Andreas Diesendorf **Gruppe7**
Artur Siubiak
Jan Wolfram

Übungszettel 6

Aufgabe 1

(1)

Ethernet:

Vertraulichkeit: Nur die am Netzwerk angeschlossenen Geräte haben Zugriff auf die Daten und den Datenverkehr

Integrität: Mit CRC32 erfolgt teilweise eine Überprüfung der Daten auf Richtigkeit. So können
Daten schlecht verändert werden. Es können auch nur Leute die mit dem Netzwerk verbunden sind
die Daten mitverfolgen.

Verfügbarkeit: Alle am Netz angeschlossenen Geräte haben jederzeit Zugriff auf die Daten im Netzwerk.

Wlan:

Vertraulichkeit: Nur die Leute die im Netzwerk sind können miteinander kommunizieren.

Integrität: Durch die WPA oder WPA2 Verschlüsselung ist es schwer Daten zu manipulieren oder
ins Netzwerk zu kommen. Ohne die Verschlüsselung kann man sich ganz einfach am Netzwerk anmelden
und könnte so zum Beispiel für Vergehen eines Dritten zur Verantwortung gezogen werden, ohne das
man dies gemerkt hat.

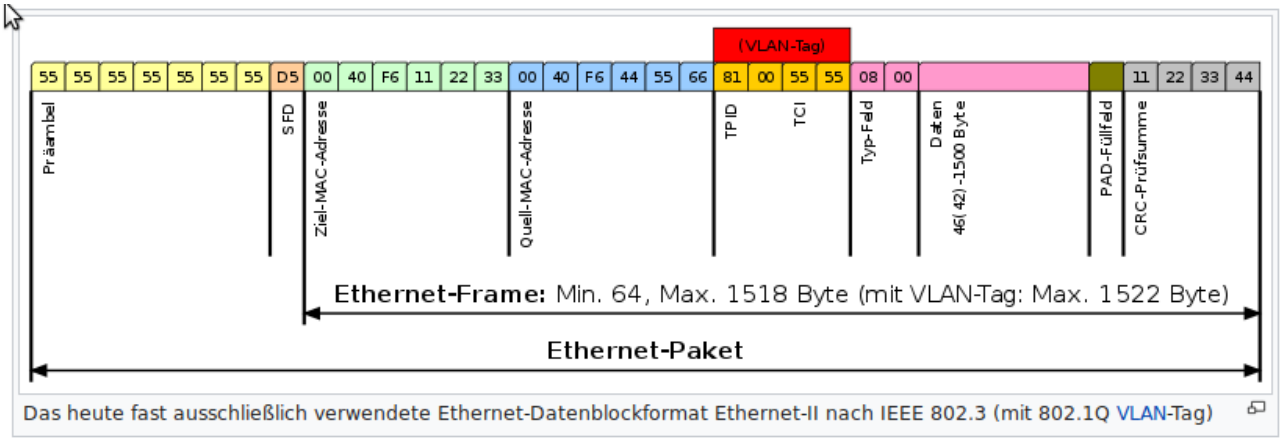
Verfügbarkeit: Man hat jederzeit Zugriff auf die Daten im Netz, solange man verbunden ist

(2)

Bei einer WI-FI-Netzwerkverbindung ist eine MAC-Adresse nicht verschlüsselt. Einige Netzwerke verwenden MAC-Filter,
um unerwünschten Zugriff zu verhindern. Hacker können MAC-Spoofing verwenden, um auf ein bestimmtes Netzwerk zuzugreifen
und Schaden anzurichten. Durch das MAC-Spoofing von Hackern wird die Verantwortung für illegale Aktivitäten auf authentische
Benutzer übertragen.

Warum wird IdentityMasking bei Ethernet nicht verwendet?

Ethernet benutzt zum Versenden von Daten einen Tagged MAC Frame. So ein Ethernet-Paket beinhaltet einen Ethernet-Frame, welcher Abweichungen durch eine CRC-Prüfsumme erkennt.



Das heute fast ausschließlich verwendete Ethernet-Datenblockformat Ethernet-II nach IEEE 802.3 (mit 802.1Q VLAN-Tag)

https://de.wikipedia.org/wiki/Ethernet#Datenframe

Aufgabe 3

1)

M = 100110101

M(X)= 1*x^8 + 0*x^7 + 0*x^6 + 1*x^5 + 1*x^4 + 0*x^3 + 1*x^2 + 0*x^1 + 1*x^0
= x^8 + x^5 + x^4 + x^2 + 1

2)

```
100110101 *x^3 = 100110101 000

G= 1001

10011010100
1001
----
   01010
    1001
    ----
    001110
      1001
      ----
      01110
       1001
       ----
       01110
        1001
        ----
        0111
```

3)

Prüfsumme = 0111

4)

CRC32 ist lediglich als Schutz vor Übertragungsfehler entworfen worden. Bei Veränderung der Nachricht lässt sich einfach die Veränderung der Prüfsumme berechnen.