Neulich habe ich auf Incom* eine hübsche Blume gelikt.

Für diesen Like wurden 3.124 Byte Daten zwischen meinem Laptop und dem Incom-Server durch das Internet transportiert. Der Transport der Daten erfolgte über Funkwellen, Kupferkabel und Glasfaser.

Jedes einzelne Bit dieser Information ist hier durch ein helles oder dunkles Quadrat dargestellt. Die einzelnen Blöcke (Pakete) lesen sich zeilenweise wie ein Text.

ΙP

Alle Kommunikation im Internet geschieht nach den Vereinbarungen des Internet Protocol. Dabei wird Informationen in einzelne Pakete geteilt und anhand einer IP-Adresse zum Ziel zugestellt. Das Internet arbeitet bei dem Transport ähnlich wie ein Postsystem, nur millionenfach schneller: Pakete können verloren gehen, sie nehmen manchmal abenteuerliche Umwege und sie können sich dabei auch gegenseitig überholen.

Die 16 einzelnen IP-Pakete sind links dargestellt. Jedes einzelne Paket trägt die (im Diagramm eingefärbte) IP-Adresse des Absenders und des Ziels. Die Einrückung zeigt an, ob das Paket von meinem Laptop zum Server läuft, oder zurück.

TCP

Um verlässliche Datenströme zu realisieren, baut das *Transmission Control Protocol* auf IP auf. Es funktioniert ähnlich wie eine Brieffreundinnenschaft: Obwohl das Substrat der Beziehung einzelne Briefe sind, ergibt sich für die Freundinnen der Eindruck einer kontinuierlichen Unterhaltung. Geht einmal ein Brief verloren, fragt die Freundin nach dem Verbleib des Briefes nach. Kommen Briefe in der falschen Reihenfolge an, lässt sich das Missverständnis schnell klären.

Alle abgebildeten Pakete bilden zusammen eine TCP-Verbindung. In den gelb markierten 8 Bit eines jeden Paketes wird durch die aktiven Bits ausge-drückt, welche Art von "Floskel" hier kommuniziert wird. Zum Beispiel bedeutet "Ich habe das letzte Paket erhalten".

TLS

Sowohl IP als auch TCP kommunizieren grundsätzlich im Klartext. Um vertrauliche Kommunikation zu gewährleisten, kommt das Protokoll Transport Layer Security zum Einsatz. Es ist dafür verantwortlich, dass die allermeiste Information die im Internet übertragen wird verschlüsselt, und damit nur für die jeweiligen Kommunikationspartnerinnen einsehbar ist.

Deswegen bestehen die letzten beiden großen Blöcke nur aus chaotischen Mustern; Sie enthalten verschlüsselte Daten. Entschlüsselt sind sie noch einmal in helleren Farben daneben dargestellt. Die Entschlüsselung konnte ich nur vornehmen, weil die Kommunikation von meinem Browser ausging. Anderer Datenverkehr lässt sich grundsätzlich nicht entschlüsseln.

Hey Server, kann ich zu dir eine TCP-Verbindung aufbauen? Hey Laptop, das funktioniert. Bitte bestätigen mir, dass du Alles klar Server, bestätigt! Hey Server, ich schicke dir jetzt Daten: Hey Server, ich würde gerne eine verschlüsselte TLS-Verbindung aufbauen. Hier ist eine Liste mit allen Verschlüsselungsverfahren, die ich beherrsche. Hey Laptop, ich habe die Nachricht von eben erhalten. Hey Laptop, ich schicke dir jetzt Daten: Hey Laptop, deine verschlüsselte Verbindung kannst du aufbauen. Wir benutzen dieses und jenes Verschlüsselungsverfahren. Server, die Daten von eben habe ich erhalten. Hey Server ich schicke dir jetzt Daten: Alles klar, dann können wir ja jetzt loslegen mit der verschlüsselten Verbindung! Hey Server, ich schicke dir jetzt Daten: Hey Server, ich schicke dir jetzt verschlüsselte Daten: Hey Server, ich möchte gerne eine HTTP-Anfrage stellen. Mein Betriebssystem ist Linux, mein Browser ist Firefox und ich bevorzuge die Sprache englisch. Außerdem bin ich bei Incom angemeldet. Kannst du bitte einen Like bei dem Proiekt 12035 vermerken? Entschlüsselte Daten Hey Laptop, ich habe die Daten von eben bekommen. Hey Laptop, ich schicke dir jetzt Daten: Hey Laptop, ich schicke dir jetzt verschlüsselte Daten: Hey Laptop, ich habe den Like erfolgreich vermerkt. Ende

Entschlüsselte Daten

aus Paket 11

Hey Server, ich habe die Daten bekommen.

Hey Server, ich schicke dir jetzt Daten:

Hey Server, alles klar, ich leg dann auch auf, ja.

Hey Server, ich beende jetzt die verschlüsselte Verbindung.

Hey Laptop, ich beende jetzt die Verbindung.

Hey Laptop, alles klar, Tschüssi, bis zum nächsten Mal.

Kerstin Humm 2. Semester Kommunikatonsdesign FH Potsdam "Die ganze halbe Wahrheit" bei Lisa Bucher https://erictapen.name/