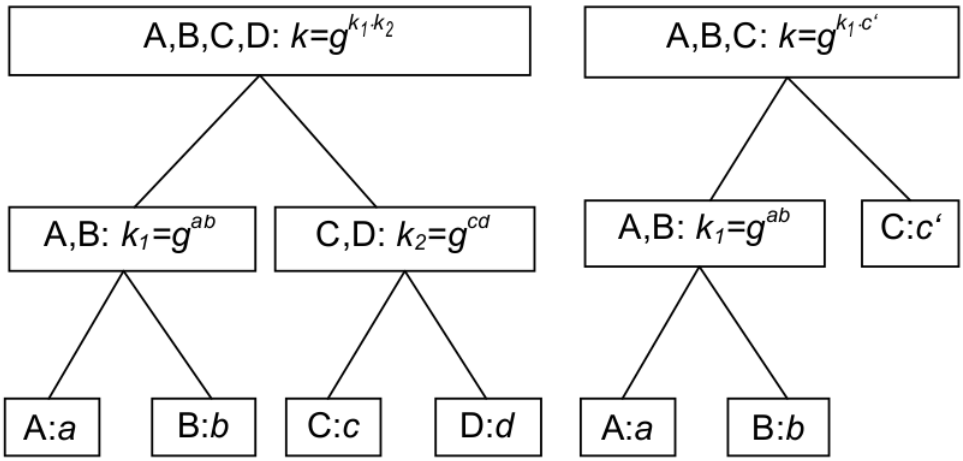

Abbildung 2: Schlüsselhierarchie des iterierten Diffie-Hellman-Verfahrens mit vier (links) und drei (rechts) Teilnehmern [2]

Zwei Teilnehmer vereinbaren einen gemeinsamen Schlüssel und als Geschwisterblätter repräsentiert. Beide werden nun als eine Gruppe angesehen. Beim Verfolgen der Baumstruktur in Richtung Wurzel repräsentiert jeder besuchte Knoten eine Supergruppe, bestehend aus den Gruppen oder Teilnehmern der Kindknoten/ Blätter.

Zwei Teilnehmer bilden zunächst einen gemeinsamen Gruppenschlüssel. Danach wird eine Ebene höher ein weiterer Gruppenschlüssel mit der anderen Gruppe/ dem anderen Teilnehmer gebildet. Dieses Verfahren wiederholt sich bis ein kompletter Gruppenschlüssel in der Wurzel des Baums gebildet wurde.

Aufnahme eines neuen Teilnehmers D:

1. An bestehenden Teilnehmer C werden zwei Blätter angehangen.
2. C und D wird jeweils ein neues Blatt zugeordnet
3. Austausch aller Schlüssel bis zur Wurzel des Baumes

Ausschluss eines Teilnehmers D:

Zugeordneter Blätter des Teilnehmers D und des Partners C werden gelöscht, C wird dem einer Ebene höher, neu entstandenem Blatt zugeordnet.

Literaturverzeichnis

[1] M. Steiner, G. Tsudik, M. Waidner, "CLIQUES: a new approach to group key agreement", Proceedings. 18th International Conference on Distributed Computing Systems (Cat. No.98CB36183). DOI 10.1109/icdcs.1998.679745.

[2] J. Schwenk, "Sicherheit und Kryptographie im Internet". Wiesbaden: Springer Vieweg, 2014. ISBN 978-3-658-06543-0.