Bezpieczeństwo komputerowe
Lista 2

Konrad Czart

4 listopada 2018

1 Część I

W celu realizacji tego zadania zostały zapisane dane z 30 rowerów (po 15 z każdej kategorii). Zanotowano numer wypożyczanego roweru, kod do zamka cyfrowego oraz kod, na jakim był ustawiony obecnie zamek. Do sprawozdania został dołączony plik bike.ods ze zgromadzonymi danymi, jednak z powodów bezpieczeństwa kody do zamków zostały ukryte.

2 Część II

2.1 Rozkład

Osoby korzystające z systemu wypożyczania rowerów często przekręcają jedną oraz dwie obręcze zazwyczaj o 2 bądź 3 pozycje. Można zauważyć, że kody do rowerów z pierwszej kategorii są mniej pomieszane od rowerów z kategorii drugiej. Jest to spowodowane tym, że rowery umieszczone w zamkach elektronicznych wcześniej mogły być podpięte zamkami mechanicznymi więc użytkownik musiał ustawić poprawny kod a zwracając dany rower do zamka elektronicznego nie przekręcał prawidłowo obręczy.

2.2 Entropia

W celu wyznaczenia entropii najpierw zostały wyznaczone odległości pomiędzy kodami pozostawionymi na zamkach a kodami otrzymanych z aplikacji. Następnie obliczono prawdopodobieństwo otrzymania poszczególnych odległości między kodami. Ostatecznie otrzymano entropie dla dwóch kategorii I i II, które wynoszą odpowiednio 2.872905595 i 3.189898095 natomiast entropia wszystkich zgromadzonych danych wynosi 3.177747163. Natomiast złodziej do odczepienia roweru potrzebowałby około 60 prób przekręcania fizycznej obręczy, przy czym dla rowerów z kategorii pierwszej liczba prób byłaby niższa jednak złodziej nie jest w stanie wyciągnięcia rowerów z zamków elektrycznych. Niskie bezpieczeństwo takiego systemu wynika z nieodpowiedniego zachowania użytkowników systemu.

3 Część III

3.1 Zachowanie użytkowników

- a) 4-cyfrowy PIN — jest to stosunkowo łatwy kod do złamania dzięki nieodpowiedniemu korzystaniu z systemu przez użytkowników.
- b) 8-cyfrowy PIN — znacząco poprawia bezpieczeństwo systemu, nawet przy nieodpowiednim korzystaniu przez użytkowników średnia liczba prób potrzebna do odczepienia roweru istotnie się zwiększa.
- c) 8-znakowe alfanumeryczne hasło — jeszcze bardziej bezpieczne hasło niż 8 znakowy PIN jednak zaprojektowanie układu obsługującego ten system jest znacznie bardziej kosztowne.

3.2 Wykrywanie oszustwa

Poprawność zebranych danych jest dosyć łatwa do weryfikacji, wystarczy, że sprawdzający porówna dane większej grupy użytkowników. Hasła otrzymane przez aplikację dla danego są takie same więc przyjmując, że chociaż jedna osoba z danej grupy zebrała wyniki prawidłowo a liczba rowerów jest ograniczona to na większej liczbie danych można w prosty sposób wykryć oszustwo. Poza tym numer roweru jest to pięciocyfrowa cyfra, która dla Wrocławskich rowerów miejskich zawsze zaczyna się od cyfr "57". Aby dane były jak najbardziej wiarygodne powinny zostać wytworzone przez cały kierunek.