BST 7 wyklad

Uwierzytelnianie – authentication (NIE AUŁTENTYKACJA) –

1. Identyfikacja – login
2. Weryfikacja – hasło

Biometria – cecha biologiczna danego obiektu organizmu –

dwie grupy: biometria statyczna (niezmienne cechy – odcisk palca, linie papilarne), biometria dynamiczna (cecha nabyta, weryfikujemy zachowanie – np. chód)

uwierzytelnianie jednokierunkowe – logowanie do systemu

uwierzytelnianie wzajemne – protokół TLS użytkownik-serwer, serwer-uzytkownik

uwierzytelnianie wielopoziomowe - dostep do kont bankowych online itp.

Poufnosc procesu

Aktualność uzytych danych

Atak powtórzeniowy – uzycie przez atakujacch kopii szyfrogramu

Sposoby ochrony przed atakami powtorzeniowymi:

Numery sekwencyjne (numery sekw danego procesu uwirzytelniania – inkrementowany z każdym kolejnym procesem)

Znaczniki czasowe – przewidziany jest określony czas na probe uwierzytelnienia

Identyfikatory żądania – chcemy się uwierzytelnić – serwer wysyla żądanie które jest pseudolosowym ciagiem danych – my uzależniamy odpowiedz od tego ciągu – ktoś podszywający się pod nas nie będzie miał możliwości odpowiedzieć kopia naszej odpowiedzi na bieżące żądanie – żądania się zmieniają z danym procesem uwierzytelniania

Hasła – dlaczego często stosowane?? – slajdziory

Hasla mieszane – ciekawe rozwiązanie – możemy wygenerować jakiś ciag danych np.macierze , podczas uwierzytelniania będziemy proszeni o podawanie fragmentow tego ciągu – każdy proces uwierzytelniania inny losowy fragment proszony o podanie.

Hasla SOLONE – XD – wartość salt – jeśli dwch roznych uzytkownikow ma takie samo haslo – to ich hashe będą takie same - chyba ze uzyjemy -salt z roznymi wartościami dla poszczególnych haseł – powoduje to rozne hashe tych samych haseł, wartość soli jawna

Uwierzytelanieanie challenge-response – bluetooth – slajdziory – żądanie i odpowiedź w sumie tyle

Karta inteligentna – slajdy – jakiś ciag bitow (informacja) w karcie – czytnik wysyła żadanie karta se na podstawie informacji w niej zawartych oblicza odpowiedz i nastepuje uwierzytelnianie. Dane na karcie trudne do podrobienia, skopiowania, taka karte lepiej zniszczyć gdy cos tam

..

..

Protokół Lamporta – wykonujemy wielokrotnie fuk=nkcjie hashujaca – X1 -> X2 - > X3 -> Xn, jako login podajemy Xn, a jako haslo podajemy wcześniejszy hash (na każdej strzałce funkcja hasujaca) obliczyć Xn-1 jest obliczyć w stanie tylko posiadacz wartości X1 (hashe sa jednokierunkowe), chop powiedział ze pokazuje nam ten protokol tylko temu ze chce pokazac ze sposobow uwierzytelniania jest kupe.