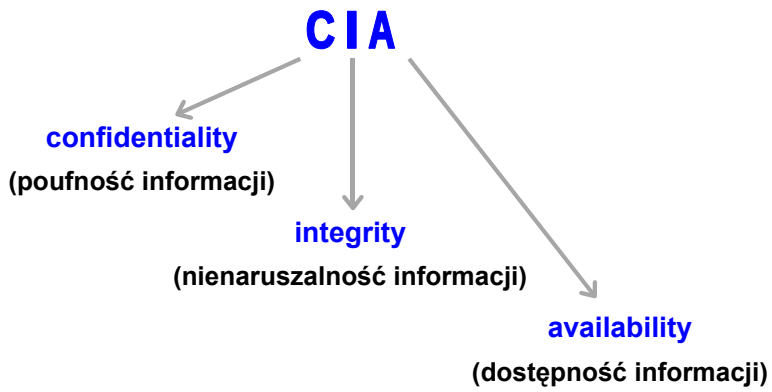
3. Ogólne własności bezpieczeństwa informacji

Podstawowe własności bezpieczeństwa

Często wyróżnia się 3 podstawowe własności bezpieczeństwa informacji, których zachowanie jest konieczne w większości zastosowań systemów informatycznych. Są to poufność, nienaruszalność i dostępność informacji (rysunek 1).



Rysunek 1. Trzy podstawowe własności bezpieczeństwa informacji

Zajmiemy się teraz omówieniem wybranych zagrożeń związanych z tymi trzema własnościami oraz krótkim przedstawieniem mechanizmów stosowanych w celu osiągnięcia tych własności.

Poufność informacji

Zagrożenia

Poufność, rozumiana – jak wiemy – jako ochrona przed nieautoryzowanym ujawnieniem (odczytem) informacji, narażona jest na ataki poprzez:

- nieuprawniony dostęp do danych w miejscu składowania w systemie, np. w bazie danych
- nieuprawniony dostęp do danych w miejscu przetwarzania, np. w aplikacji końcowej użytkownika
- podsłuchanie danych przesyłanych w sieci

Szczególny nacisk można położyć na szeroko rozumiany podsłuch, który dotyczy nie tylko oczywistego przypadku transmisji danych. Należy podkreślić techniczną możliwość podsłuchu zdalnego większości urządzeń infrastruktury systemu komputerowego, poprzez tzw. receptory Van Ecka. Dotyczy to urządzeń emitujących promieniowanie elektromagnetyczne (jak np.

monitory ekranowe, szczególnie starszego typu – CRT). Zatem ten rodzaj podsłuchu stanowi teoretyczne zagrożenie również dla danych składowanych oraz przetwarzanych na stanowiskach komputerowych, niezależnie od komunikacji sieciowej.

Mechanizmy obrony

W celu ochrony informacji przed jej nieautoryzowanym odczytem należy przede wszystkim umieć określić czy zamierzony odczyt jest autoryzowany oraz zminimalizować prawdopodobieństwo „wycieku" danych poza mechanizmem kontroli dostępu (w transmisji). Zatem mechanizmy obrony stosowane do zapewnienia poufności realizować będą następujące zadania:

- uwierzytelnianie
- autoryzację i kontrolę dostępu do zasobów
- utrudnianie podsłuchu

Omówimy kolejno problematykę wymienionych zadań i pokażemy przykłady mechanizmów, które je realizują.

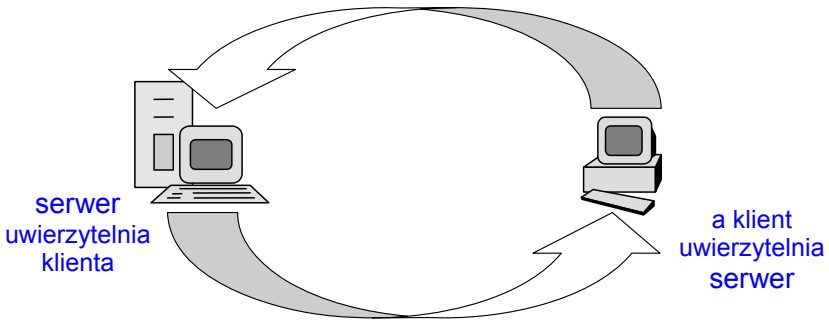
Uwierzytelnianie

W systemach informatycznych stosuje się następujące rodzaje uwierzytelniania:

1. uwierzytelnianie **jednokierunkowe** – polega na uwierzytelnieniu jednego podmiotu (uwierzytelnianego), np. klienta aplikacji, wobec drugiego (uwierzytelniającego) – serwera. Obrazuje to rysunek 2. Uwierzytelnienie następuje poprzez zweryfikowanie **danych uwierzytelniających** przekazanych przez podmiot uwierzytelniany. Typowymi danymi uwierzytelniającymi są np. identyfikator użytkownika i jego hasło dostępu.

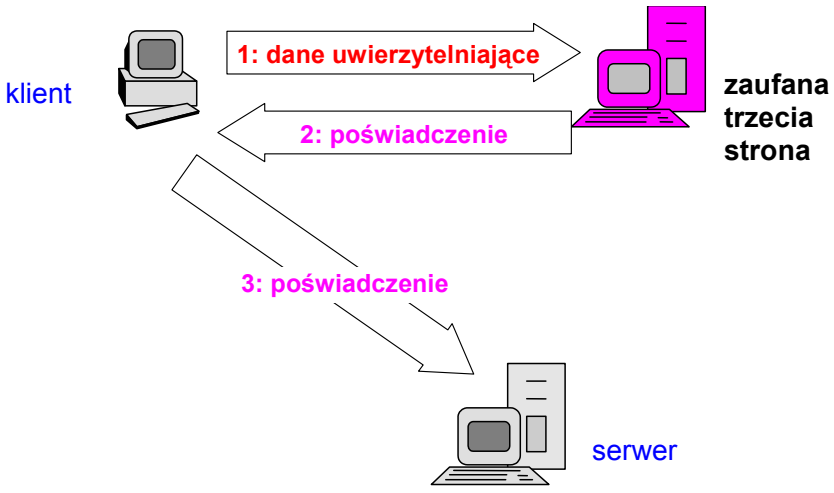
Rysunek 2. Uwierzytelnianie jednokierunkowe

2. uwierzytelnianie **dwukierunkowe** – polega na kolejnym lub jednoczesnym uwierzytelnieniu obu podmiotów (które są wzajemnie i naprzemiennie uwierzytelnianym oraz uwierzytelniającym). Obrazuje to rysunek 3. Jeżeli wzajemne uwierzytelnianie następuje sekwencyjnie (np. najpierw klient wobec serwera, a później serwer wobec klienta), mówimy o uwierzytelnianiu **dwuetapowym**, natomiast jednoczesne uwierzytelnienie obu stron nazywamy **jednoetapowym**.



Rysunek 3. Uwierzytelnianie dwukierunkowe

3. uwierzytelnianie **z udziałem zaufanej trzeciej strony** – włącza w proces uwierzytelniania trzecią zaufaną stronę, która bierze na siebie ciężar weryfikacji danych uwierzytelniających podmiotu uwierzytelnianego. Po pomyślnej weryfikacji podmiot uwierzytelniany otrzymuje poświadczenie, które następnie przedstawia zarządcy zasobu, do którego dostępu żąda (serwerowi). Schemat ten pokazuje rysunek 4. Podstawową zaletą tego podejścia jest przesunięcie newralgicznej operacji uwierzytelniania do wyróżnionego stanowiska, które można poddać szczególnie podwyższonemu zabezpieczeniu. Należy też podkreślić potencjalną możliwość wielokrotnego wykorzystania wydanego poświadczenia (przy dostępie klienta do wielu zasobów, serwerów). Zaufana trzecia strona może być lokalna dla danej sieci komputerowej (korporacyjnej) lub zewnętrzna (wykorzystująca infrastrukturę uwierzytelniania dostępną w sieci rozległej np. publiczne urzędy certyfikujące).

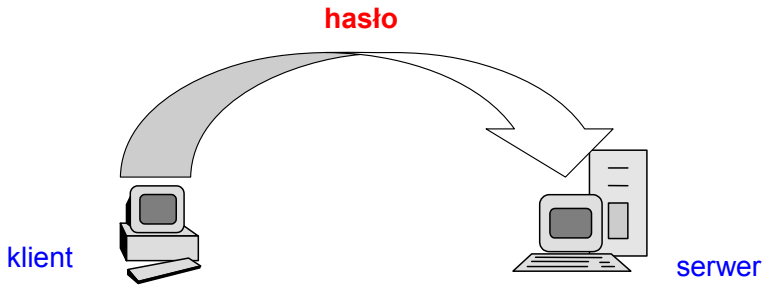


Rysunek 4. Uwierzytelnianie z udziałem zaufanej trzeciej strony

Mechanizmy uwierzytelniania użytkowników

Klasyczne uwierzytelnianie użytkownika

W przypadku wielu współczesnych środowisk informatycznych, systemów operacyjnych lub systemów zarządzania bazami danych, funkcjonuje klasyczny mechanizm uwierzytelniania poprzez hasło. Proces uwierzytelniania rozpoczyna klient żądając zarejestrowania w systemie (*login*). Serwer pyta o identyfikator (nazwę) użytkownika, a następnie o hasło i decyduje o dopuszczeniu do sieci. W większości przypadków nazwa użytkownika i hasło są przesyłane tekstem jawnym, co stanowić może kolejny problem zapewnienia poufności, jaką właśnie mamy osiągnąć stosując opisywany mechanizm. Stąd też takie klasyczne podejście nadaje się do wykorzystania jedynie w ograniczonej liczbie przypadków, kiedy np. mamy uzasadnioną skądinąd pewność wykluczenia możliwości podsłuchu danych uwierzytelniających.



Rysunek 5. Klasyczne uwierzytelnianie użytkownika

Hasła nie są najefektywniejszą, ani najbezpieczniejszą formą weryfikacji tożsamości użytkownika, z następujących powodów

- hasło można złamać:
  - odgadnąć, np. metodą przeszukiwania wyczerpującego (*brute-force attack*) lub słownikową (*dictionary attack*) – często hasła są wystarczająco nieskomplikowane by ułatwiło to odgadnięcie ich przez atakującego
  - podsłuchać w trakcie niezabezpieczonej transmisji
  - wykraść z systemowej bazy haseł użytkowników – zwykle hasła nie są przechowywane w systemie w postaci jawnej, często są zakodowane funkcją jednokierunkową lub zaszyfrowane, jednak niekiedy można stosunkowo łatwo jest pobrać i następnie starać się odzyskać ich oryginalną postać
  - pozyskać inną metodą (np. kupić)
- hasła się starzeją – czas przez który możemy z dużą pewnością polegać na tajności naszego hasła skraca się nieustannie, przez co hasła wymagają systematycznych zmian na nowe
- w niektórych środowiskach aplikacyjnych stosuje się predefiniowane konta użytkowników (również o charakterze administracyjnym) i przypisuje się im dość

powszechnie znane hasła domyślne – usuwanie lub dezaktywowanie takich kont czy zmiany haseł wymagają dużej staranności

Hasła są przedmiotem ataków – słownikowego i metodą przeszukiwania wyczerpującego. Słownikowy atak polega na podejmowaniu kolejnych prób zweryfikowania czy hasło wybierane ze zbioru popularnie stosowanych haseł (tzw. słownika) odpowiada hasłu aktualnie ustawionemu dla konta będącego celem ataku. Wariantem tego ataku jest wykradzenie nawet zakodowanych danych uwierzytelniających z systemu, aby po weryfikować czy kolejne hasła ze słownika dają po odpowiednim zakodowaniu któraś z postaci przechowywanych w systemie.

Przykładem analizy podatności haseł na atak słownikowy jest kilkukrotnie wykonane badanie, znane powszechnie jako raport Kleina. Operacje wykonywane w tym badaniu doskonale odzwierciedlają metodologię tworzenia słownika i mogą być doskonałą ilustracją zagrożeń wynikających z wyboru słabych haseł. W skrócie opisując Klein wykonał następujące operacje służące do uzyskania słownika haseł:

- wejściową postać słownika utworzyły nazwy użytkowników w systemie, ich inicjały oraz inne dostępne informacje (np. daty urodzin)
- następnie dodane zostały imiona i ich permutacje, nazwy miejsc, nazwiska sławnych ludzi, tytuły filmów i książek S-F oraz nazwiska postaci, dziedziny sportu i terminy sportowe
- wejściowy rozmiar słownika objął w efekcie ok. 1 500 haseł
- na tej zawartości słownika wykonane zostały przekształcenia powszechnie stosowane przez użytkowników: np. zmiana pierwszej litery na wielką, zastąpienie pierwszej litery znakiem sterującym, zamianę litery *o* na 0 czy *l* na 1, utworzenie liczby mnogiej, dodanie przed- i przyrostków
- dalej dołączone zostały kombinacje małych i wielkich liter haseł
- co dało łącznie ok. 1 000 000 słów

Z tak przygotowanym słownikiem zrealizowano atak na hasła użytkowników w rzeczywistym systemie. Efekty przedstawia poniższa lista trafień haseł (fragment) ze słownika wg poszczególnych kategorii (bez uwzględniania wśród nich przekształceń i kombinacji):

- nazwa użytkownika: ponad 10%
- nazwy pospolite: ponad 16%
- imiona żeńskie: 4,8%
- imiona męskie: 4%
- mity i legendy: 2%
- sport: 0,8%
- słownik środowiska korekty językowej dostępny w systemie operacyjnym (/usr/dict/words): blisko 30%

Wszystkie wymienione kategorie (nie jest to lista kompletna) należy uznać, jak widać, za słabe hasła i wystrzegać się ich przy wyborze własnego.

Przeszukiwanie wyczerpujące („atak brutalny”) polega kolejnym weryfikowaniu całej przestrzeni haseł, czyli wybieraniu wszystkich możliwych permutacji znaków z alfabetu wykorzystywanego

przy ustawianiu hasła użytkownika. Taki atak jest oczywiście kosztowny czasowo – wymaga prób dopasowania każdej permutacji do odgadywanego hasła, co zależy od wielkości alfabetu i długości hasła (rozmiaru przestrzeni haseł).

Prawdopodobieństwo odgadnięcia hasła wyraża wzór (1):

$$P = \frac{L \cdot R}{S} \qquad (1)$$

gdzie L = czas obowiązywania hasła
R = współczynnik szybkości (ilość prób na jednostkę czasu)
S = przestrzeń haseł – dla haseł o długości k z alfabetu N znaków: $S = N^k$

Uwzględniając zagrożenia wynikające z przedstawionych ataków na hasła, można zaproponować następujące „żelazne reguły" higieny haseł:

czego nie wolno:

- wybierać hasła o długości krótszej niż 6 znaków
- wybierać jako hasło znanego słowa, imienia, nazwiska, daty urodzenia, numeru telefonu, numeru rejestracyjnego
- zmieniać hasła tak, by nowe było zależne od starego (np. z 012345 na 123456)
- zapisywać hasła w widocznych lub łatwo dostępnych miejscach (jak np. fragment biurka zakryty klawiaturą, wnętrze szuflady czy płyta z danymi)
- informować nikogo o swoim haśle

co należy:

- wybierać długie i mało znane słowo lub frazę (kombinacja różnych znaków)
- wybrać hasło w sposób na tyle losowy na ile tylko możliwe
- zmieniać hasło możliwie często, lecz w nieprzewidywalny sposób
- zmienić hasło natychmiast, jak tylko rodzi się podejrzenie, że ktoś mógł je poznać

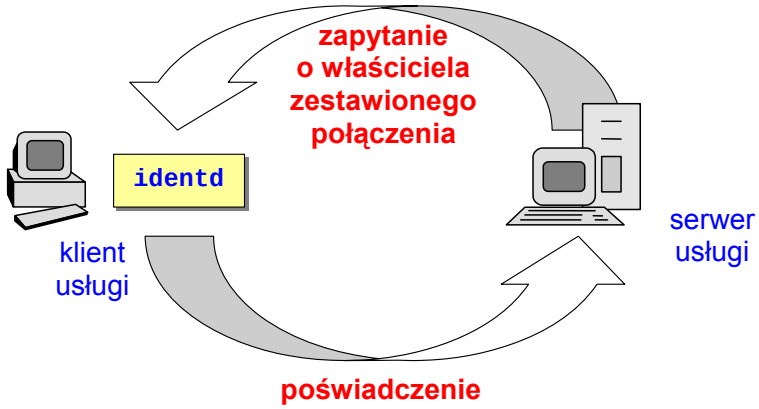
co warto:

- opracować własny algorytm generowania haseł – wybór pierwszych liter słów ulubionej fraszki, ostatnich znaków z wersów wiersza lub wybranej strony książki itp.
- zlecić systemowi wygenerowanie trudnego hasła

Zdalne potwierdzanie tożsamości użytkownika

W środowisku sieci TCP/IP wypracowano mechanizm prostego potwierdzania tożsamości użytkownika, który żąda zdalnego uwierzytelniania. W tym celu powstał standard RFC 1413 opisujący usługę o nazwie ident. Niezależnie od jej aktualnej przydatności i powszechności warto zdawać sobie sprawę z istoty jej działania, którą łatwo opisać w następujący sposób:

- użytkownik uruchamia klienta usługi i nawiązuje połączenie z serwerem
- serwer kontaktuje się z wydzielonym serwerem – identd, pracującym na stacji klienta (113/tcp) w celu poświadczenia nazwy (lub identyfikatora) użytkownika wykorzystującego usługę



Rysunek 6. Klasyczne uwierzytelnianie użytkownika

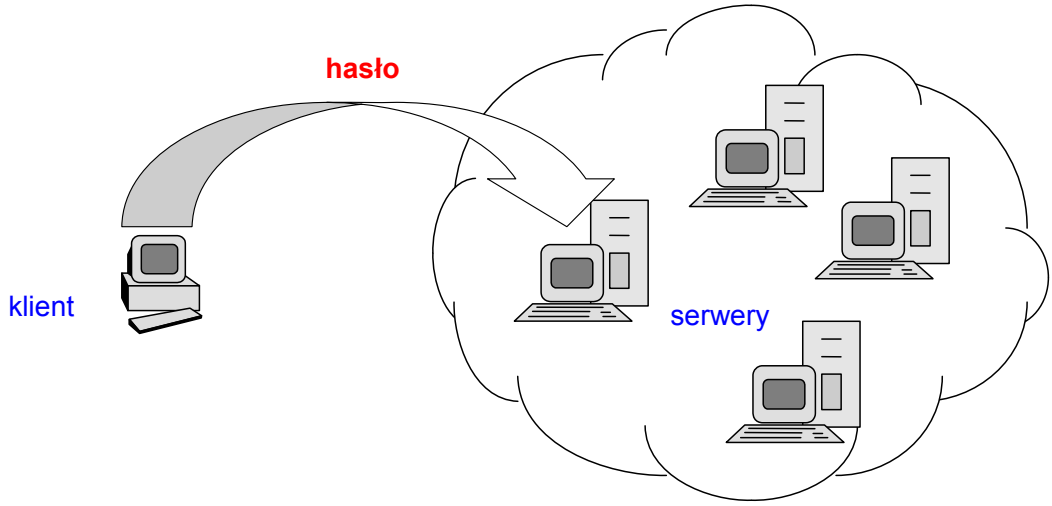
Należy też zdawać sobie sprawę z potencjalnych zagrożeń jakie niesie udostępnianie przez usługę ident informacji o przynależności procesów dokonujących komunikacji sieciowej (nie tylko klientów). W standardzie RFC 1413 oraz w praktycznych implementacjach nie realizuje się bowiem uwierzytelniania podmiotu żądającego informacji z tej usługi, może ona być zatem również nadużyta przez potencjalnego włamywacza.

Uwierzytelnianie jednokrotne (SSO – *single sign-on*)

Procedury uwierzytelniania jednokrotnego są częściowym rozwiązaniem problemu ochrony danych uwierzytelniających przed złamaniem w systemie wielozasobowym, np. sieci komputerowej z wieloma serwerami.

Ideą procedury uwierzytelniania jednokrotnego jest minimalizacja ilości wystąpień danych uwierzytelniających w systemie – hasło powinno być podawana jak najrzadziej. Zgodnie z tą zasadą, jeśli jeden z komponentów systemu (np. system operacyjny) dokonał pomyślnie uwierzytelniania użytkownika, pozostałe komponenty (np. inne systemy lub zarządcy zasobów) ufać będą tej operacji i nie będą samodzielnie wymagać podawania ponownie danych uwierzytelniających. Przy tym jest możliwe teoretycznie, że wszystkie komponenty samodzielnie korzystają z odmiennych mechanizmów uwierzytelniana. Wówczas, dodatkowo po pierwszorazowym uwierzytelnieniu użytkownika, system może oddelegować specjalny moduł do przechowywania odrębnych danych uwierzytelniających użytkownika i poświadczania w przyszłości jego tożsamości wobec innych komponentów systemu.

Schemat SSO przedstawia rysunek 7. W przedstawionej na rysunku sytuacji tylko jeden serwer dokonuje uwierzytelniania klienta, reszta ufa uwierzytelnianiu dokonanemu przez ten serwer.



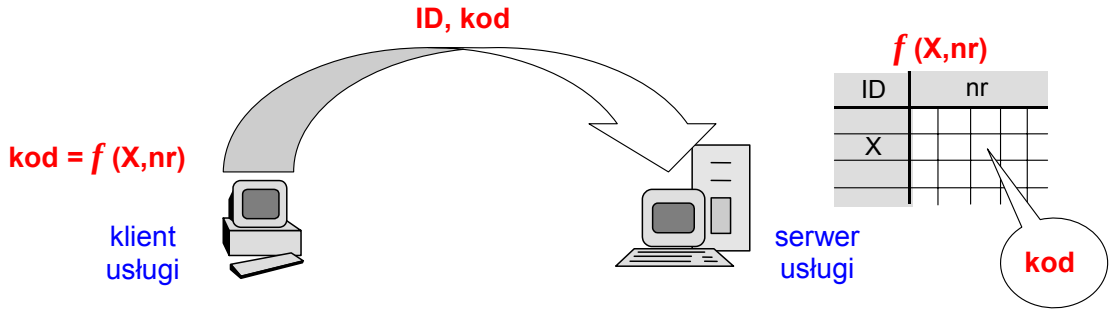
Rysunek 7. Uwierzytelnianie jednokrotne (SSO)

Hasła jednorazowe (OTP – *one-time passwords*)

Istota wykorzystania haseł jednorazowych wynika zamiaru ochrony ich przed przechwyceniem i nieautoryzowanym wykorzystanie, w przyszłości. Jednak nie polega na zapewnieniu ich poufności w transmisji lecz na uczynieniu ich *de facto* bezwartościowymi po przechwyceniu. Opiera się na, jak sama nazwa wskazuje, tylko użyciu danej postaci hasła tylko raz. Hasła jednorazowe mają przy każdym kolejnym uwierzytelnieniu inną postać. Raz przechwycone hasło jednorazowe nie jest przydatne, bowiem przy kolejnym uwierzytelnieniu będzie obowiązywać już inne. Komunikacja między podmiotami procesu uwierzytelniania może być zatem jawna. Stosujące takie hasła procedury uwierzytelniania muszą jedynie oferować brak możliwości odgadnięcia na podstawie jednego z haseł, hasła następnego.

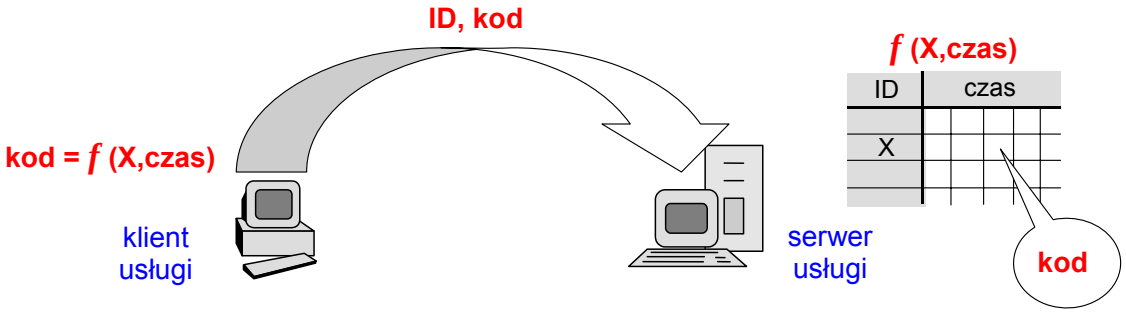
Hasła jednorazowe generowane są przy pomocy listy haseł, synchronizacji czasu lub metody zawołanie-odzew. Dostępne są najczęściej w następujących postaciach: listy papierowe, listy-zdrapki, tokeny programowe i tokeny sprzętowe.

Listy haseł to najprostsza i najtańsza metoda identyfikacji metodą haseł jednorazowych. Użytkownik otrzymuje listę zawierająca ponumerowane hasła. Ta sama lista zostaje zapisana w bazie systemu identyfikującego. W trakcie logowania użytkownik podaje swój identyfikator, a system prosi o podanie hasła z odpowiednim numerem. Klient za każdym razem posługuje się kolejnym niewykorzystanym hasłem z listy.



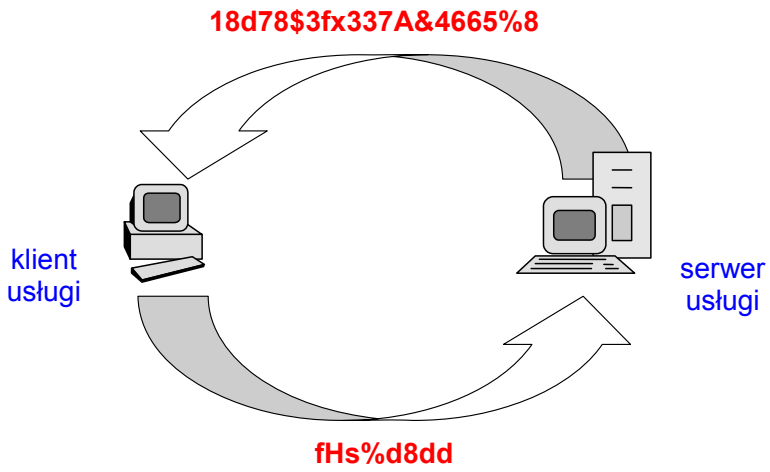
Rysunek 8. Uwierzytelnianie metodą listy haseł jednorazowych

W metodzie z synchronizacją czasu (*time synchronization*) klient generuje **unikalny kod** w funkcji pewnego parametru **X** użytkownika (identyfikatora, kodu PIN, hasła, numeru seryjnego karty identyfikacyjnej) oraz bieżącego **czasu**. Serwer następnie weryfikuje otrzymany od klienta kod korzystając z identycznej funkcji (z odpowiednią tolerancją czasu).



Rysunek 9. Uwierzytelnianie metodą z synchronizacją czasu

Natomiast w metodzie zawołanie-odzew (*challenge-response*) serwer pyta o nazwę użytkownika, a następnie przesyła unikalny ciąg („zawołanie"). Klient koduje otrzymany ciąg (np. swoim hasłem lub innym tajnym parametrem pełniącym rolę klucza) i odsyła jako „odzew". Serwer posługując się identycznym kluczem weryfikuje poprawność odzewu.



Rysunek 10. Uwierzytelnianie metodą listy haseł jednorazowych

Tokeny programowe to specjalne programy generujące hasła. W zależności od implementacji program na podstawie kwantu czasu lub zawołania serwera generuje hasło jednorazowe, które weryfikuje serwer.

Token sprzętowy jest małym przenośnym urządzeniem spełniającym wszystkie funkcje tokenu programowego.

Pewną ciekawostką zyskującą na popularności jest wykorzystanie telefonu komórkowego w uwierzytelnianiu za pomocą haseł jednorazowych. Cały proces polega przesłaniu hasła jednorazowego z serwera na telefon w postaci wiadomości SMS. W tym przypadku rola telefonu jako swoistego tokena sprowadza się tylko do medium odbierającego i wyświetlającego dane.

Inne mechanizmy uwierzytelniania

Do uwierzytelniania użytkowników można wykorzystać również przedmioty, których posiadaniem musi się wykazać uwierzytelniany. Mogą to być np. karty magnetyczne, karty elektroniczne czy tokeny USB. Ponadto, w przypadku ludzi, można posłużyć się również cechami osobowymi wynikającymi z odmienności parametrów niektórych naturalnych składników organizmu (uwierzytelnianie biometryczne), takich jak m.in.:

- klucz DNA
- małżowina uszna
- geometria twarzy
- termogram twarzy
- termogram dłoni
- obraz żył krwionośnych na zaciśniętej pięści
- odcisk palca (dermatoglify)
- chód
- geometria dłoni
- tęczówka oka

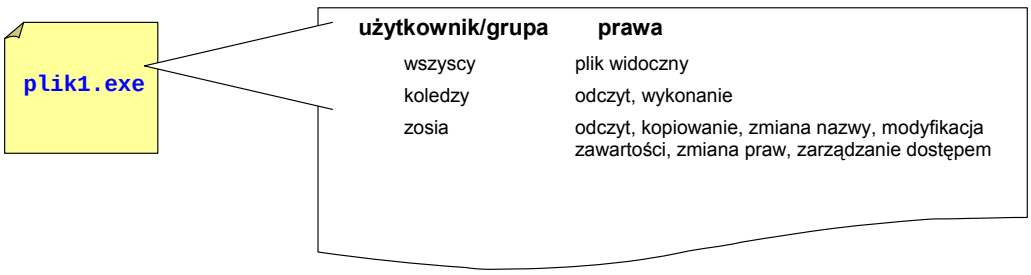
- odcisk dłoni
- obraz siatkówki
- podpis odręczny
- głos

Autoryzacja i kontrola dostępu do zasobów

Mechanizmy ochrony dostępu do danych

Zadania autoryzacji i kontroli dostępu legalnych użytkowników należą do podstawowych funkcji systemów operacyjnych czy systemów zarządzania bazą danych oraz środowisk przetwarzania rozproszonego. W większości przypadków te funkcje są realizowane podobnie.

Aktualnie jednym z najczęściej stosowanych mechanizmów weryfikacji praw dostępu jest lista kontroli dostępu, której implementacje, w zależności od konkretnego systemu, noszą nazwy ACL (Access Control List), ARL (Access Rights List) lub Trustees. Ogólna koncepcja działania mechanizmu listy kontroli polega na wyspecyfikowaniu dla każdego udostępnianego zasobu listy indywidualnych użytkowników lub ich grup bądź kategorii oraz przydzieleniu im podzbiorów uprawnień wybranych ze zbioru wszystkich uprawnień dostępnych dla danego zasobu (rysunek 11).



Rysunek 11. Lista kontroli dostępu do pliku

W kolejnych modułach (<A HREF="bsk-m6.doc">moduł 6</A> i (<A HREF="bsk-m11.doc">moduł 11</A>) omówione zostaną przykłady realizacji autoryzacji i kontroli dostępu użytkowników wybranych systemów operacyjnych oraz systemów zarządzania bazą danych.

Utrudnianie podsłuchu

Atak poprzez podsłuch jest zwykle skierowany przeciwko określonym zasobom i ma konkretny cel (np. przechwycenie hasła, lub zawartości konkretnych plików). Atak taki w istocie polega na wykonaniu operacji umożliwiających dostęp do kanału transmisyjnego (wpięcie się do medium transmisyjnego, podłączenie do stacji bazowej sieci bezprzewodowej itp.) a następnie wyłuskaniu z całego ruchu odbywającego się w tym kanale informacji poszukiwanych.

Ogólna koncepcja utrudniania podsłuchu polega zatem na uczynieniu możliwie jak najbardziej kłopotliwym obu kroków ataku – wpięcia się do kanału komunikacyjnego i wyłuskania użytecznych danych. Operacje utrudniania podsłuchu obejmują:

- stosowanie topologii sieciowej utrudniającej ewentualny posłuch lub ułatwiającej jego wykrycie, np. topologii gwiazdy (okablowanie strukturalne)
- stosowanie medium mniej podatnego na podsłuch; przykładowo popularne przewodowe media transmisyjne można uszeregować wg łatwości i skuteczności ich ewentualnego podsłuchu: UTP $\rightarrow$ FTP $\rightarrow$ STP $\rightarrow$ SSTP $\rightarrow$ FO
- utrudnianie wyłuskania użytecznych danych poprzez sztuczne generowanie ruchu (*traffic padding*) – wypełnianie wolnego pasma przenoszenia sieci danymi bezużytecznymi, co czyni trudniejszym, przynajmniej potencjalnie, rozróżnienie danych użytecznych od reszty (w wyniku zwiększenia proporcji danych bezużytecznych w całym ruchu)
- tworzenie zamkniętych grup użytkowników, poprzez separację ruchu sieciowego kierowanego z i do odrębnych grup użytkowników systemu (wspierają to już dojrzałe technologie VLAN ACL, Wire-rate ACL i in.)
- kontrola dostępu do zasobów infrastruktury sieciowej, poprzez dopuszczanie do udziału w ruchu sieciowym tylko uwierzytelnionych stacji sieciowych (co realizuje np. protokół IEEE 802.1x)
- szyfrowanie danych – stanowiące niewątpliwie najbardziej uniwersalny mechanizm ochrony poufności danych (czy ja zobaczymy wkrótce – szerzej rozumianej ochrony danych)
- ograniczanie emisji elektromagnetycznej – atak przez przechwycenie promieniowania van Ecka jest nadal tańszy od innego typu ataków na poufność danych (np. ataku kryptoanalitycznego), mimo że wymaga bardzo specjalistycznego sprzętu. Skutecznie można utrudnić ten atak poprzez wykorzystanie materiałów pochłaniających istotnie dużą część promieniowania elektromagnetycznego. Mamy do dyspozycji ekranujące materiały konstrukcyjne (obudowy komputerów i urządzeń peryferyjnych) oraz ekranujące materiały elastyczne do przygotowania pomieszczeń (tapety, wykładziny podłogowe i sufitowe). W niektórych zastosowaniach, jak np. przetwarzanie danych niejawnych, obowiązuje standard TEMPEST (*Transient Electromagnetic Pulse Emanation Standard*), który definiuje wymagania stanowiska komputerowego o ograniczonej emisji elektromagnetycznej. Stanowiska komputerowe zgodne z TEMPEST to wydatek rzędu kilkunastu, kilkudziesięciu tysięcy złotych.

Nienaruszalność informacji (integralność)

Kolejnym po poufności aspektem bezpieczeństwa omawianym w tym module jest nienaruszalność informacji, rozumiana jako ochrona danych przed ich nieautoryzowanym zmodyfikowaniem (dostępem do zapisu, w odróżnieniu od poufności, która oznacza ochronę przed nieautoryzowanym dostępem do odczytu).

Zagrożenia

Zagrożeniem nienaruszalności informacji jest zatem celowa lub przypadkowa modyfikacja danych przez nieuprawnionych użytkowników bądź oprogramowanie (np. wirusowe).

Mechanizmy obrony

Mechanizmy obrony stosowane do zapewnienia nienaruszalności informacji obejmują w szczególności:

- kontrolę dostępu do danych – wymienione wcześniej mechanizmy list kontroli dostępu
- sumy kontrolne zbiorów danych (np. plików dyskowych)
- kryptograficzne sumy kontrolne i podpis elektroniczny
- rejestrację operacji na danych (*auditing*) – niezbędną dla formalnego wykrycia naruszeń integralności; zwykle spotyka się podział danych audytu co najmniej na rejestr zdarzeń systemowych oraz rejestr zdarzeń aplikacji.
- kontrolę antywirusową

Dostępność informacji

Zagrożenia

Wśród zagrożeń nienaruszalności informacji należy wymienić przede wszystkim: