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 Registrieungsprocesses 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 ein vorgeschlagenes zufälliges t_i der Länge n wählen 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 des Verfahrens liegt darin, dass sehr einfach weitere Decoys generiert werden können. Zum erstellen weiterer Decoys werden lediglich die Zahlen t_i neu zufällig generiert. 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 gleichverteilte Chance das richtige Passwort zu raten (1% bei 100 Decoys). 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 Registrierungsprocess speziel Aufgebaut sein muss. Desweiteren ist es nicht immer einfach für den Benutzer sich t_i zu merken, was dazu führen kann, dass er sich diese notiert.

2.

Fall 1: Alice Wir gehen davon aus, dass Alice so schlau war die zufälligen Suffixe zu akzeptieren. Dann ist es unrelevant 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 und daher nicht enthalten sein müssen.

Fall 2: Bob Da Bob sich dazu entschieden hat auf beiden Servern die gleichen Passwörter zu wählen kann von dem Angreifer die Schnittmenge aus den beiden Datensätzen gebildet werden um sein Passwort zu ermitteln. Diese kann mehr als ein Passwort betragen, wenn Decoys zufällig gleich sind, 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.