ZABEZPIECZANIE DOSTĘPU DO SYSTEMÓW OPERACYJNYCH KOMPUTERÓW PRACUJĄCYCH W SIECI.

Zabezpieczanie systemów operacyjnych jest jednym z elementów zabezpieczania systemów komputerowych, a nawet całych sieci komputerowych. Współczesne systemy operacyjne są narażone na naruszenia bezpieczeństwa przypadkowe i celowe.

System operacyjny

Wybranie SO odpowiedniego do potrzeb; zaprojektowanie SO w taki sposób, by sam mógł chronić się przed naruszeniami bezpieczeństwa o różnej genezie

Sieciowy

Zabezpieczenie danych przesyłanych za pośrednictwem różnych mediów transmisyjnych i zapewnienie ich poufności oraz integralności; wykluczenie możliwości przechwycenia transmisji

Uwierzytelnianie (autentykacja)
Jest to jeden z podstawowych sposobów ograniczania dostępu do systemu komputerowego do kręgu zaufanych użytkowników. Najpopularniejszą metodą sprawdzania tożsamości użytkowników jest stosowanie haseł (właściwie par identyfikator/hasło). Nowoczesne systemy operacyjne nie przechowują haseł użytkowników w postaci jawnej (niezaszyfrowanej). Przy każdorazowej próbie dostępu do chronionych zasobów systemu hasło wprowadzone przez użytkownika jest szyfrowane i porównywane z tzw. hash-em, czyli skrótem kryptograficznym obliczanym według pewnego algorytmu.

Uwierzytelnianie za pomocą haseł

Zalety:
Łatwe do wdrożenia i proste w stosowaniu
Użytkownicy są przyzwyczajeni do systemów, w których stosowane są różne rozwiązania oparte na hasłach

Wady:
Hasło może zostać skompromitowane (złamane, odgadnięte, podejrzane, przechwycone, wyjawione celowo lub przypadkowo)

ZABEZPIECZANIE DOSTĘPU DO SYSTEMÓW OPERACYJNYCH KOMPUTERÓW PRACUJĄCYCH W SIECI.

Użytkownicy są z natury „leniwi”, tzn. mają tendencję do stosowania nieskomplikowanych haseł, powielania haseł i ich beztroskiego ujawniania
Ludzie są podatni na socjotechnikę

Utwardzanie haseł
Stosowanie odpowiednio silnych algorytmów kryptograficznych
Wymóg stosowania haseł długich i skomplikowanych, wykorzystujących wszystkie znaki dostępne z klawiatury (a. . . z, A. . . Z, 0. . . 9, znaki specjalne)
Regularne zmiany haseł i uniemożliwienie ich powtarzania
Uniemożliwienie stosowania haseł słownikowych
Ograniczenie ilości niedanych prób logowania w połączeniu z czasową blokadą konta
Okresowe badanie odporności haseł stosowanych przez użytkowników

Metody biometryczne
Polegają na analizie indywidualnych, niepowtarzalnych cech żywych organizmów i wykorzystaniu tej wiedzy np. do identyfikacji poszczególnych osobników. W przypadku systemów komputerowych pozwalają na dokładniejszą kontrolę dostępu do tychże systemów. Cechy biometryczne można podzielić na fizyczne oraz behawioralne (związane z zachowaniem). W celu dokładniejszej identyfikacji można łączyć pomiary różnych cech jednej osoby. Pomiar cech biometrycznych powinien być szybki, dokładny i nie wymagający zbyt wielkiego zaangażowania ze strony weryfikowanej osoby. Potencjalna niedogodność: cechy biometryczne ulegają zmianom z biegiem czasu i/lub przypadkowo!

Fizyczne cechy biometryczne
Układ linii papilarnych
Geometria twarzy
Geometria dłoni
Wzór tęczówki lub siatkówki oka

Układ naczyń krwionośnych
Kształt ucha
Mapa temperaturowa określonych części ciała
Układ zębów
Zapach
Kod genetyczny

Behawioralne cechy biometryczne
podpis odręczny
głos (tembr głosu, szybkość mówienia, akcent)
chód (długość kroku, nacisk na podłoże, rozłożenie masy ciała)
sposób pisania na klawiaturze (szybkość pisania, siła nacisku na klawisze, odstęp między kolejnymi naciśnięciami klawiszy)
reakcja mózgu na znany bodziec

Kryptografia
Często chcemy ukryć pewne informacje, by nie zostały odczytane przez osoby postronne. Z pomocą przychodzi nam kryptografia. W największym uproszczeniu mianem kryptografii określamy techniki zapisu informacji w sposób niejawny, czyli zaszyfrowany. Założenie kryptografii (z greckiego ukryte pismo) jest zatem takie, że nikt nie powinien mieć dostępu do ukrytej informacji, jeśli nie ma wiedzy o metodzie, jakiej użyto dla uczynienia tej informacji nieczytelną. Kryptografia służy również do zapewnienia autentyczności przekazu informacji. W obecnych czasach termin kryptografia lub równoważne mu pojęcie szyfrowanie jest używany praktycznie tylko w odniesieniu do komputerów i sieci komputerowych. Kryptografia opiera się na tzw. kluczach, czyli informacjach niezbędnych do zaszyfrowania, odszyfrowania, podpisania, sprawdzenia poprawności podpisu pewnej porcji danych.

Kryptografia – kilka pojęć
Szyfrowanie — zastosowanie pewnego algorytmu kryptograficznego do ukrycia przekazu
Odszyfrowywanie — zastosowanie algorytmu kryptograficznego do odczytania zaszyfrowanego przekazu

ZABEZPIECZANIE DOSTĘPU DO SYSTEMÓW OPERACYJNYCH KOMPUTERÓW PRACUJĄCYCH W SIECI.

Wiadomość jawna — informacja przed poddaniem jej procesowi szyfrowania; inaczej: tekst otwarty
Kryptogram — informacja w postaci zaszyfrowanej; inaczej: tekst zaszyfrowany

Dwa główne powody, dla których stosuje się techniki kryptograficzne, to:

chęć zapewnienia poufności — zawężenie kręgu odbiorców komunikatu lub danych do zaufanych osób lub określonych aplikacji, będących w posiadaniu klucza. W tym znaczeniu szyfrowanie jest komplementarne do uwierzytelniania

potwierdzenie autentyczności — zawężenie kręgu potencjalnych nadawców komunikatu lub danych do zaufanych osób dysponujących kluczem (główne zastosowanie: podpisy cyfrowe).

Do tych cech można jeszcze dodać **integralność**, czyli zapewnienie, że informacja lub dane nie uległy zmianie w czasie przesyłania.

Integralność nie jest tożsama z potwierdzeniem autentyczności nadawcy informacji!

Sposoby szyfrowania

Istnieją dwie podstawowe gałęzie szyfrów:

symetryczne — istnieje tylko jeden klucz, używany zarówno do szyfrowania, jak i odszyfrowywania informacji Przykłady algorytmów: DES, 3DES, AES, Blowfish, IDEA

asymetryczne — istnieje para kluczy (prywatny i publiczny), z których jeden jest używany do szyfrowania informacji, a drugi do jej odszyfrowania. Przykłady algorytmów: RSA, DSA, ECIES, ECDSA

Poufność i autentyczność

Poufność
Informacja jest zaszyfrowana pewnym kluczem publicznym. Dla jednego klucza publicznego istnieje tylko jeden odpowiadający mu klucz prywatny, dlatego też tylko posiadacz odpowiedniego klucza prywatnego będzie mógł odszyfrować wiadomość.

Autentyczność

Nadawca szyfruje wiadomość swoim kluczem prywatnym i przesyła ją osobie, która posiada klucz publiczny nadawcy. Skoro wiadomo, że tylko posiadacz odpowiedniego klucza prywatnego był w stanie wygenerować taki kryptogram, który da się odszyfrować pasującym do tego klucza prywatnego kluczem publicznym, można przyjąć, że wiadomość pochodzi od konkretnego zaufanego nadawcy.

Podpis cyfrowy

Służy do dodatkowego potwierdzenia autentyczności pochodzenia i/lub integralności wiadomości lub pliku. W praktyce procedura opatrywania informacji podpisem cyfrowym wygląda następująco: autor informacji wylicza skrót wiadomości i szyfruje ów skrót swoim kluczem prywatnym. Potencjalny odbiorca wiadomości odszyfrowuje skrót kluczem publicznym autora informacji, samodzielnie wylicza skrót wiadomości i porównuje go z uprzednio odszyfrowanym skrótem. Jeśli wyniki są identyczne, można uznać, że wiadomość jest autentyczna i nie uległa zmianie podczas przesyłania. Do podpisywania cyfrowego stosuje się najczęściej algorytmy RSA, ElGamal i DSA.