Uwierzytelnianie

Materiały pomocnicze do wykładu

Bezpieczeństwo systemów informatycznych

Uwierzytelnianie

Co to jest uwierzytelnianie?

Autentyczny (*authentic*) **wg słownika Webstera:**

Być rzeczywiście i dokładnie tym, czym się twierdzi, że się jest.

Uwierzytelnianie (*authentication*) jest procesem stwierdzania autentyczności czyli wiarygodności, weryfikacji tożsamości użytkownika.

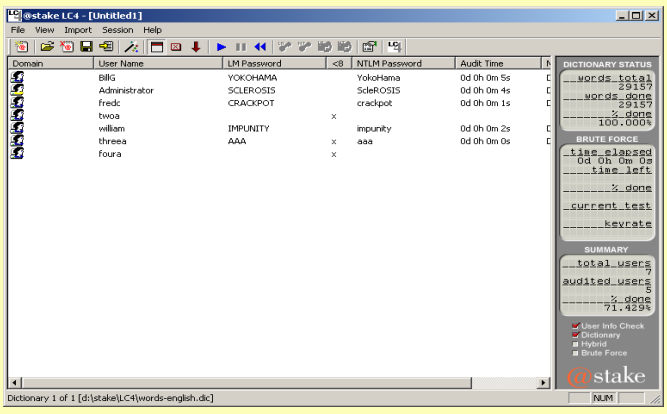
Uwierzytelnianie na podstawie:

- **tego, co użytkownik wie,**
- **tego, co użytkownik posiada,**
- **tego, kim użytkownik jest.**

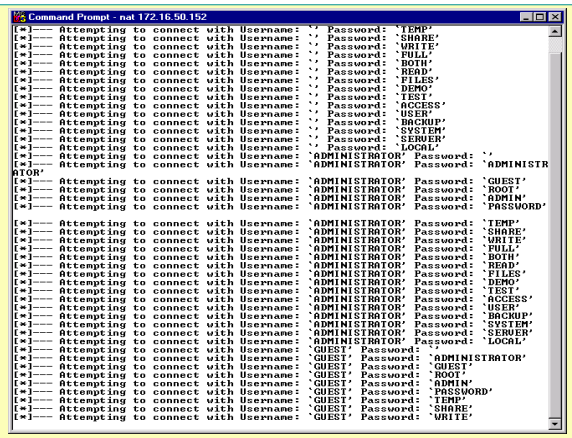
Słowniki haseł

- **Wykaz nazw użytkowników, ich inicjałów, nazw kont i innej informacji związanej z użytkownikiem.**
- **Wykaz słów z różnych słowników: imiona i ich permutacje, nazwy miejsc, tytuły filmów i książek i postaci w nich występujących.**
- **Różne przekształcenia słów z kroku poprzedniego.**
- **Dowolne zamiany liter małych na duże i odwrotnie.**
- **Słowa w obcych językach dla użytkowników obcokrajowców.**

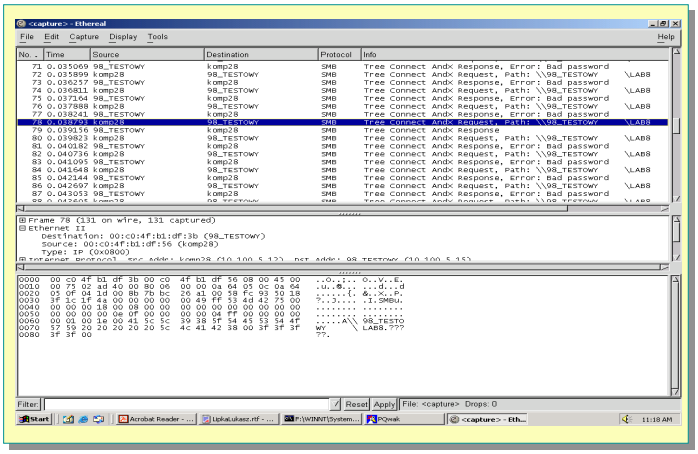
Łamanie haseł – program *L0phtCrack*



Łamanie haseł – program *nat*



Łamanie haseł – program *Pqwak*



Ochrona haseł

- Nadzorowanie haseł (wybór, pielęgnacja):
  - ✓ Komunikaty systemowe.
  - ✓ Wprowadzanie hasła.
  - ✓ Ograniczanie ilości prób rejestracji.
  - ✓ Starzenie się haseł.
  - ✓ Systemy z dwoma hasłami.
  - ✓ Minimalna długość hasła.
  - ✓ Blokowanie konta użytkownika.
  - ✓ Ochrona hasła administratora.
  - ✓ Generowanie hasła przez system.

Ochrona haseł

- Zabezpieczanie przed odgadnięciem poprzez odrzucanie zbyt łatwych haseł.
  - ✓ Sprawdzanie bierne.
  - ✓ Sprawdzanie czynne.
- Bezpieczne przechowywanie haseł.

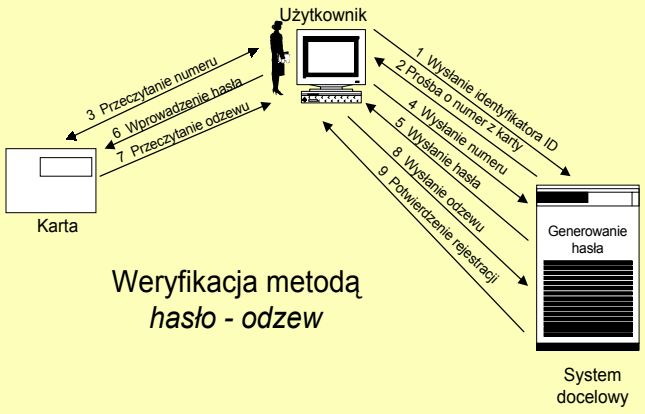
Hasła jednorazowe – system S/Key (RFC 1760) 1

- Klient i serwer są wstępnie skonfigurowani tym samym hasłem oraz licznikiem iteracji. Licznik iteracji określa wymaganą ilość powtórzeń funkcji mieszającej. Przy każdym logowaniu licznik iteracji stronie klienta maleje.
- Klient inicjuje wymianę wysyłając pakiet inicjujący.
- Serwer odpowiada numerem sekwencji. Wysyła również tzw. *ziarno*.
- Po stronie klienta wyliczane jest hasło jednorazowe:
  - ✓ operator wprowadza tajne hasło, które jest łączone z *ziarnem*,
  - ✓ kilkakrotnie wykonywana jest funkcja mieszająca generująca dane wyjściowe (wg licznika powtórzeń),
  - ✓ dane wyjściowe przekształcane są do postaci czytelnej i prezentowane operatorowi.

Hasła jednorazowe – system S/Key (RFC 1760) 2

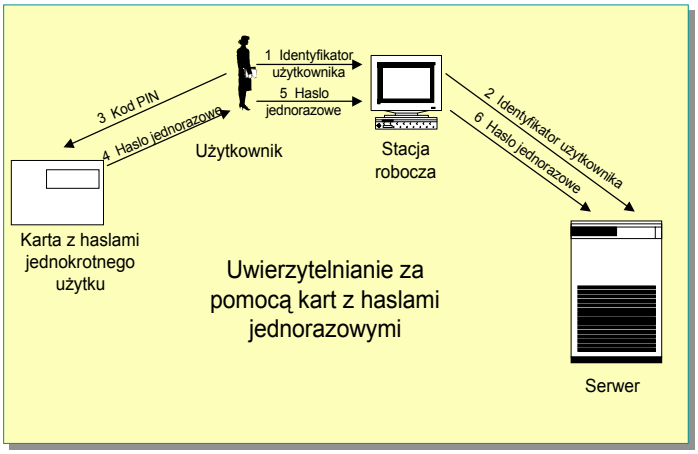
- Klient przesyła jednorazowe hasło do serwera.
- W serwerze znajduje się plik zawierający dla każdego użytkownika jednorazowe hasło z poprzedniego pomyślnego logowania.
- Serwer jednokrotnie przepuszcza odebrane hasło jednorazowe przez funkcję mieszającą. Wynik powinien odpowiadać hasłu z poprzedniego logowania.

Hasła jednorazowe

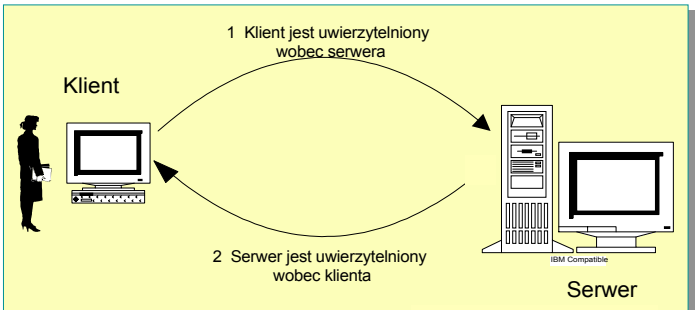


Weryfikacja metodą
hasło - odzew

Hasła jednorazowe



Hasła jednorazowe



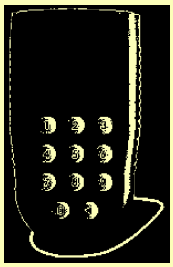
Procedury uwierzytelniania X.509

- Uwierzytelnianie jednokierunkowe.
  - ✓ Nazwa nadawcy.
  - ✓ Nazwa odbiorcy.
  - ✓ Znaczniki czasu określające czas utworzenia i ważności wiadomości.
  - ✓ Liczba losowa wygenerowana przez nadawcę.
  - ✓ Podpis cyfrowy nadawcy.
- Uwierzytelnianie jednokierunkowe.
- Uwierzytelnianie jednokierunkowe.

Tokeny

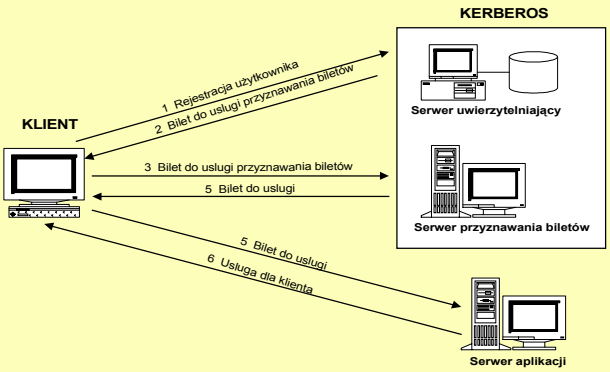
ActiveCard Plus

RSA SecureID



Vasco DigiPass 300

Kerberos - idea



Kerberos - komunikaty

CL>AS: CL, TGS, T_2

AS>CL: $\{TGS, K_{CL,TGS}, T_2, L_2, \{TGT_{CL,TGS}\}K_{AS,TGS}\}K_{CL}$

CL>TGS: $\{SR, CL, T_3\} K_{CL,TGS}, \{TGT_{CL,TGS}\}K_{AS,TGS}$

TGS>CL: $\{K_{CL,SR}, SR, T_4, \{B_{CL,SR}\}K_{SR,TGS}\}K_{CL,TGS}$

CL>SR: $\{B_{CL,SR}\}K_{SR,TGS}, \{CL, T_5\}K_{CL,SR}$

SR>CL: $\{T_5 + 1\}K_{CL,SR}$

Kerberos - atrybuty biletów

- **Bilety początkowe** (flaga INITIAL).
- **Bilety nieważne** (flaga INVALID)
- **Bilety odnawialne** (flaga RENEWABLE)
- **Bilety postdatowane**
  (flagi MAY_POSTDATE, POSTDATED)
- **Bilety upełnomocniające się i upełnomocnione**
  (flagi PROXIABLE i PROXY)
- **Bilety przekazywalne**
  (flagi FORWARDABLE i FORWARD)

Zbigniew Suski BSI - uwierzytelnianie 18