



CERB

Silne bezpieczeństwo w zasięgu telefonu

Paweł Jakub Dawidek

<p.dawidek@wheel.pl>



- podstawy teoretyczne
- wybrane metody uwierzytelnienia
 - m.in. piekło haseł statycznych
- popularne rozwiązania komercyjne
- *CERB* - zasada działania
- *CERB* - założenia projektowe
 - bezpieczeństwo nie będące koszmarem dla użytkownika?
- *CERB* - zastosowanie
- *CERB* - analiza bezpieczeństwa
- *CERB* - podsumowanie



- siłę hasła określa się poprzez ilość entropii jaką posiada
- entropia określa nieprzewidywalność (losowość) danych
- losowo wygenerowany bajt ma 8 bitów entropii
- losowo wygenerowana cyfra ma 3.25 bita entropii
- entropia tekstu to 1.1-1.6 bita na znak
- ilość pracy (kroków) potrzebna do złamania hasła statycznego to 2^x gdzie "x" oznacza ilość entropii



Hasła statyczne: zalety

- wygodne (nie dla użytkownika)
- nie wymagają żadnych urządzeń dodatkowych



Hasła statyczne: wady

- człowiek jest (tylko) człowiekiem
- łatwe do zapamiętania – łatwe do złamania
 - trudne do złamania – trudne do zapamiętania
- powszechnie używane
 - sporo do zapamiętania dla użytkownika (poczta elektroniczna, karta bankomatowa, gadu-gadu, allegro, komputer domowy, komputer firmowy, telefon, szyfr do walizki, BOK, itd.)
- mizerne bezpieczeństwo
- wymaga świadomych użytkowników



Hasła statyczne: wojna

- Użytkownik: “ala”
- Administrator: conajmniej jedna cyfra
- U: “ala85”
- A: conajmniej 6 znaków
- U: “alicja85”
- A: wielkie i małe litery
- U: “Alicja85”
- A: zmiana hasła co miesiąc obowiązkowa
- U: “Zmianahasła1” -> “Alicja85”
- A: trzy ostatnie hasła nie mogą być użyte



Hasła statyczne: wojna

- U: “Zmiana1” -> “Zmiana2” -> “Zmiana3” -> “Alicja85”
- A: hasło jest blokowane po zmianie na 15 dni
- U: Czy mógłby mi Pan zmienić hasło, ponieważ kiedyś wygadałam je koleżance, z którą się właśnie pokłóciłam?



Hasła statyczne: entropia

- według NIST (National Institute of Standards and Technology)
 - 1 znak – 4.7 bita
 - ≤ 8 znaków – 2.3 bita/znak
 - długie hasła - ~ 1 bit/znak
- 8-mio znakowe hasło = 18.4 bita entropii



- hasła jednorazowe
 - wymaga dodatkowego oprogramowania
 - konieczność regeneracji głównego hasła
 - (OPIS, S/Key) zbyt skomplikowane dla użytkownika
 - przyzwoite bezpieczeństwo
- karty zdrapki
 - duży koszt utrzymania systemu
 - uciążliwe w użytkowaniu, łatwe do zgubienia, itp.
- biometryka
 - nowa technologia – ograniczone zaufanie
 - uwierzytlenie lokalne
 - dodatkowe urządzenie po stronie użytkownika



- klucze asymetryczne (np. klucze ssh)
 - ograniczone zastosowanie
 - zbyt skomplikowane dla użytkownika
 - brak standardowych metod wysyłania/pobierania klucza publicznego
- PKI
 - umocowane prawnie, lecz brak zgodności między krajami
 - skomplikowana infrastruktura
 - wysokie wymagania po stronie użytkownika
 - konieczność noszenia karty
 - wysokie bezpieczeństwo



- tokeny sprzętowe
 - konieczność posiadania dodatkowego urządzenia (dla każdego systemu)
 - łatwe w użyciu
 - wysokie bezpieczeństwo

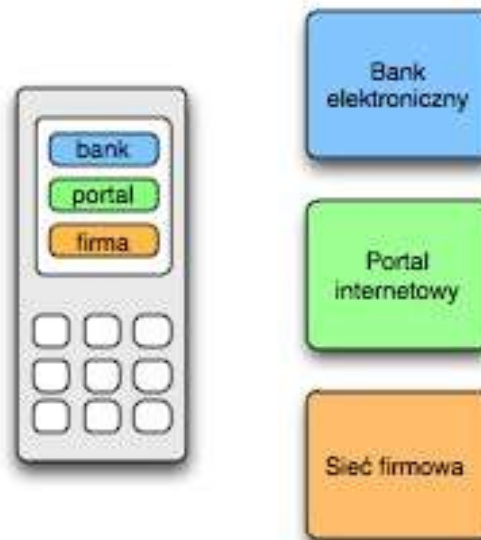


- systemy tokenowe
 - RSA SecureID
 - ActivCard
 - Vasco
 - Wheel
- systemy PKI
 - Entrust
 - RSA Security
 - SpyruS
 - Digital Signature Trust



CERB – Zasada działania

- *CERB* to system tokenowy
- oparty na zasadzie “coś wiesz i coś masz”
- telefon zamiast sprzętowego tokena
- użytkownik loguje się do systemu przy pomocy hasła wyświetlanego w telefonie





CERB – Założenia projektowe

- telefon jest bardzo wygodnym nośnikiem haseł
 - zawsze pod ręką
 - trudno zgubić (można zadzwonić)
- aplikacja *JavaToken*
 - jedna aplikacja zamiast wielu tokenów (niezależna obsługa wielu systemów)
 - intuicyjna i szybka w obsłudze
 - przede wszystkim bezpieczna
- moduł *SMSToken*
 - hasła dostarczane SMS-em



Lista Hasel jednorazow...

**Lista Hasel
jednorazowych:**

1. G23zsD11
2. 6za2SdeE
Wazne: 8h

Options Back



CERB – Założenia projektowe

- modułarna strona serwerowa
 - moduły uwierzytelniające (passwd, token, OTP, ODP)
 - moduły bazodanowe (pgsql, ldap, mysql)
 - moduły transportowe (dla ODP)
- wykorzystanie standardowych protokołów
 - RADIUS
 - PAM
 - libcercbclient



CERB – Zastosowanie

- serwisy internetowe, jako dostęp do chronionej treści
- w bankach elektronicznych – ochrona dostępu do konta i potwierdzanie transakcji
- w sieciach firmowych, intranetach i extranetach jako kontrolowany dostęp do zasobów
- uwierzytelnienie zestawiania tuneli VPN
- logowanie do systemów operacyjnych
- w systemach telefonii VoIP
- w systemach sieci bezprzewodowych
- w systemach mikropłatności z wykorzystaniem technologii SMS



CERB – Bezpieczeństwo

- dwuskładnikowy model bezpieczeństwa
- aplikację *JavaToken* chronioną nieweryfikowalnym PIN
- silna kryptografia (AES256, SHA256)
- opcjonalne dodatkowe hasło statyczne
- ochrona haseł statycznych przy użyciu PKCS#5v2
- limitowanie nieudanych prób logowania
- 6 bitów entropii na znak
- konfigurowalna długość tokenu
- konfigurowalna częstotliwość generacji tokenów



- silne bezpieczeństwo
- brak konieczności posiadania dodatkowych urządzeń
- przyjazny dla użytkownika
 - łatwa w obsłudze aplikacja
 - brak problemu “0 czy 0?”
- darmowa aplikacja *JavaToken* (licencjonowana tylko strona serwerowa)
- jeden telefon (jedna aplikacja) pozwala na logowanie do wielu niezależnych systemów
- prosta administracja



Pytania?