Analiza i ocena bezpieczeństwa systemów usługowych i IoT
Ocena skuteczności różnych metod łamania haseł
Raport 1

Jan Pajdak
Wojciech Słowiński
Maria Filemonowicz

7 kwietnia 2019

Prowadzący: Dr hab. inż. Grzegorz Kołaczek

1 Cel eksperymentu

Hasła tekstowe to obecnie najpopularniejsza metoda uwierzytelniana używana do ograniczania dostępu do zasobów takich jak serwisy czy e-mail przez osoby nieupoważnione. Zabezpieczenia tego typu są łatwe w użyciu jednakże proste do złamania — w ramach eksperymentu skupimy się na łamaniu haseł przy użyciu programów implementujących algorytmy *BFM* oraz *Weira*

Eksperyment będzie przeprowadzony przy użyciu bazy realnych haseł, które następnie będą badane pod kątem odporności na złamanie przez poszczególne algorytmy.

2 Plan eksperymentu

2.1 Źródło danych

Jako źródło danych wybrane zostały hasła dostępne na stronie *Have I Been Pwned* (*https://haveibeenpwned.com/Passwords*). Baza zawiera 551 509 767 haseł, które pojawiły się w wyciekach informacji użytkowników, najczęściej z powodu niewystarczającego zabezpieczenia systemów.

Hasła znajdują się w pojedynczym pliku tekstowym o wielkości 22.6 GB. Praca z tak wielkim plikiem jest problematyczna, więc zostanie on podzielony na mniejsze pliki, które mogą zostać łatwo wczytane do pamięci komputera.

2.2 Metoda oceny

3 Przebieg eksperymentu

4 Wyniki

5 Analiza wyników

6 Podsumowanie