Zusammenfassung - Kryptographie

Marc Meier

4. November 2015

Korrektheit und Vollständigkeit der Informationen sind nicht gewährleistet. Macht euch eigene Notizen oder ergänzt/korrigiert meine Ausführungen!

Inhaltsverzeichnis

1 Grundlagen **2**

2 Protokolle **4**

3 Adressierung **4**

4 ARP, RARP **4**

5 DNS und WHOIS **4**

6 Migration von IPv4 nach IPv6 **4**

7 Timeouts, ACK, Bestätigungen **4**

8 Routingkonzepte **4**

9 Quality of Service **4**

10 Multicasts **4**

11 Zeitsynchronisation **4**

12 Internet Control Message Protocol **4**

13 Voice over IP **4**

14 World Wide Web und HTTP **4**

15 Peer-to-Peer **4**

16 E-Mail **4**

17 Autokonfiguration **4**

18 Dateien und Drucken **4**

19 Telnet, SSH und rlogin **4**

20 Extensible Messaging and Presence Protocol (XMPP) **4**

21 LDAP **4**

22 Authentication Protocols **4**

23 Simple Network Management Protocol **4**

24 Mac-Sublayer **4**

25 Mobile Netzwerke **4**

26 HTTP2 und SCTP **4**

Literatur **5**

Glossar **6**

1 Grundlagen

1.1 Grundprinzipien und Entwicklung des Internets

Das Internet entwickelte sich ab den 1960er Jahren. Es ging aus dem am Ende des Jahrzehnts entstandenen, vornehmlich militärisch und akademisch geprägten ARPA-Net hervor. Heutzutage wird es international kommerziell, industriell und auch akademisch (Katzenbilder) genutzt. Bei seiner Entstehung war vor allem eine dezentrale Struktur ohne zentrale Verwaltung von Interesse. Grund hierfür war die Angst des amerikanischen Department of Defense, dass eine atomarer Angriff zentrale Kommunikationspunkte außer Kraft setzen könnte. Die Kommunikation findet über hochgradig vernetzte Knoten mithilfe von Paketen statt.

Literatur: [1, 2]

1.2 Packet Switching

Paketvermittelte Übertragung bedeutet die Abkehr von der leitungsbasierten Vermittlung. Dabei werden längere Nachrichten in Datenpakete aufgeteilt und voneinander unabhängig versendet. Dies ermöglicht eine faire Verteilung der Leistungskapazität und redundante Wege bei einem Ausfall von Knoten oder Verbindungen. Im Gegenzug können konstante Bandbreiten nicht ohne Weiteres (Abschnitt 9) gewährleistet werden, ebenso ergeben sich unterschiedliche Laufzeiten von Paketen.

1.3 Dezentrale Verwaltung des Internets

1.3.1 Prinzipien

- Keine zentrale Verwaltung oder Behörde (trotz Einflussnahme)
- Demokratisches Zusammenwirken der Beteiligten / Wahlen
- Selbstorganisation
- Standards dort, wo sie erforderlich sind
- Dynamisch, offen für Neuigkeiten

1.3.2 Organisationen

ICANN: Vergibt IP-Adressen und betreibt die DNS-Rootserver.

IETF: Standardisierung von Protokollen in RFCs [3]

RIPE: Administration und technische Koordination

RIPE NCC: Adressvergabe in Europa und Zentralasien, Verwaltung der WHOIS-Datenbank.

DENIC eG: Domain-Verwaltung für die Zone .de

1.4 Standards

Standards ermöglichen die Kooperation im Netzwerk, nur durch sie können Geräte verschiedener Hersteller miteinander kommunizieren. Sie können textuell, mithilfe einer Referenzimplementierung oder anhand von Automaten (meist für zustandsbehaftete Protokolle) festgelegt werden.

Protokoll Standardisierte Regeln (Vorschriften) und Vereinbarungen zu Form, Ablauf, Steuerung und Sicherung (Fehler) der Datenübertragung in und zwischen Rechnernetzen, zwischen Einzel-Rechnern und zwischen Rechnern und Peripheriegeräten.

Standard Ein Standard wird von den verschiedensten internationalen und nationalen Organisationen sowie von großen Firmen erstellt. Ein Standard wird als verbindliche oder unverbindliche (empfohlene) Festlegungen schriftlich niedergelegt.

1.5 Netze, Autonome Systeme und Schichten

2 Protokolle

2.1 OSI-7-Schichten-Modell

2.2 Zustandslose und zustandsbehaftete Protokolle

2.3 Ethernet

2.4 Switching

2.5 Asynchronous Transfer Mode

2.6 Internet Protocol

2.6.1 IPv4

2.6.2 IPv6

2.7 User Datagram Protocol

2.8 Transmission Control Protocol

3 Adressierung

4 ARP, RARP

5 DNS und WHOIS

6 Migration von IPv4 nach IPv6

7 Timeouts, ACK, Bestätigungen

8 Routingkonzepte

9 Quality of Service

10 Multicasts

11 Zeitsynchronisation

12 Internet Control Message Protocol

13 Voice over IP

14 World Wide Web und HTTP

15 Peer-to-Peer

16 E-Mail

17 Autokonfiguration

18 Dateien und Drucken

19 Telnet, SSH und rlogin

20 Extensible Messaging and Presence Protocol (XMPP)

21 LDAP

22 Authentication Protocols

Literatur

[1] Janet Abbate. *Inventing the internet*. MIT press, 2000.

[2] Paul Baran et al. On distributed communications. *Volumes I-XI, RAND Corporation Research Documents, August*, pages 637–648, 1964.

[3] Paul Hoffman and Scott Bradner. Defining the ietf. 2002. `http://www.ietf.org/rfc/rfc3233.txt`.