Studiengang Informatik
apsi 2020

Fachhochschule Nordwestschweiz
Arno Wagner, Michael Schläpfer

Lösungsblatt 4 — 12. Oktober 2020

Aufgabe 4-1: Entropie

(a) Analog zum Beispiel in der Vorlesung berechnen wir

$$E = -\sum_{i=0}^{n-1} p_i * log_2(p_i)\ bit$$

mit 256 Symbolen, die alle gleich wahrscheinlich auftreten ergibt sich also folgende Berechnung für E:

$$E = -\sum_{i=0}^{255} \frac{1}{256} * log_2(\frac{1}{256})\ bit$$

also,

$$E = -log_2(\frac{1}{256}) = 8\ bit$$

(b) Nehmen wir folgendes vereinfachtes Beispiel anhand eines Münzwurfs. Bei einer fairen Münze ist die Entropie

$$E = -log_2(\frac{1}{2}) = 1\ bit$$

Vergleichen wir dies nun mit einer unfairen Münze, bei der Kopf mit einer Wahrscheinlichkeit von $p = \frac{3}{4}$ auftritt. Damit ergibt sich folgende Entropie:

$$E = -\left[\frac{3}{4} * log_2(\frac{3}{4}) + \frac{1}{4} * log_2(\frac{1}{4})\right] \sim 0.8\ bit$$

Das Ergebnis eines unfairen Münzwurfes ist also vorhersehbarer und weniger überraschend. Demnach ist auch der Informationsgehalt tiefer. Was mit der Intuition übereinstimmt.

(c) Kryptographische Protokolle basieren auf Zufallszahlen, beispielsweise für die Erstellung von Schlüsseln um eine Verbindung abzusichern, etc. Sind diese Zufallszahlen vorhersehbar für einen Angreifer, kann er die kryptographischen Funktionen nachvollziehen und deren Schutz umgehen. Werden beispielsweise gleich nach einem Systemstart, wenn noch wenig Entropie zur Verfügung steht, Schlüssel generiert, so stellen diese unter Umständen Schlüssel aus einer kleinen Menge möglicher Schlüssel dar und dies unabhängig von der Länge der Schlüssel selbst.

Aufgabe 4-2: Applied Cryptography am Beispiel von C

Der Link gibt Aufschluss über einige der Herausforderungen, welche sich im Zusammenhang mit Kryptographie stellen.

Aufgabe 4-3: Die vier Reiter der Infokalypse

Der Link beschreibt eine typischen Angriffsmethode auf die allgemeine Verfügbarkeit von Kryptogtaphie. Impliziert wird, dass nur die gelisteten Personengruppen sichere Kryptographie benutzen wollen. Ein typisches Argument ist das "rechtschaffene" Personen nichts zu verbergen haben und daher keine Einwände gegen unsichere Kryptographie haben (d.h. Kryptographie mit Backdoors). Hierbei wird regelmässig ignoriert, dass solche Backdoors nicht effektiv schützbar sind, und zu erwarten ist, dass diese sowohl missbraucht werden und als nach einiger Zeit auch kriminellen zur Verügung stehen würden.