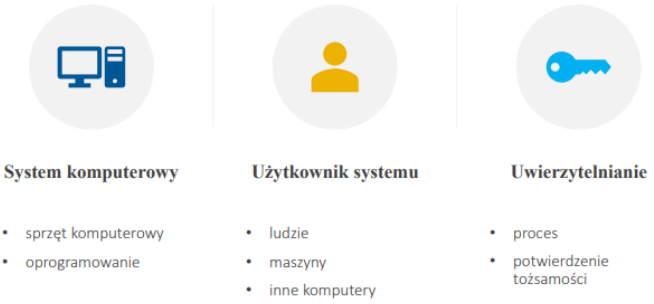
Pytanie: K1

Temat: Metody uwierzytelniania użytkowników w systemach komputerowych

Przygotował: Jakub Batogowski

Spis opracowania

Pojęcia związane z tematem



System komputerowy to układ, w którym współdziałają ze sobą dwie składowe: *sprzęt komputerowy* oraz *oprogramowanie*. Systemy komputerowe bardzo często pracują z innymi systemami w sieci komputerowej (np. w sieci Internet).

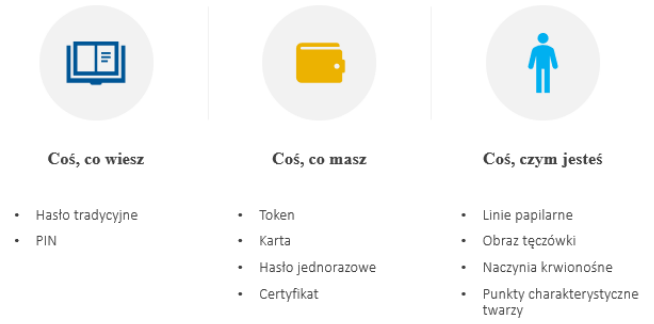
Użytkownik systemu to osoba, inny system lub maszyna korzystająca z systemu komputerowego.

Uwierzytelnianie to proces polegający na sprawdzeniu i potwierdzeniu (lub nie) tożsamości zadeklarowanej przez podmiot (użytkownika systemu) biorący udział w procesie komunikacji.

Uzyskiwanie dostępu do chronionego zasobu

Uzyskiwanie dostępu do chronionych zasobów składa się z **3 kroków**. W pierwszej kolejności podmiot (użytkownik) deklaruje swoją tożsamość, która następnie jest weryfikowana przez system, z którym użytkownik chce nawiązać komunikację. Po pomyślnym uwierzytelnieniu użytkownika, w procesie autoryzacji, nadawane są mu odpowiednie prawa.

Podział metod uwierzytelniania



Metody uwierzytelniania można podzielić na **3 grupy**. Do pierwszej z nich zaliczają się metody polegające na weryfikacji tożsamości za pomocą danych znanych jedynie użytkownikowi. Druga grupa zawiera metody polegające na przedstawieniu systemowi czegoś, co uwierzytelniający się podmiot posiada. Ostatnia grupa to metody biometryczne, uwierzytelniające użytkownika-człowieka na podstawie jego ludzkich cech (np.: na podstawie odcisków linii papilarnych lub kształtu twarzy).

Hasła tradycyjne

Hasła tradycyjne to najbardziej popularna metoda uwierzytelniania. Proces weryfikacji użytkownika polega na wpisaniu tajnego hasła, które sprawdzane jest z oryginalnym hasłem podanym np. podczas rejestracji w systemie. W celu umożliwienia uwierzytelniania podmiotów w ten sposób, hasła wszystkich użytkowników przechowywane są po stronie systemu posiadającego chronione zasoby. Najczęściej jednak, ze względów bezpieczeństwa, hasła te nie są przechowywane w jawnej postaci. Jedną z metod utajniania haseł jest **hashowanie** wykonywane za pomocą funkcji skrótu (np. MD5, SHA). Tak zaszyfrowane hasła nie są możliwe do rozszyfrowania, dzięki czemu mogą być bezpiecznie przechowywane. Nie mniej jednak z tego samego powodu, niemożliwe jest również bezpośrednie porównanie zaszyfrowanego oryginalnego hasła z hasłem podawanym przez podmiot podczas uwierzytelniania. W celu rozwiązania tego problemu, hasło podawane przez weryfikującego swoją tożsamość użytkownika jest w pierwszej kolejności hashowane i dopiero tak uzyskany skrót porównywany jest z jego oryginalnym odpowiednikiem znajdującym się w bazie danych.

Aspekt techniczny:

- w systemie operacyjnym UNIX hasła przechowywane są w */etc/passwd* lub */etc/shadow*
- na serwerze najczęściej porównywane są hashe a nie hasła!
- często stosowaną praktyką jest również **zasalanie haseł** przed operacją hashowania w celu uniemożliwienia późniejszego sprawdzenia, czy kilku użytkowników ma takie samo hasło

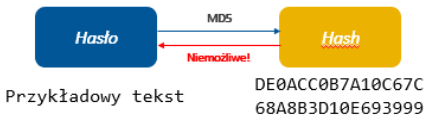
Zalety:

- proste w użyciu

Wady:

- łatwe do podejrzenia/zgadnięcia
- możliwe do przechwycenia/podsłuchania
- kosztowne w zarządzaniu
- łatwe do zapomnienia
- często użytkownicy korzystają z tego samego hasła w różnych serwisach co jest niebezpieczną (z punktu widzenia bezpieczeństwa) praktyką

Funkcja skrótu



Funkcja skrótu, zwana jest również **funkcją mieszającą** lub **funkcją haszującą,** transformuje dowolnej długości dane wejściowe na stałej długości ciąg bitów. Długość danych wyjściowych zależy od wybranego algorytmu (np.: dla **MD5** – 128 bitów, dla **SHA** – 512 bitów)

Cechy charakterystyczne funkcji skrótu:

- nieodwracalność przeprowadzonej operacji (nie da się przywrócić oryginalnych danych ze skrótu)
- stałej długości wyjście
- niejednoznaczność wyjścia (wiele różnych danych wejściowych może wygenerować takie same dane wyjściowe)
- mała złożoność obliczeniowa (obliczanie skrótu jest operacją szybką)

Listy haseł

Listy haseł są najczęściej używane jako dodatkowa metoda uwierzytelniania. Stosowane są głównie w serwisach bankowych. Pierwotnie, listy haseł wysyłane były do użytkownika pocztą. Obecnie jednak, ze względu na wygodę, wykorzystuje się jednorazowe hasła SMS.

Aspekt techniczny:

- przy każdorazowej próbie uwierzytelnienia należy podać nowe, niewykorzystane dotąd, zażądane przez serwer hasło

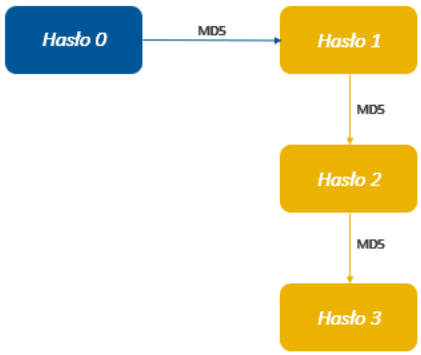
Zalety:

- najtańsza implementacja haseł jednorazowych
- zgubienie lub kradzież fizycznej karty łatwo zidentyfikować, dzięki czemu będąc pewnym jej utraty, można ją zablokować

Wady:

- wysyłana pocztą – długi okres oczekiwania
- kartę należy mieć przy sobie

Hasła jednorazowe



Hasła jednorazowe wprowadzone zostały w celu poprawy bezpieczeństwa uwierzytelniających się użytkowników. Korzystanie z nich odbywa się w sposób zbliżony do korzystania z listy haseł. Nie mniej jednak, w przypadku haseł jednorazowych, należy najpierw je wygenerować, aby móc później z nich korzystać.

Generowanie haseł polega na podaniu **tajnego hasła 0**, z którego wyliczany jest **hash** (**hasło 1**). Z tak obliczonego skrótu wyliczany jest **kolejny** (**hasło 2**) itd. Liczbę generowanych haseł podaje się przed rozpoczęciem ich generowania.

Aspekt techniczny:

- hasła generowane są za pomocą funkcji skrótu (najczęściej **MD5** lub **SHA**)
- *hasło n* to hash *hasła n-1*
- *hasło 0* jest tajne, to z niego generowane są pozostałe hasła
- podczas każdego logowania podajemy hasła od końca aż do ich wyczerpania, po czym należy wygenerować nową listę haseł przy użyciu innego tajnego *hasła 0*
- Obliczenie *hasła n+1* z *hasła n* jest bardzo proste
- Obliczenie *hasła n-1* z *hasła n* jest niemożliwe
- W Unix'ie hasłą jednorazowe generowane są za pomocą funkcji *skeyinit* i *skey*

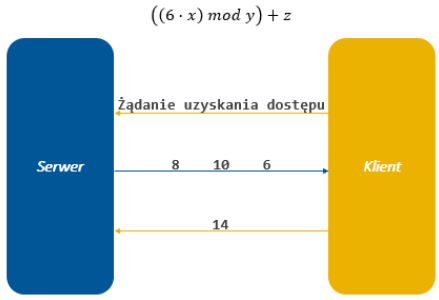
Zalety:

- Zwiększony poziom bezpieczeństwa
- Przechwycenie ostatnio użytego hasła nie jest niebezpieczne

Wady:

- Należy pamiętać *hasło 0*, aby w procesie uwierzytelniania móc obliczyć wymagane hasło

Systemy challenge-response



Systemy challenge-response działają w oparciu o prostą zasadę, polegającą na udzieleniu odpowiedzi na zadane przez system pytanie. W przypadku udzielenia poprawnej odpowiedzi użytkownik zostaje uwierzytelniony i przyznawany jest mu dostęp do chronionych zasobów. W najprostszej postaci systemy challenge-response żądają udzielenia prawidłowej odpowiedzi na proste pytania dotyczące użytkownika np. o jego ulubiony film. Nie mniej jednak, w praktyce stosuje się specjalne urządzenia zwane tokenami. W procesie uwierzytelniania serwer podaje pewną liczbę, którą należy wpisać do tokena, który to za pomocą złożonych funkcji matematycznych oblicza odpowiedź. Uzyskaną odpowiedź używa się w celu zweryfikowania tożsamośc.

Aspekt techniczny:

- Identyfikacja użytkownika na podstawie znajomości algorytmu
- Algorytm ten najczęściej jest „zaszyty” w specjalnym urządzeniu zwanym tokenem

Zalety:

- Złożone funkcje matematyczne znacząco zwiększają bezpieczeństwo
- Przechwycenie jednego użytego hasła nie jest niebezpieczne

Wady:

- Złamanie algorytmu „zaszytego” w tokenie równoważne jest z odgadnięciem tradycyjnego hasła i pozwala atakującemu na uzyskanie dostępu do chronionych zasobów zaatakowanego
- Token należy mieć zawsze przy sobie
- Proces uwierzytelniania się jest dłuższy i bardziej uciążliwy

Hasła zmienne w czasie

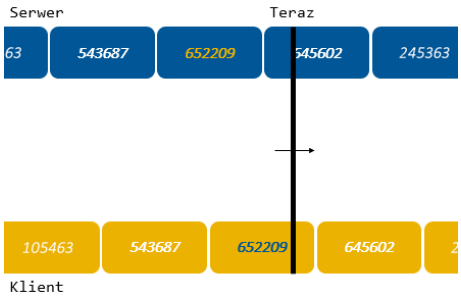
Kolejną metodą uwierzytelniania użytkowników są hasła zmienne w czasie. Podobnie jak w poprzednio omawianym przykładzie, metoda ta wykorzystuje zewnętrzne urządzenie zwane tokenem. Token co minutę generuje nowe jednorazowe hasło, które należy podać podczas uwierzytelniania się. Wpisane hasło porównywane jest z tak samo generowanym hasłem po stronie serwera. W przypadku zgodności tychże haseł użytkownikowi przydzielane są odpowiednie prawa dostępu do chronionych zasobów.

Aspekt techniczny:

- Hasło zmienia się najczęściej co minutę
- Hasło jest jednorazowe

Zalety:

- Większy, niż w przypadku tradycyjnego hasła, poziom bezpieczeństwa
- Gwarancja na token to zazwyczaj 2-3 lata



Wady:

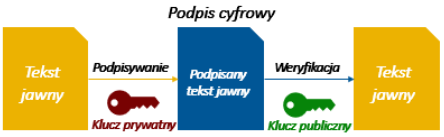
- Do uwierzytelnienia się potrzebne jest specjalne urządzenie
- Problem synchronizacji zegarów tokena i serwera

Techniki kryptograficzne

Techniki kryptograficzne wykorzystywane są głównie do zabezpieczania danych przed niepowołanym dostępem. Wykorzystują one algorytmy szyfrujące, umożliwiające utajnienie danych. Nie mniej jednak, kryptografia nie jest wykorzystywana tylko w tym celu. Algorytmy asymetryczne wykorzystywane są również w implementacji podpisów lub certyfikatów cyfrowych. Ponadto techniki kryptograficzne często stosowane są wraz z omówionymi dotąd metodami uwierzytelniania, co zdecydowanie podnosi poziom bezpieczeństwa użytkowników i ich danych.

Podpis elektroniczny

Podpis elektroniczny wykorzystuje algorytmy szyfrujące z kluczem publicznym (**algorytmy asymetryczne**). W przeciwieństwie do szyfrowania, w podpisie cyfrowym oryginalna wiadomość szyfrowana (**podpisywana**) jest kluczem prywatnym, a rozszyfrowywana (**weryfikowana**) kluczem publicznym.



Podpis cyfrowy zazwyczaj wykonywany jest wraz z szyfrowaniem. Nie mniej jednak w tym celu wykorzystywane są dwie pary kluczy. Jedna używana do podpisu i weryfikacji, a druga do szyfrowania i rozszyfrowywania.

W związku z wysoką złożonością obliczeniową algorytmów asymetrycznych, podpis cyfrowy najczęściej wykonuje się na skrócie wiadomości obliczonym za pomocą dowolnej metody haszującej.

Aspekt techniczny:

- Wykorzystywane są kryptograficzne algorytmy asymetryczne

Zalety:

- Skutecznie zabezpiecza przed spoofingiem
- Możliwość dodatkowego szyfrowania danych

Wady:

- Kosztowne obliczeniowo

Certyfikaty cyfrowe

Certyfikat jest elektronicznym zaświadczeniem, zawierającym niezbędne informacje pozwalające zweryfikować przynależność klucza publicznego do danego podmiotu. Dzięki temu, wykorzystując zaufaną stronę trzecią, możliwe jest jednoznaczne zweryfikowanie tożsamości użytkownika udzielającego dostępu do zasobów. Certyfikat zawiera trzy podstawowe informacje: klucz publiczny podmiotu, opis jego tożsamości oraz podpis cyfrowy złożony przez centrum certyfikujące.

Aspekt techniczny:

- Wykorzystywane w protokołach http, telnet, smtp, imap, pop3
- Istnieją dwa standardy opisujące certyfikaty cyfrowe
    - X.509 ze scentralizowaną instytucją certyfikującą
    - Zdecentralizowany PGP oparty o tzw. sieć zaufania
- W przeglądarce oznaczane jako zielona kłódka

Zalety:

- Skutecznie zabezpiecza przed spoofingiem
- Wbudowane w przeglądarki internetowe

Wady:

- Instytucje certyfikujące dla standardu X.509 są scentralizowane przez co są bardziej podatne na ataki i podszywanie się

Zabezpieczenia biometryczne

Zabezpieczenia biometryczne wchodzą w skład trzeciej grupy metod uwierzytelniania – *coś, kim jesteś*. Wykorzystują one ludzkie cechy, na podstawie których weryfikowana jest tożsamość użytkownika. Ze względu na popularność i niekiedy wygodę używania, metody te często wykorzystywane są w smartfonach jako jedyna lub jedna z metod uwierzytelniania (np. podczas odblokowywania telefonu). Niestety, wszystkie poniżej wymienione zabezpieczenia charakteryzują się dużą złożonością obliczeniową oraz obszernym zbiorem danych do analizy co niekiedy uniemożliwia ich skuteczne użycie w praktyce.

Czytnik linii papilarnych

- Sprawdza cechy charakterystyczne opuszka wybranego palca
- Musi działać szybko i dokładnie
- Możliwy do oszukania

Skaner twarzy

- Wykonuje zdjęcie tworzy
- Sprawdza cechy charakterystyczne (np.: odległość między oczami)
- Łatwe do oszukania w przypadku użycia kamer 2D

Skaner tęczówki oka

- Lokalizuje oczy
- Wykonuje zdjęcia tęczówki o bardzo wysokiej rozdzielczości
- Jest odporny na mruganie oczami, przymykanie oczu, celowe ruchy głowy
- Wykrywa cechy charakterystyczne
- Niestety większość tego urządzeń nie zapewnia zadowalającej skuteczności

Wykrywacz układu naczyń krwionośnych

- Skanuje dłoń przy pomocy promieni podczerwonych
- Analizuje cechy charakterystyczne

Skaner geometrii dłoni

- Wykonuje serię zdjęć 3D
- Oblicza i analizuje cechy charakterystyczne (np.: długość i szerokość palców, odległość między nimi lub pomiędzy kostkami)

BLIK

BLIK jest polskim systemem płatności mobilnych, wykorzystywanym przez użytkowników smartfonów. Umożliwia on na dokonywanie płatności, wypłacanie gotówki oraz wykonywanie przelewów, nawet pomiędzy bankami. Ponadto system ten pozwala na generowanie czeków.

System BLIK może być wykorzystywany tylko przez klientów korzystających z bankowości mobilnej, a transakcja realizowana jest pomiędzy klientem, który posiada odpowiednią, wydaną przez bank, aplikację mobilną a sklepem lub innym odbiorcą, zwanym akceptantem.

Identyfikacja użytkownika realizowana jest na podstawie jednorazowych kodów generowanych przez system Polskiego Standardu Płatności na żądanie banku. Proces uwierzytelniania i autoryzacji za pomocą systemu BLIK jest bardzo szybki wygląda następująco:

- Na początku generowany jest kod
- Kod wprowadzany jest przez użytkownika np. do terminalu w sklepie
- Autoryzacja przekazywana jest przez akceptanta do agenta rozliczeniowego Polskiego Standardu Płatności
- Weryfikacja kodu, identyfikacja banku, przekazanie autoryzacji do banku
- Autoryzacja przez bank, wysłanie odpowiedzi do akceptanta

Podsumowanie

Istnieje wiele metod uwierzytelniających użytkowników w sieci. Każda metoda ma swoje wady i zalety, dlatego warto je poznać i być ich świadomym. Żadna metoda nie jest najlepsza, a najskuteczniejszym sposobem zabezpieczenia się przed niepożądanym dostępem do chronionych zasobów jest wykorzystanie co najmniej dwóch różnych metod uwierzytelniania.