Bezpieczne korzystanie z komputerów

Uwierzytelnianie użytkownika, sesje w sieci lokalnej

Hasła i logowanie

- **Ataki słownikowe**
  - Próbowane słowa ze słownika (kilkadziesiąt - kilkaset tysięcy, z uwzględnieniem przypadków, rodzajów - rząd miliona)
  - Używane małe i duże litery
  - Dodawane na początku / końcu cyfry i znaki interpunkcji

Złożoność do trylionów kombinacji (10^{12}) nie stanowi przeszkody przy współczesnym poziomie mocy obliczeniowych

- **Budowanie dobrych haseł**

Oczywiście, pamiętam hasło logowania na swoje konto - to imię mojego psa. Chcę dodać, że:

  - mój pies wabi się 7&uo(#DF-<Qa
  - zmieniam mu imię co trzy tygodnie

Hasła

- Budowanie dobrych haseł
  - >6,8 znaków, wstawianie znaków innych niż litery

    50 przycisków klawiatury, SHIFT - 2*50 = 100 symboli ⇒ Jeżeli hasło przypadkowe 100^6 - 100^8

    Atak metodą prób i błędów - 10^{16} kombinacji dla hasła 8-znakowego

    Uwzględnienie ALT i CTRL - daje ok. 200 różnych symboli (ASCII)
  - Skróty (lub elementy) fraz: Pmps (Polak mądry po szkodzie)
  - Mieszanie dwóch (lub więcej) wyrazów

    kloss bond ⇒ kbloosnsd
- Przechowywanie haseł w systemie
  - Kradzież pliku z hasłami

    Hasła przechowywane w formie zaszyfrowanej lub jako skróty - kradzież nie daje bezpośrednio możliwości logowania (ale dla skrótu, hasło można odgadnąć w drodze ataku słownikowego)

Bezpieczeństwo systemów informatycznych

Hasła

- Inne problemy związane z hasłami
  - Ataki ‘psychologiczne’

    Ktoś podaje się za technika i mówi że wystąpił problem w sieci, prosząc jednocześnie o podanie hasła

    ⇓ wykorzystanie naturalnej skłonności niesienia pomocy

    Działa zaskakująco skutecznie - w 2000 w USA zanotowano ok. 60 tysięcy takich przypadków
  - Problemy z zapamiętywaniem haseł

    Redakcja NYT donosi o średnio 1000 przypadkach zapominania haseł na tydzień
- Ochrona przed atakami słownikowymi

  Zawieszanie możliwości logowania na określony czas po kilku nieudanych próbach (timeout-y)

Krzysztof Ślot © 2002

Zdalne logowanie

- Problem zdalnego logowania - hasło może być przechwycone

  Powszechnie stosowane aplikacje przesyłające hasła tekstem jawnym:

  FTP, telnet, POP3, SMTP, HTTP... ☹

- Wysyłanie hasła w formie zaszyfrowanej lub w postaci skrótu

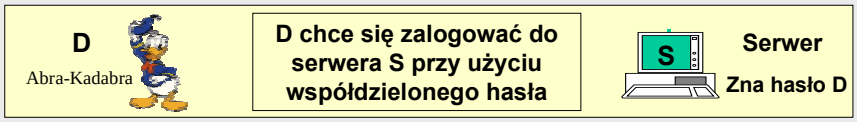
  W niczym nie rozwiąże problemu, bo można przechwycić i wykorzystać bez odgadywania hasła ☹

- Wysyłanie hasła w formie zaszyfrowanej (lub skrótu hasła) powiększonego o losowo zmienianą informację

  Technika challenge-response- CR (hasło i odzew) ☺

Logowanie do serwera

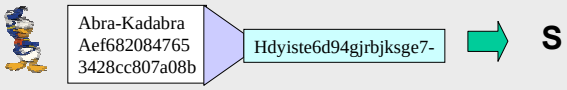
Technika CR



1. S generuje liczbę losową i wysyła ją do D

2. D wyznacza skrót hasła, powiększonego o liczbę losową i odsyła do S

3. S wyznacza skrót znanego hasła i wygenerowanej liczby losowej i porównuje go z otrzymaną wiadomością

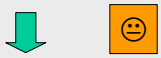
Logowanie do serwera

- Implementacja idei CR - protokół CHAP

Zastosowanie - autoryzacja użytkownika w PPP

Nie jest odporne na atak słownikowy

Atakujący zna skrót i zna przesłaną liczbę losową - może więc samemu dla różnych haseł próbować wygenerować skrót (algorytm jest znany) taki sam, jak przesłany serwerowi



Uwierzytelnienie nie jest bezpieczne gdy hasło jest słabe

Logowanie do serwera

- Modyfikacja uodparniająca na atak słownikowy

S i D mają współdzielony klucz szyfrowania

1. S szyfruje kluczem liczbę losową i wysyła do D
2. D rozszyfrowuje kryptogram i odtwarza liczbę losową
3. D zmienia w umówiony sposób liczbę losową (dodaje 1 itp.) i odsyła do S
4. S sprawdza kryptogram

Atakujący nie ma dostępu do liczby losowej - nie może przeprowadzić ataku słownikowego

Jeżeli do liczby losowej dodana zostanie dodatkowa informacja, np. ID użytkownika, wtedy metoda pozwala na uwierzytelnienie obydwu stron

Inne metody uwierzytelniania

- Uniemożliwienie ataku słownikowego - mocne hasło

  Żetony (bilety) i kalkulatory haseł

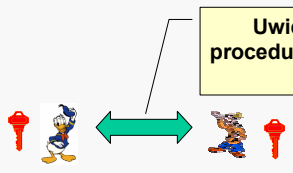
  Stosowanie metody CR, tyle że samo hasło jest długie, przydzielone danemu użytkownikowi, pamiętane w formie pliku, autonomicznego ‘kalkulatora’, karty elektronicznej

- Biometria
  - Odcisk palca
  - Obraz tęczówki
  - Głos
  - Kształt dłoni
  - Obraz siatkówki
  - Podpis, dynamika pisania

Sesje w sieci lokalnej

- Zadanie - zapewnić bezpieczne logowanie i bezpieczny przebieg sesji między komputerami pracującymi w sieci lokalnej

1. Wykorzystanie współdzielonego klucza tajnego



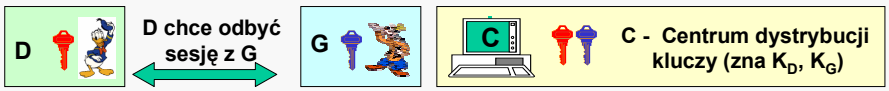
Tajny klucz jest inny dla każdej pary uczestników komunikacji

Wada #1 metody - problemy z gospodarką kluczami

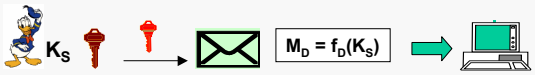
Wada #2 metody - problemy z generacją dobrego klucza

Sesje w sieci lokalnej

2 Ustanowienie centrum dystrybucji kluczy sesyjnych



➡ D generuje losowy klucz sesji K_S, szyfruje go kluczem K_D i wysyła do C



➡ C deszyfruje klucz sesyjny, szyfruje go kluczem K_G i wysyła do G

➡ G rozkodowuje klucz sesyjny 

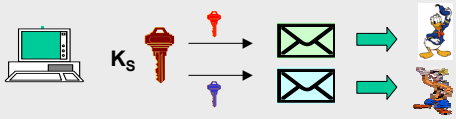
Wada - D, G mogą nie potrafić wygenerować silnego klucza, więc...

Sesje w sieci lokalnej

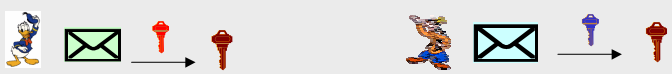
3 Zmiana roli centrum dystrybucji kluczy sesyjnych - centrum generuje klucze sesji

➡ D wysyła prośbę o klucz sesji do C

➡ C generuje losowy klucz sesji K_S, szyfruje go kluczem K_D i wysyła do D oraz szyfruje go kluczem K_G i wysyła do G

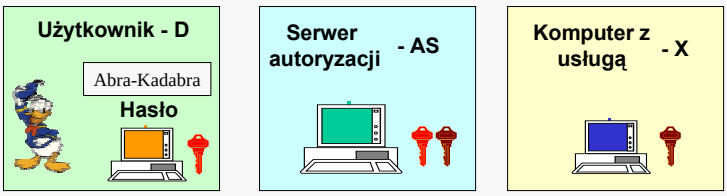


➡ D i G deszyfrują klucz sesyjny



Systemy dystrybucji kluczy - Kerberos

Podstawowa architektura systemu



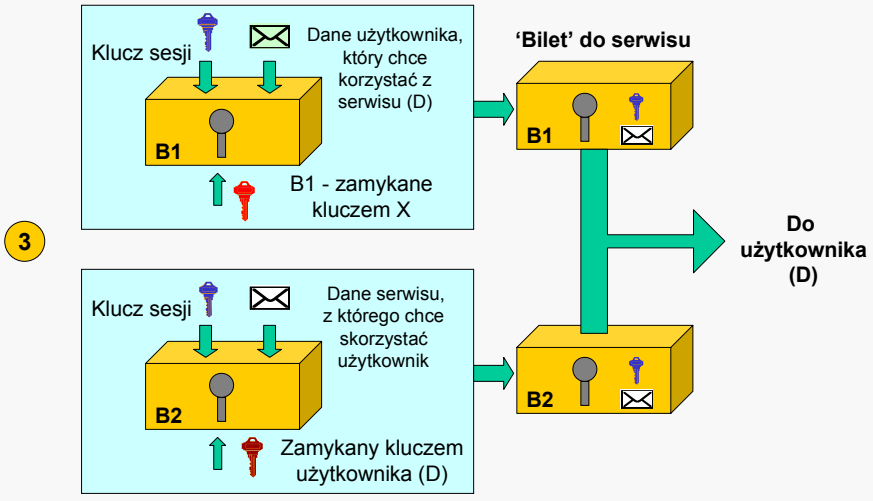
AS współdzieli klucze symetrycznej komunikacji z komputerem D i z komputerem oferującym usługę X

Algorytm przeprowadzania sesji

1. Użytkownik wysyła do AS życzenie skorzystania z usługi X
2. AS tworzy dwie kopie klucza symetrycznego (klucza sesji)

Kerberos

AS



Kerberos

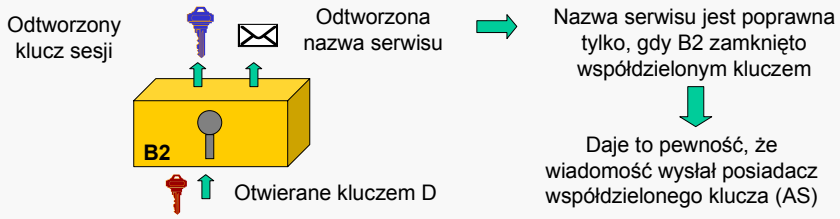
Użytkownik

4 **Rozszyfrowuje wiadomość z AS**

a Loguje się do systemu, używając swojego hasła (pewnie kiepskiego)

System (moduł Kerberosa) przekształca hasło użytkownika (w drodze szyfrowania) na klucz użytkownika (bazuje na tajnych stałych).

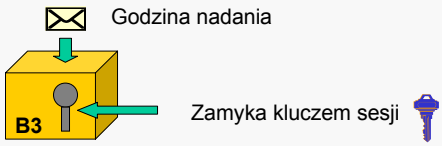
b Dokonuje deszyfracji B2 przy użyciu utworzonego klucza



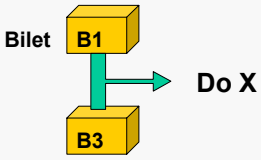
Kerberos

Użytkownik

5 **Przygotowuje dodatkową informację przeznaczoną dla X**



6 **Wysyła wiadomości B1 i B3 do X**

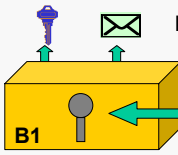


Kerberos

Serwis

7 **Rozszyfrowuje przesyłkę od AS z kluczem sesji**

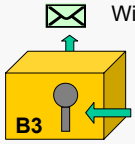
Odszyfrowany klucz sesji



Informacje o użytkowniku, który chce korzystać z serwisu

Otwiera swoim kluczem

8 **Sprawdza aktualność klucza sesji, dodatkowo uwierzytelnia D**



Wie kiedy rozpoczęto komunikację

Chroni przed próbą późniejszego użycia przechwyconego klucza (t=8,21h)

Otwiera kluczem sesji

Upewnia się co do tego, że użytkownik jest uprawniony (bo zna klucz sesji, którym zakodował czas rozpoczęcia sesji)

Bezpieczeństwo systemów informatycznych

Kerberos

Wada przedstawionej procedury

Każdy kontakt z serwisem wymaga powtarzania hasła logowania użytkownika (niezbędne do wytworzenia klucza D)

Klucz użytkownika (do komunikacji z AS) może być tymczasowo pamiętany, tak by ominąć logowanie, rozwiązanie takie nie jest jednak bezpieczne

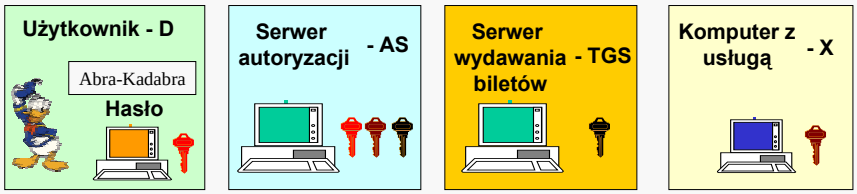
Modyfikacja procedury

Wprowadzenie ‘tymczasowego’ klucza użytkownika (odpowiednik tymczasowego identyfikatora)

Krzysztof Ślot © 2002

Kerberos

Modyfikacja architektury



- Użytkownik najpierw zawsze zwraca się do AS z prośbą o wydanie biletu do TGS (tak jakby to był dowolny serwis)
- Wydawaniem biletów do serwisów zajmuje się TGS
  Bilet do TGS (TGT - bilet zapewniający bilet / ticket granting ticket) jest pamiętany przez komputer użytkownika i używany za każdym razem, gdy chce się skorzystać z serwisów.
  TGT jest kluczem 'sesyjnym' używanym do komunikacji z TGT - jest więc tymczasowy

Kerberos

Systemy z wieloma AS/TGS

- Niezbędne by zapewnić efektywność w większych sieciach

Sieć jest dzielona na domeny (realms) obsługiwane przez osobne AS/TGT

Bilety do usług w każdej domenie są wydawane przez lokalne TGS, konieczne jest więc zapewnienie odpowiednich mechanizmów komunikacji między AS domen