

Exercise 17

1

Unser Vorschlag wäre eine Abwandlung von dem unter den Namen “Take a tail” vorgestellte Methode aus dem Paper Honeywords.

Bei diesem Verfahren wird während des Registrierungsprozesses der User dazu gezwungen eine Folge von Zahlen t_i der Länge n an den ursprünglich gewählten Usernamen u'_i anzuhängen. Dabei kann dem User eine zufälliges t_i empfohlen werden um die Sicherheit zu verbessern. Also:

$$u_i = u'_i \circ t_i$$

Zum Beispiel wenn $n = 3$ und $t_i = 157$ und $u'_i = foo$ dann wäre ein möglicher Username $u_i = foo157$.

Der Vorteil dieses Verfahrens liegt darin, dass sehr einfach weitere Decoys erstellt werden können. Zum erstellen weiterer Decoys werden lediglich die Zahlen t_i neu zufällig generiert und angehängen. Die Methode ist leider nicht epsilon flach sobald sich gegen die Zufallszahl entschieden wird. Dies kann kompensiert werden, durch das generieren vieler Decoys auf Kosten des Speicherplatzes. Bei Benutzung des zufälligen Suffixes hat der Angreifer eine 1% Chance das richtige Passwort zu raten. Sobald der Mensch selbst wählt sollte die Anzahl höher gewählt werden, um der Berechenbarkeit des Menschen entgegenzuwirken.

Der Nachteil dieser Methode liegt darin das der Registrierungsprozess speziell aufgebaut sein muss. Desweiteren ist es nicht immer einfach für den Benutzer sich die angehängenen Zahlen zu merken, was dazu führen kann, dass er sich diese notiert.

2.

Fall 1: Alice Wir gehen davon aus das Alice so schlau war die zufälligen Suffixe zu akzeptieren. Hier ist es irrelevant ob die Decoys aus den anderen Datensätzen bekannt sind, da jeder Decoy gleich Wahrscheinlich ist. Auch eine eventuelle Schnittmenge aus mehreren Datensätzen ist keine Hilfe für den Angreifer da Alices Passwörter unterschiedlich sind.

Fall 2: Bob Da Bob sich dazu entschieden hat auf beiden Servern die gleichen Passwort zu wählen kann von dem Angreifer die Schnittmenge aus den beiden Datensätzen gebildet werden. Diese kann mehr als ein Passwort betragen, was den Angreifer wieder zu einer Wahl zwingt. Trotzdem haben sich seine Chancen enorm verbessert.

Wenn nur eine Datensatz bekannt ist kommt es darauf an ob Bob sich für oder gegen das Zufällige Suffix entschieden hat. Im letzteren Fall kann der Angreifer seine Chancen verbessern in dem er statistische Beobachtung über die Natur des Menschen beim wählen von Zahlen miteinbezieht.