Σ 5/5

Cihasev Adam
Erdogan Ibrahim
Jaber Muhamed

Rechnernetze – Media Networking (WiSe 2023/2024)

Übung 01

Aufgabe 1) In einem fiktiven Netztyp bietet eine technische Weiterentwicklung eine gegenüber der Originalversion verzehnfachte Datenrate an. Inwiefern wirkt sich dies auf die Paketlaufzeiten aus: Was ändert sich? Was bleibt unverändert? Kurze Begründung

Eine Datenrate gibt an, wie viele Informationen in einer bestimmten Zeit übertragen werden können. Wichtige Entwicklungen bezüglich Netze/Netzkopplungen ist die Steigerung der Bandbreite (Ethernet-Generationen). Diese Entwicklungen zeigen, dass leitungsgebundene Netze auf Glasfasertechnik basieren, die kaum Bitkipper aufweisen – nur auf sehr kurzen Strecken (aufgrund von Kupferleitungen). Die höheren Übertragungsraten sind mit kürzen Bits zu begründen – folgen also in einer höheren Taktung schneller aufeinander. Dennoch ist ein vollständiges Paket bei einer höheren Übertragungsrate schneller übertragen, weil die Bits eben schneller aufeinander folgen.

Abbildung 1 Paketlaufzeit

Im Grunde bedeutet eine verzehnfachte Datenrate, dass mehr Daten in derselben Zeit übertragen werden können. Dies kann zu einer Verringerung der Paketlaufzeit führen, da mehr Datenpakete gleichzeitig übertragen werden. Es ist jedoch wichtig zu beachten, dass die Paketlaufzeit nicht nur von der Datenrate abhängt, sondern auch von anderen Faktoren wie der Netzwerklatenz, die Menge an Daten und die Auslastung des Netzwerks. Diese Faktoren bleiben unverändert, wenn nur die Datenrate erhöht wird. Die Netzwerklatenz, also die Zeit, die ein Datenpaket benötigt, um vom Sender zum Empfänger zu gelangen, hängt von der physischen Distanz und der Qualität der Netzwerkinfrastruktur ab. Die Menge an Daten, die in einem einzelnen Paket gesendet werden können, hängt von der Netzwerktechnologie ab. Ein weiterer unveränderter Faktor ist der Quality of Service (Sicherstellung einer hohen Dienstgüte). Denn eine höhere Datenrate allein verbessert nicht notwendigerweise die Qualität einer Übertragung. So sind z.B. Paketverluste nicht ausgeschlossen und die Zuverlässigkeit bleibt weiterhin relevant.

2 Punkte

Cihasev Adam
Erdogan Ibrahim
Jaber Muhamed

Aufgabe 2) In einer fiktiven Gruppenkommunikation soll ein asymmetrisches Verschlüsselungsverfahren für die Authentisierung der Nachrichten verwendet werden. Wäre dies ein Problem? Begründung.

Für eine echte Gruppenkommunikation braucht man eine Mehrpunktbeziehung. Dabei ist das Erreichen der Kommunikationspartner abhängig von der Netztopologie: Bei Bussen, Ringen und Funkzellen erreichen die Nachrichten sowieso alle Teilnehmer, hier muss beim Empfängersystem entsprechend gefiltert werden. Bei Sternen und Bäumen gibt es nur einen Weg zu jedem Knoten, wenn Nachrichten auf sämtlichen Links einmal verteilt sind, dann sind alle Empfängersysteme einbezogen. Allerdings könnte es sein, dass nicht alle Knoten eines Sterns oder Baums zu einer Gruppe gehören, daher wäre es nützlich ein Verfahren zu haben, welches sicherstellt, dass nur die relevanten Links bedient werden. In einer Gruppenkommunikation muss die Mehrpunktbeziehung auch entsprechend verwaltet werden. Daher sollte auf folgende Fragen Antworten geliefert werden: Wer darf teilnehmen? Können Teilnehmer später kommen bzw. früher gehen? Wer darf Informationen senden? Wie wird eine zuverlässige Übertragung erreicht? (…). Im Hinblick der oben aufgeführten Thematik wird im Rahmen der Kommunikationsanforderung, hier Folie 33 " rnmn-01-ueberblick.pdf" in Rechnernetze-Media Networking (WiSe2023/2024), Punkt f) Sicherheitsanforderungen, das in Abbildung 1 aufgeführte Szenario näher erläutert. In dem dort abgebildeten Konferenzszenario ist ein potenzieller Angriff von C nicht ausgeschlossen. Durch das dadurch entstandene Anzapfen des Kanals, kann C unerlaubt Informationen lesen, ändern und als Sender ausgeben. Solche Angriffe können nicht mit Sicherheit verhindert werden, aber durch die Anwendung von Verschlüsselungsverfahren können negative Folgen minimiert bzw. vermieden werden.

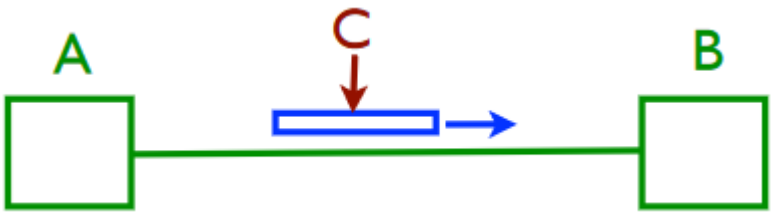

Abbildung 2 Kommunikationskanal mit Angriffspotential

In Bezug auf Telekonferenzen ist der Einsatz von Verschlüsselungsverfahren zu empfehlen, die keine erhebliche Zeit in Anspruch nehmen. Das liegt an den zeitabhängigen Strömen (würde zusätzliche Verzögerung bedeuten). Daten, die geheim gehalten werden, dürfen nur von Nutzern/Geräten/Systemen verändert oder eingesehen werden, die dazu berechtigt sind.

Cihasev Adam
Erdogan Ibrahim
Jaber Muhamed

Um auf geheim gehaltene Daten zugreifen zu können, muss ein Nutzer/Gerät/System sich zuerst authentisieren, also beweisen, dass er/sie/es berechtigt ist, die Daten einzusehen / zu verändern. Kommunikationskanäle sind hier potenziellen Angriffen ausgesetzt, da ein Eindringling (Man in the Middle) einen Kanal anzapfen kann und so die Gefahr besteht, dass dieser sich als der Sender ausgibt und Informationen unerlaubt gelesen oder verändert werden.

Nehmen wir nun an, dass wir asymmetrische Verschlüsselungsmethoden zur Authentifizierung von Nachrichten in einer Gruppenkommunikation einsetzen wollen. Dies ist mit digitalen Signaturen realisierbar. In einer Gruppenkommunikation würde der Prozess in folgenden Schritten ablaufen: Der Absender der Nachricht berechnet eine digitale Signatur für die Nachricht. Dazu berechnet er den Hashwert der Nachricht und verschlüsselt ihn mit seinem öffentlichen Schlüssel. Zuletzt fügt er die Signatur an die Nachricht an und sendet sie an die Empfänger bzw. an eine Gruppe. Die Empfänger können die Signatur anhand des öffentlichen Schlüssels des Absenders verifizieren. Dadurch werden die Authentizität und Integrität der Nachricht sichergestellt. Die einzige Frage, die sich dabei stellt, ist, wie der öffentliche Schlüssel den Empfängern übermittelt werden soll. Hierbei bieten sich zwei Möglichkeiten an:

nee

1. **Versenden des Schlüssels in einer Nachricht**
   Bei der ersten Variante sendet der Absender seinen öffentlichen Schlüssel als herkömmliche Nachricht an die Gruppe. Dies bedeutet, dass die allererste Nachricht, nämlich die mit dem Schlüssel, nicht authentifiziert werden kann und auch anfällig für Man-in-the-Middle-Angriffe ist. Darüber hinaus ändern sich die Gruppen dynamisch, d. h. neue Mitglieder treten bei oder derzeitige Mitglieder verlassen die Gruppe. Zwar könnte der Schlüssel periodisch verteilt werden, doch wäre dies nur in sehr kurzen Abständen sinnvoll, was wiederum die Bandbreite überlasten würde. Schließlich könnte sich generell jeder Angreifer als legitimer Absender ausgeben - und notfalls auch seine IP-Adresse vortäuschen - und einen eigenen öffentlichen Schlüssel an die Gruppenmitglieder weiterreichen, was wiederum zu Konflikten führen würde, wenn mehrere Schlüssel im Umlauf sind.
2. **Veröffentlichung des Schlüssels in einem Online-Dienst**
   Bei dieser Variante wird der öffentliche Schlüssel in einem vertrauenswürdigen Online-Dienst veröffentlicht. Hier müssen die Gruppenmitglieder den Schlüssel von dem Dienst abrufen, bevor sie der Gruppe beitreten. Dies kann ein effizienterer und zuverlässigerer Ansatz sein, da die Schlüsselverteilung zentralisiert ist. Allerdings erfordert dies die Mitwirkung der Mitglieder beim Abrufen des Schlüssels.

Cihasev Adam
Erdogan Ibrahim
Jaber Muhamed

Weiterhin sind keine asymmetrischen Verfahren bei einer Gruppenkommunikation zur Geheimhaltung möglich, da hierbei der öffentliche Schlüssel des Partners beim Verschlüsseln verwendet wird. Wenn man mehrere Kommunikationspartner hat, dann kann man auf diese Weise keine gemeinsame Nachricht für alle dieser Partner produzieren. Jeder dieser Partner müsste diese Nachricht mit seinem eigenen privaten Schlüssel entschlüsseln können (asymmetrische Verfahren sind für Geheimhaltungszwecke selten in Gebrauch). Dahingegen wird bei symmetrischer Verschlüsselung ein gemeinsamer Sitzungsschlüssel benötigt. Diesen Schlüssel müsste man unter Verwendung geeigneter Verfahren aushandeln (…).

1 Punkt

Aufgabe 3) In einer fiktiven Gruppenkommunikation wird die folgende IPv4-Adresse verwendet: 228.058.214.102.

a) Wie sieht die zugehörige Ethernet-Gruppenadresse aus?

b) Auf welche Weise könnte sich die zugrundeliegende Adressabbildung als suboptimal herausstellen? Wie kann man damit umgehen?

Aufgabe 3a)

Die Ethernet-Gruppenadresse ist 48 Bit lang. Die erste Hälfte der Adresse wird für die Herstellerkennung als Organizationally Unique Identifier (OUI) verwendet, gefolgt von dem Multicast-Bit, welches auf 0 gesetzt wird. Das OUI der IETF setzt sich in Hexadezimal wie folgt zusammen: 01 00 5E.

In Binär wäre das also (laut Tabelle): 0000 0001 0000 0000 0101 1110

gefolgt von der 0 als Multicast Bit, bleiben 23 Bits übrig. Diese werden auf die letzten 23 Stellen der IPv4-Adresse gesetzt.

IPv4-Adresse: 228.058.214.102.

Umwandlung in Binär:

1 Oktett	2 Oktett	3 Oktett	4 Oktett
228:2 = 114, Rest = 0 (Rest im Folgenden mit R abgekürzt) 114:2 = 57, R = 0 57:2 = 28, R = 1 28:2 = 14, R = 0 14:2 = 7, R = 0 7:2 = 3, R = 1 3:2 = 1, R = 1	58:2 = 29, R = 0 29:2 = 14, R = 1 14:2 = 7, R = 0 7:2 = 3, R = 1 3:2 = 1, R = 1 1:2 = 0, R = 1 Es ergibt sich: **0011.1010**	214:2 = 107, R = 0 107:2 = 52, R = 1 52:2 = 26, R = 1 26:2 = 13, R = 0 13:2 = 6, R = 1 6:2 = 3, R = 0 3:2 = 1, R = 1 1:2 = 0, R = 1	102:2 = 51, R = 0 51:2 = 25, R = 1 25:2 = 12, R = 1 12:2 = 6, R = 0 6:2 = 3, R = 0 3:2 = 1, R = 1 1:2 = 0, R = 1 Es ergibt sich: **0110.0110**

Cihasev Adam
Erdogan Ibrahim
Jaber Muhamed

1:2 = 0, R = 1 Gelesen von unten nach oben ergibt sich: **1110.0100**		Es ergibt sich: **1101.0110**	

Tabelle 1 Umwandlung in Binär

Insgesamt lautet die IPv4 binär: 1110.0100.0011.1010.1101.0110.0110.0110
Mit den 23 letzten Bits: 011.1010.1101.0110.0110.0110
Die zugehörige Ethernet-Gruppenadresse lautet dann:
0000 0001 0000 0000 0101 1110 0011 1010 1101 0110 0110 0110

Aufgabe 3b)
Um die Abbildung von IPv4-Gruppenadressen auf Ethernet-Adressen zu ermöglichen, ist eine spezielle Lösung erforderlich. Denn IPv4-Adressen sind 32 Bit lang, wobei lediglich 28 Bits für die Gruppennummer zur Verfügung stehen. Ethernet-Adressen hingegen sind 48 Bit lang, wobei das erste Bit das Multicast-Bit ist und die erste Hälfte der Adresse als OUI (Organizationally Unique Identifier) für die Herstellerkennung verwendet wird. Dies bedeutet, dass die Ethernet-Adressen nicht direkt 1 zu 1 von den IPv4-Gruppenadressen abgeleitet werden können. Um dennoch eine Abbildung zu ermöglichen, hat die IETF (Internet Engineering Task Force) ein eigenes OUI-Präfix beschafft, das speziell für die Verwendung in Ethernet-Gruppenadressen vorgesehen ist. Das nächste Bit in der Ethernet-Adresse wird auf 0 gesetzt, wodurch 23 Bits übrigbleiben, die für die eigentliche Abbildung der Gruppenadressen verwendet werden können. In der Praxis bedeutet dies, dass die 23 niederwertigen Bits der IPv4-Gruppenadresse direkt in die Ethernet-Adresse übernommen werden. Obwohl dies zu einer gewissen Redundanz führt, da die 28-Bit-IPv4-Gruppenadresse auf die 23-Bit-Ethernet-Adresse abgebildet wird, ermöglicht diese Methode dennoch die effektive Weiterleitung von Multicast-Paketen im lokalen Netzwerk. Das bedeutet, dass 32 verschiedene IP-Gruppen-Adressen dieselbe Ethernet Gruppen-Adresse bekommen. Daher gibt es keine Garantie von Eindeutigkeit, aber es ist praktisch sehr wahrscheinlich, weil es eben unwahrscheinlich ist, dass es in einem Netz gleichzeitig zwei Gruppen gibt, die dieselben 23 letzten Stellen in ihrer Gruppen-Adresse haben. Die Pakete dieser Gruppen können in der IP-Implementierung des Empfänger-Systems aussortiert werden.

Quellen:
https://www.mathe-lexikon.at/mengenlehre/zahlensysteme/hexadezimalzahlen/hexadezimalzahl-in-binaerzahl-umrechnen.html

2 Punkte