Karlsruher Institut für Technologie

Institut für Telematik
Karlsruher Institut für Technologie (KIT)
Prof. Dr. M. Zitterbart
T. Gerhard, M.Sc.
M. Flittner, M. Sc.
M. Jung, M. Sc.
S. Friebe, M. Sc.

Einführung in Rechnernetze
Sommersemester 2017

7. Übungsblatt

Aufgabe 1: E-Mail: Komplettsicht

Abbildung 1 zeigt Ihr LAN-Netz. Als technikbegeisterter Mensch haben Sie sich einen eigenen E-Mail-Server auf Ihrem Rechner eingerichtet. Auf diesem haben Sie die E-Mail-Adresse `admin@myawesomemailserver.com`

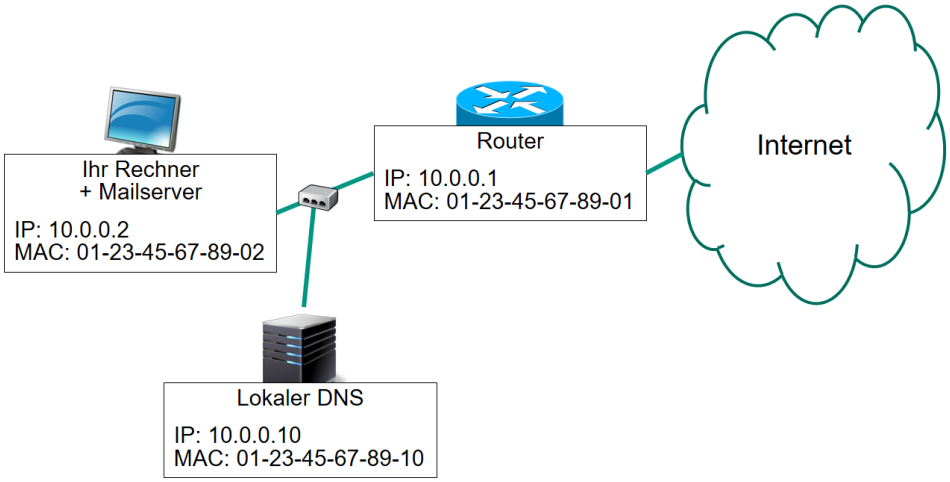

Abbildung 1: Lokales Netzwerk. Die drei Geräte sind über einen **Ethernet-Hub** verbunden.

Nun möchten Sie eine E-Mail an Ihre Freundin Alice senden. Die E-Mail-Adresse lautet `schickmirnichts@gmail.com`. Der Inhalt Ihrer Nachricht, die Sie am 11. Juli 2017 um 13:00 Uhr verfasst haben, lautet:

```
Betreff: Hallo!

Hallo Alice,
wie geht es dir? Habe schon lange nichts mehr gehoert!
Gruesse!
```

(a) Wie sieht die via SMTP-DATA übertragene Nachricht aus?

(b) Die E-Mail befindet sich von nun an bereits in Ihrem E-Mail-Server - dieser muss sie nun an den Mailserver des Empfängers zustellen. Zum weiteren Übertragen benötigt Ihr Rechner dazu die IP-Adresse des Ziel-Mailservers. Alle Caches seien zu Beginn leer. Um diese IP-Adresse mit Hilfe von DNS zu ermitteln wird jedoch erst die **MAC-Adresse des lokalen Nameservers** benötigt. Mit welchem Protokoll ermittelt er diese MAC-Adresse, und welche Rahmen (inkl. Inhalte) werden dafür durch das lokale Netz geschickt?

(c) Zeichnen Sie in einem Weg-Zeit-Diagramm den **Ablauf der DNS-Abfrage** ein, wenn Ihr Rechner rekursiv am lokalen Nameserver fragt, und dieser iterativ die notwendigen Nameserver im Internet befragt.

Hinweis: Nutzen Sie zur Lösung dieser Aufgabe ein DNS-Anfragetool wie *dig* oder *nslookup*. Beachten Sie, dass ein einzelner Nameserver durchaus für verschiedene DNS-Zonen zuständig sein kann.

(d) Nehmen Sie nun an, alle Nameserver arbeiten rekursiv. Wie sähe die Anfrage dann aus?

(e) An welche **MAC-Adresse** sendet **Ihr Rechner** nun die Ethernet-Rahmen, welche die IP-Pakete zur Übertragung der E-Mail enthalten?

(f) Nehmen Sie an, dass jede SMTP-Nachricht in einem eigenen TCP-Segment übertragen wird. Zeichnen Sie in einem Weg-Zeit-Diagramm alle TCP-Segmente ein, die zur Übertragung der E-Mail zwischen Ihrem Rechner und dem Ziel-Mailserver geschickt werden. Geben Sie für jedes Segment zusätzlich zum Inhalt die relevanten TCP-Flags sowie Sequenznummern an.

Aufgabe 2: Sicherheit

Nehmen Sie an, Alice und Bob einigen sich über einen sicheren Kanal auf einen gemeinsamen symmetrischen Schlüssel S. Sie wollen diesen für die Integritätssicherung verwenden:

Sobald Alice eine Nachricht an Bob versendet, berechnet sie den SHA-3-Hashwert H_{Send} ihres Nachrichtentextes, verschlüsselt diesen mit S und hängt das Ergebnis $S(H_{Send})$ an ihre Nachricht.

Sobald Bob die Nachricht erhält, entschlüsselt er $S(H_{Send})$ mit Hilfe von S und erhält H_{Send}. Jetzt berechnet er den SHA-3-Hashwert H_{Recv} des erhaltenen Nachrichtentextes. Falls $H_{Send} = H_{Recv}$ gilt, weiß er, dass er die Originalnachricht von Alice unmanipuliert erhalten hat.

Da der Schlüssel S symmetrisch ist, funktioniert das Verfahren für Nachrichten von Bob an Alice identisch.

(a) Wenn das Verschlüsselungsverfahren selbst öffentlich bekannt, standardisiert und verfügbar ist, woraus erfolgt dann die Sicherheit?

(b) Welche Nachteile hat das oben vorgestellte Verfahren dennoch, verglichen mit der Verwendung von asymmetrischer Kryptographie, wie Sie sie von z.B. von digitalen Signaturen kennen?

(c) Folgt aus dem erfüllten Schutzziel Vertraulichkeit automatisch Datenintegrität? Folgt aus dem erfüllten Schutzziel Datenintegrität automatisch Vertraulichkeit?

(d) Warum bietet eine kryptographische Hashfunktion einen besseren Integritätscheck als die TCP-Prüfsumme?

(e) Kann man das Urbild eines Hashwerts einer kryptographischen Hashfunktion wieder herstellen? Wann gilt eine Hashfunktion also als „sicher“? Begründen Sie Ihre Antwort.

(f) Auf welcher Annahme beruht die Sicherheit von RSA?

Aufgabe 3: Web of Trust

Studierende der Vorlesung Einführung in Rechnernetze haben untereinander ein **Web of Trust** aufgebaut um in Zukunft Mails vertraulich und authentisch austauschen zu können. In Abbildung 2 werden die Signaturen der Studierenden untereinander dargestellt. In gelb ist in der Abbildung gekennzeichnet in welche Nutzer Sie teilweise vertrauen haben und mit grün in welche Sie volles Vertrauen haben.

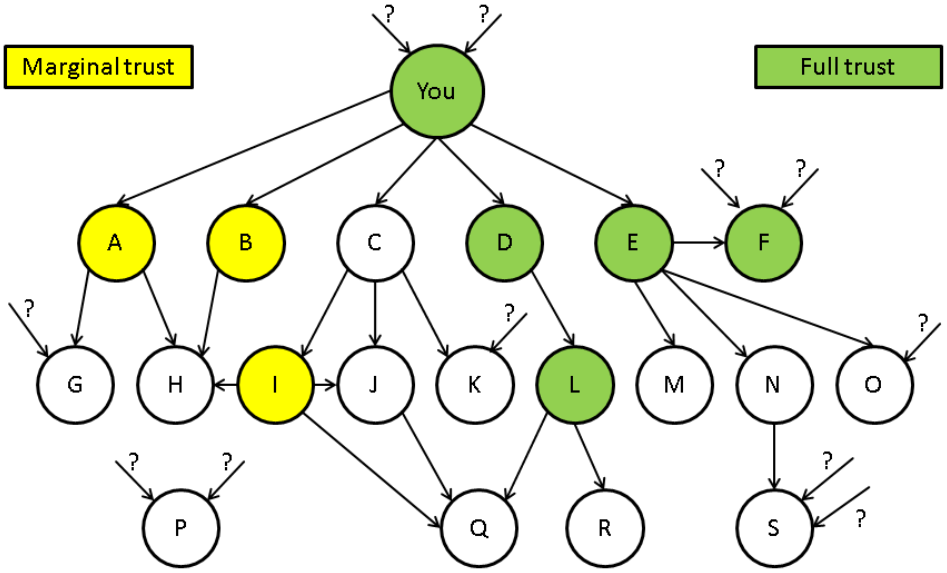

Abbildung 2: Web of Trust (Signaturen)

(a) Welche Art von Schlüsseln muss jeder Nutzer wie erzeugen um beim Web of Trust mitmachen zu können? Wie werden diese Schlüssel untereinander bekannt gemacht?

(b) Erläutern Sie, wie im Web of Trust prinzipiell überprüft wird, ob ein öffentlicher Schlüssel authentisch ist, also ob dieser tatsächlich zu einer bestimmten Mailadresse gehört.

(c) Für welche Schlüssel können Sie die Authentizität ohne Beachtung der Key Legitimacy angeben? Und warum?

(d) Geben Sie aus Ihrem Blickwinkel für jeden dargestellten Schlüssel das Vertrauen in den Nutzer und die Authentizität des Schlüssels an. Berücksichtigen Sie dazu als Key Legitimacy: zwei teilweise vertrauenswürdige Signaturen oder eine voll vertrauenswürdige Signatur.

(e) Sind **Vertrauen in Nutzer**, **Signaturen auf Schlüssel** und **Authentizität der Abbildung zwischen Schlüssel und Nutzer** unabhängig voneinander oder abhängig?