Ein Ansatz für eine effiziente Schlüsselverteilung für kleine geschlossene Peer-Gruppen

Fuwen Liu und Hartmut König
Brandenburgische Technische Universität Cottbus
Lehrstuhl Rechnernetze und Kommunikationssysteme
PF 10 13 44, 03013 Cottbus
email: {lfw,koenig}@informatik.tu-cottbus.de

Abstract: Vertraulichkeit ist eine der Schlüsselanforderungen für geschäftliche Kommunikation über das Internet. In einer zunehmend mobilen Gesellschaft sind dabei zunehmend spontane Beratungen in Ad hoc-Umgebungen, mitunter mit wechselnden Partnern, erforderlich. Um die Vertraulichkeit der Beratung zu sichern, müssen sich die Partner auf einen gemeinsamen Schlüssel einigen, mit dem sie ihre Kommunikation verschlüsseln. Audio- und Videokonferenzsysteme, die auf einem zentralistischen Ansatz beruhen, bieten dafür praktikable Lösungen an. Dezentrale Lösungen, die dem Peer-to-Peer-Ansatz folgen, bieten hierfür flexiblere Lösungen, die Spontaneität und Flexibilität besser unterstützen. Ein effizienter Schlüsselaustausch stellt für solche Systeme noch eine Herausforderung dar. In diesem Beitrag stellen wir das Schlüsselverteilungsprotokoll VTKD vor, das speziell für den Schlüsselaustausch von kleinen dynamischen Peer-Gruppen mit bis zu 100 Partnern entworfen wurde. Es besteht aus zwei Bestandeilen: einer gegenseitigen Authentifizierung der Partner und einer sicheren Verteilung des Sitzungsschlüssels an die Partner. Der Beitrag beschreibt das Prinzip der sicheren Verteilung.

1 Motivation

Moderne gruppenorientierte und kollaborative Applikationen nutzen verstärkt das Peer-to-Peer-Prinzip. Das bietet gegenüber zentralistischen Ansätzen den Vorteil einer größeren Unabhängigkeit von einer möglicherweise teuren Infrastruktur, wie sie z. B. für Audio- und Videokonferenzen mit H.32x-Systemen existiert. Dezentrale Systeme erweisen sich hier flexibler, da es keinen *Single Point of Failure* gibt und sich die Abhängigkeit von einer Infrastruktur reduziert. Dezentrale Lösungen unterstützen insbesondere spontane Treffen und die Mobilität der Partner. Dies ist insbesondere für die geschäftliche Kommunikation über das Internet von Vorteil. Dezentrale Lösungen erfordern jedoch auch entsprechende Mechanismen, um die Vertraulichkeit der geschäftlichen Absprachen abzusichern. Dazu sind insbesondere Verfahren für den Schlüsselaustausch erforderlich, die eine konsistente Erneuerung der Schlüssel bei allen Gesprächspartnern sichert. Während für zentralistische Ansätze praktikable Lösungen existieren, ist die Entwicklung effizienter und sicherer Protokolle für verteilte Lösungen noch Gegenstand der Forschung.

Eine sichere Kommunikation zwischen einer Gruppe von Geschäftspartnern erfordert, dass nur die aktiven Partner den aktuellen Gruppen- bzw. Sitzungsschlüssel teilen, um die ausgetauschten Daten zu verschlüsseln. Bei einer sich möglicherweise ändernden Gruppenzusammensetzung kann es darüber hinaus gewünscht und gefordert sein, dass Inhalte und Gegenstand der Beratung Partnern, die später beitreten oder diese eher verlassen, nicht zugänglich werden. Wir betrachten im hier diese komplexere Variante einer vertraulichen Beratung. Varianten mit geringeren Vertraulichkeitsanforderungen an eine sich verändernde Gruppenzusammensetzung können daraus abgeleitet werden. Fast selbstverständlich erscheint daneben die Forderung nach einem effizienten Schlüsselaustauschprotokoll, um die Interferenzzeiten in der Kommunikation für die Schlüsselerneuerung, insbesondere für Realzeit-Anwendungen wie Audio- und Videokonferenzen zu minimieren, da im asynchronen Internet Hosts i. d. R. nicht in Lage sind die Schlüssel synchron zu erneuern [3], [4].

In diesem Beitrag stellen wir das Grundprinzip des Schlüsselaustausch-Protokoll VTKD (*virtual token based key distribution*) vor. VTKD ist ein Schlüsselverteilungsprotokoll, das insbesondere die Schlüsselerneuerung in kleinen geschlossenen Peer-Gruppen mit bis zu 100 Mitgliedern unterstützen soll. Es erfüllt u. a. Sicherheitsanforderungen wie Schlüsselauthetifitizität, Vorwärts- und Rückwärtsvertraulichkeit, Kollusions-Freiheit und Resistenz gegen bekannte Schlüsselattacken [1], [2]. VTKD weist im Vergleich zu anderen Schlüsselaustauschprotokollen eine bessere Effizienz auf. Das Protokoll ist im Kontext der Videokonferenzforschung an unserem Lehrstuhl entstanden. Es ist Bestandteil der Sicherheitsarchitektur des Mehrteilnehmer-Videokonferenzsystems BRAVIS [5], um vertrauliche Videokonferenzen zu unterstützen. Der Begriff der geschlossenen Gruppe bezieht sich dabei auf eine Gruppenzusammensetzung, in der sich alle Teilnehmer kennen. Der Beitritt zur Gruppe erfolgt über eine explizite Einladung, die bei einer vertraulichen Konferenz mit einer Authentifizierung der Partner verbunden ist. Die angestrebte Obergrenze von 100 Teilnehmern ist sehr großzügig ausgelegt. Im Alltag haben Geschäftsberatungen häufig weniger als 15 Teilnehmer. VTKD besteht aus zwei Bestandeilen: einer gegenseitigen Authentifizierung der Partner und einer sicheren Verteilung des Sitzungsschlüssels an die Partner. Für die gegenseitige Authentifizierung wird Internet-Protokoll IKEv2 genutzt. Dieser Beitrag kann sich nur auf die Skizzierung des Prinzips der sicheren Schlüsselverteilung beschränken.

2 Prinzip von VTKD

VTKD ist ein verteiltes Schlüsselverteilungsprotokoll, das auf dem Prinzip des Schlüsselaustauschs nach Diffie-Hellman (DH) beruht [6], d. h. es gibt keine zentrale Schlüsselverwaltung. Im Unterschied zum Schlüsselaustausch zwischen zwei Partnern berechnet beim verteilten Ansatz jedes Gruppenmitglied mit jedem Partner einen geheimen Schlüssel nach dem Diffie-Hellmann-Prinzip, der im Weiteren als gemeinsames oder zweiseitiges DH-Geheimnis bezeichnet wird. Diese zweiseitigen Geheimnisse werden bei den Gruppenmitgliedern gespeichert und werden dann für die Verteilung des Gruppenschlüssels genutzt. Bezüglich der Gruppenmitglieder wird angenommen, dass sie dieselben Rechte haben und ihnen das gleiche Vertrauen

entgegengebracht wird. Das bedeutet, dass jedes Gruppenmitglied ein neues Mitglied authentifizieren darf und den Gruppenschlüssel erneuern kann. Wir nehmen ferner an, dass ein in die Gruppe aufgenommenes Mitglied vertrauenswürdig ist und nicht aktiv versucht die Beratung zu stören oder den Sitzungsschlüssel an Nichtmitglieder weiterzugeben. Es werden jedoch keine Annahmen über die Vertrauenswürdigkeit der Partner nach dem Verlassen der Gruppe getroffen. Diese Annahmen entsprechen der praktischen Verfahrensweise.

VTKD ist ein Token-Protokoll. Nur der Tokenhalter hat jeweils das Recht zur Erneuerung des Gruppenschlüssels und zur Authentifizierung beitretender Partner. VTKD verwendet jedoch nur ein virtuelles Token. Virtuell bedeutet in diesem Fall, dass die Position des virtuellen Tokens und damit des Tokenhalters für jede Schlüsselverteilung neu berechnet wird. Damit wird die explizite Tokenweitergabe mit allen damit verbundenen Problemen wie Tokenverlust und -dopplung vermieden. Die neue Tokenposition *PT* wird wie folgt berechnet:

$$PT = VK \bmod n \qquad (1)$$

wobei bezeichnet *VK* die jeweilige Versionsnummer des Gruppenschlüssels und *n* die Gruppengröße bezeichnet. *VK* wird bei jeder Erneuerung des Gruppenschlüssels um 1 erhöht. Neben der Bestimmung der Tokenposition wird die Versionsnummer im Protokoll auch dazu genutzt Replay-Attacken zu vermeiden. Die Gewährleistung einer virtuellen Synchronisation durch das unterliegende Gruppenkommunikationsprotokoll sichert, dass jedes Mitglied die aktuelle Gruppengröße und die Schlüsselversion kennt und damit die Position des virtuellen Tokens eindeutig bestimmen kann.

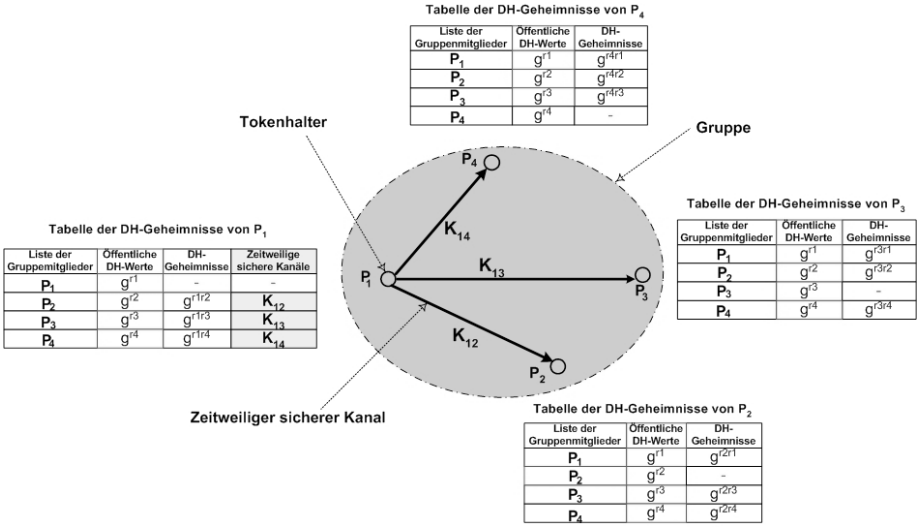

Abb.1: Schlüsselverteilung über zeitweilige sichere Kanäle

Die Schlüsselerneuerung wird, wie eingangs bereits erwähnt, durch eine Veränderung der Gruppenzusammensetzung ausgelöst. Der jeweilige Tokenhalter generiert einen neuen Schlüssel und beginnt mit der Verteilung an die Gruppenmitglieder. Dazu baut er zeitweilige separate Kanäle zu jedem Gruppenmitglied unter Nutzung des gespeicherten gemeinsamen DH Geheimnisses auf. Abbildung 1 zeigt das Prinzip an einer Gruppe von vier Teilnehmern (P_1, P_2, P_3 und P_4), wobei P_1 der aktuelle Tokenhalter sei. Jedes Mitglied kennt sein Geheimnis mit den anderen Teilnehmern. So speichert P_1 die Geheimnisse g^{r1r2}, g^{r1r3}, und g^{r1r4}, P_2 entsprechend die Geheimnisse g^{r2r1}, g^{r2r3}, und g^{r2r4} usw. P_1 baut dann unter Verwendung der gemeinsamen Geheimnisse g^{r1r2}, g^{r1r3}, g^{r1r4} geheime Kanäle K_{12}, $K_{13,}$ and K_{14} zu P_2, P_3, und P_4 auf, über die er dann den neuen Gruppenschlüssel verteilt. Die separaten geheimen Kanäle sind durch einen geheimen Schlüssel K_{ij} definiert, der zwischen den beiden Gruppenmitgliedern berechnet wird. Dabei wird folgendes Berechnungsschema benutzt:

$$K_{ij-e} = H(g^{rirj}, g^{rirj} \| N_i \| ID_i \| ID_j \| 0) \qquad (2)$$

$$K_{ij-a} = H(g^{rirj}, g^{rirj} \| N_i \| ID_i \| ID_j \| 1) \qquad (j=1, 2,...n \text{ and } j \neq i) \qquad (3)$$

Es wird ein Schlüsselpaar berechnet. $K_{ij\text{-}e}$ wird für die Verschlüsselung der Nachricht genutzt, während $K_{ij\text{-}a}$ zur Prüfung der Authentizität der Nachrichten dient. Die Erzeugung der Schlüssel erfolgt mit Hilfe einer kryptographischen Hash-Funktion H(*k,M*) berechnet, wobei *k* eine Schlüssel und *M* die Nachricht bezeichnet. In unserem Fall wird HMAC genutzt. In die Berechnung gehen das gemeinsame Geheimnis zwischen dem Tokenhalter und dem Gruppenmitglied, ihre Identitäten *ID* und eine Zufallszahl *N* ein, die der Tokenhalter an das Gruppenmitglied schickt. Das Symbol „|“ bedeutet dabei Verkettung.

Die entscheidende Vorbedingung für VTKD ist, das jedes Gruppenmitglied jeweils die gemeinsamen DH Geheimnisse mit den anderen Gruppenmitgliedern entsprechend der aktuellen Gruppenzusammensetzung besitzt. Diese Vorbedingung ist einfach zu erfüllen. Wenn ein Gruppenmitglied die Gruppe verlässt, löschen die verbleibenden Mitglieder jeweils das zugehörige Geheimnis in ihren Tabellen. Der umgekehrte Fall ist komplizierter, da das neue Gruppenmitglied wie auch die alten Mitglieder jeweils nicht den öffentlichen DH-Wert der Gegenseite kennen. Deshalb sendet der Tokenhalter während der Authentifizierungsphase alle öffentlichen DH-Werte der Gruppe an das neue Mitglied. Umgekehrt übergibt das neue Mitglied seinen öffentlichen DH-Wert an den Tokenhalter, der es an die Gruppenmitglieder weiterleitet. Jedes Gruppenmitglied berechnet dann das gemeinsame Geheimnis mit dem neuen Mitglied. Damit ist die Vorbedingung wieder erfüllt und jedes Mitglied könnte die Schlüsselerneuerung und –verteilung ausführen, falls ihm das Token zugewiesen wird.

3 Schlussbemerkung

In dem vorliegenden Beitrag haben wir ein neues Schlüsselverteilungsprotokoll vorgestellt, das ein einfaches und intuitives Prinzip nutzt. VTKD erweist sich für den

angestrebten Einsatz für kleine dynamische Peer-Gruppen effizienter als existierende Protokolle. Die spezifizierte Obergrenze von 100 Teilnehmern ist sehr großzügig ausgelegt. In der Regel sind für vertrauliche Treffen viel weniger Teilnehmer üblich. Grundlage für das vorgestellte Prinzip ist die Verwendung eines Gruppenkommunikationsprotokolls, das eine virtuelle Synchronisation der Partner gewährleistet. Solche Protokolle existieren in der Zwischenzeit und wie in [7] gezeigt wird, sind damit sogar Konferenzen im EU-Bereich möglich. VTKD wird gegenwärtig in das verteilte Mehrteilnehmer-Videokonferenzsystem BRAVIS zur Unterstützung vertraulicher Konferenzen integriert.

Literaturverzeichnis

[1] J. Snoeyink, S. Suir, and G. Vorghese: A Lower Bound for Multicast Key Distribution. IEEE INFOCOM 2001, pp. 422-431.

[2] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone: Handbook of applied cryptography, CRC Press series on discrete mathematics and its applications, 1997.

[3] P. McDaniel, A. Prakash, and P. Honeyman: Antigone: A Flexible Framework for Secure Group Communication“, CITI Technical Report 99-2, University of Michigan, September 8, 1999

[4] P. S. Krus: A survey of multicast security issues and architectures. 21st National Information Systems Security Conference (NISSC), Oct. 1998. http://csrc.nist.gov/nissc/1998/proceedings/paperF10.pdf.

[5] The BRAVIS video conference system. http://www.bravis.tu-cottbus.de

[6] E. Rescorla: Diffie-Hellman Key Agreement Method. RFC 2631, June 1999.

[7] M. Zuehlke, and H. Koenig: A Signaling Protocol for Small Closed Dynamic Multipeer Groups. In Z. Mammeri and P. Lorenz (eds.): High Speed Networks and Multimedia Communications (HSNMC 2004). Springer-Verlag, Berlin, Heidelberg 2004, pp. 973 – 984