Metody ochrony informacji:

- fizyczne
- organizacyjno-proceduralne
- techniczne

Fizyczne:

- wyznaczenie stref administracyjnych i bezpieczeństwa
- odpowiednia zabezpieczone i zamykane pomieszczenia
- sejfy i szafy metalowe
- systemy kontroli wejść i wyjść

Organizacyjno-proceduralne:

- właściwa struktura organizacyjna
- opracowanie strategicznych dokumentów (polityka bezpieczeństwa, SWB, PBE, instrukcje, zarządzenia)
- bezpieczeństwo osobowe (poświadczenia bezpieczeństwa, szkolenia)
- zarządzanie bezpieczeństwem systemu (analiza ryzyka i istniejących zagrożeń, reagowanie na incydenty)
- prowadzenie szkoleń i akcji uświadamiających

Techniczne:

- zabezpieczenia programowe i sprzętowe (np. metody kryptograficzne)
- systemy automatycznej identyfikacji i kontroli dostępu (karty identyfikacyjne, klucze, kody)
- systemy monitoringu
- systemy alarmowe
- zabezpieczenia elektromagnetyczne
- zastosowanie dróg obejściowych w celu zwiększenia zabezpieczenia transmisji

Zabezpieczenia programowe – kryptografia (pojęcia):

- Kryptologia - dziedzina wiedzy o przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem
- Kryptografia - zajmuje się zabezpieczaniem informacji (szyfrowanie, deszyfrowanie). Obejmuje metody utajniania danych w wyniku ich przekształcenia metodami matematycznymi w szyfry
- Kryptoanaliza - czyli gałąź wiedzy o przełamywaniu zabezpieczeń oraz o deszyfrowaniu wiadomości przy braku klucza lub innego wymaganego elementu schematu szyfrowania

Techniki kryptograficzne przed czym chronią:

- Techniki kryptograficzne pozwalają zabezpieczyć przed niepowołanym dostępem dane znajdujące się na dysku, nawet gdy inni mają dostęp do tego komputera
- Zaszyfrowane dane mogą być w bezpieczny sposób transmitowane przez sieć i nawet jeśli zostaną przechwycone, ich zawartość jest nadal bezpieczna.
- Szyfrowanie może być dokonywane w miarę potrzeb – np. tylko na czas transmisji, w celu utworzenia bezpiecznego kanału komunikacyjnego..
- Kryptografia pomaga wykryć przypadkowe lub celowe modyfikacje danych
- Technik kryptograficznych można użyć w celu weryfikacji autora dokumentu (podpis elektroniczny)

Techniki kryptograficzne przed czym nie chronią:

- Kryptografia nie zabezpiecza przed usunięciem plików
- Jeśli jakiś program lub osoba jest w staje podmienić programy, z których korzystasz, może uzyskać dostęp do jawnej wersji plików
- Wersje plików w postaci niezaszyfrowanej mogą znajdować się w katalogach tymczasowych, co może prowadzić do potencjalnej kradzieży danych

Szyfrowanie pojęcia:

- Algorytm szyfrowania –Funkcja, oparta na solidnych podstawach matematycznych, dokonująca właściwego szyfrowania lub deszyfracji.
- Klucz szyfrowania – używany przez algorytm szyfrujący do przekształcenia danych z postaci jawnej do zaszyfrowanej lub na odwrót.
- Długość klucza – zależna od używanego algorytmu. Dłuższe klucze są bezpieczne, ale wymagają dłuższego czasu na szyfrowanie/deszyfrowanie, więc konieczny jest kompromis.
- Tekst jawny – informacje które szyfrujemy.
- Tekst niejawny lub zaszyfrowany – informacje uzyskane po zaszyfrowaniu teksu jawnego.

Rodzaje szyfrów:

- Szyfry strumieniowe
- Szyfry blokowe

Szyfry strumieniowe:

- Algorytm symetryczny, który szyfruje oddzielnie każdy bit wiadomości. Algorytm ten składa się z generatora strumienia bitowego, będącego kluczem szyfrującym oraz elementu dodającego (na przykład operacji XOR)
- Szyfry strumieniowe nadają się raczej do szyfrowania ciągłej transmisji bitów pomiędzy stronami niż pojedynczej wiadomości.

- Generator strumienia klucza jest generatorem okresowym. Długość okresu stanowi o bezpieczeństwie systemu.

Szyfry blokowe:

- Polega na szyfrowaniu bloku wejściowego (np. fragmentu pliku) na podstawie zadanego klucza, przekształcając go na blok wyjściowy o takiej samej długości w taki sposób, że niemożliwe jest odwrócenie tego przekształcenia bez posiadania klucza.
- Typowe rozmiary bloku oraz kluczy to 64, 128, 192 lub 256 bitów, przy czym klucze mniejsze od 128 bitów nie zapewniają współcześnie bezpieczeństwa.

Szyfry blokowe - podstawowe tryby pracy:

ECB – Elektroniczna Książka kodowa

- Każdy blok tekstu jest szyfrowany niezależnie od pozostałych
- Najłatwiejszy do zastosowania
- Błąd transmisji/uszkodzenie w pojedynczym bloku szyfrogramu powoduje uszkodzenie pojedynczego bloku tekstu jawnego
- Podatny na kryptoanalizę jeśli mamy dostęp do tekstu jawnego i szyfrogramu, możemy zacząć odtwarzać książkę kodową.
- Podatny na ataki z podstawieniem lub powtórzeniem bloku.

CBC – Wiązanie Bloków Zaszyfrowanych

- Tekst jawny jest przed zaszyfrowaniem sumowany modulo 2 z poprzednimi blokami szyfrogramów
- Podatny na błędy transmisji – uszkodzenie bloków szyfrogramu powoduje niemożność odszyfrowania kolejnych bloków.

CFB – Szyfrowanie ze sprzężeniem zwrotnym

- dane są szyfrowane w jednostkach mniejszych niż rozmiar bloku
- Tryb CFB może być użyty do szyfrowania dowolnej liczby bitów.
- Błędy bitowe w tekście niejawnym bloku szyfru powodują błąd bitowy na tych samych pozycjach w tekście jawnym

CTR(*Counter*) - tryb licznikowy

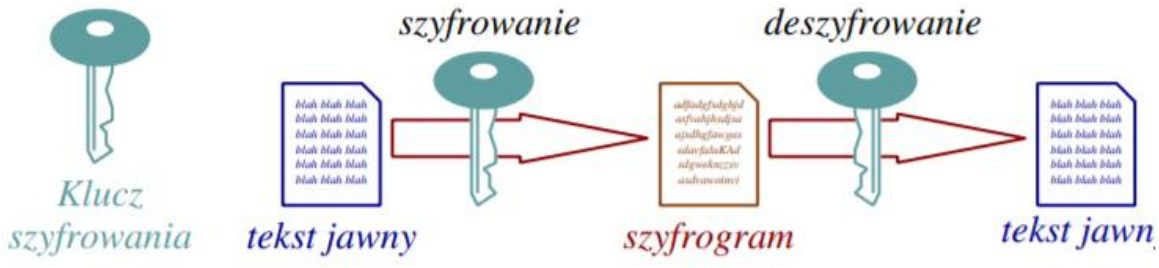
CCM(Counter with CBC-MAC) - Szyfrowanie i uwierzytelnianie

OFB(*Output Feedback*) – z wyjściowym sprzężeniem zwrotnym

OCB (Offset Codebook Mode) – książka kodowa z przesunięciem

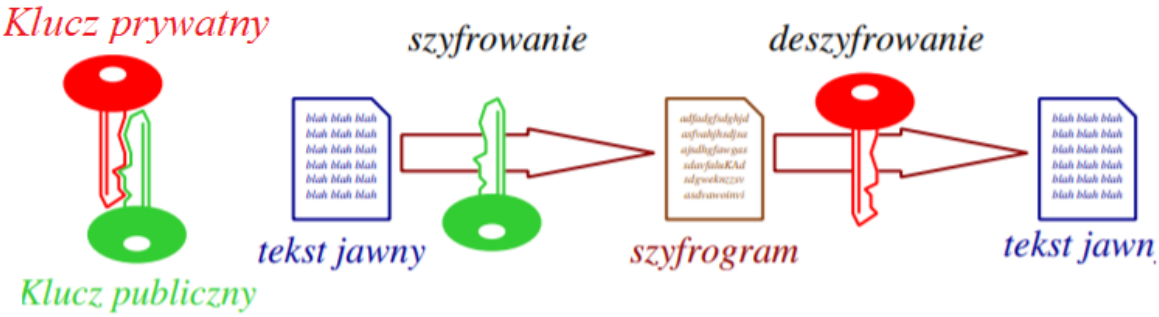
Systemy z kluczem prywatnym:

- Ten sam klucz jest używany zarówno do szyfrowania jak i deszyfrowania. Jeżeli szyfrowana jest transmisja danych, klucz musi być znany dla oby stron przed rozpoczęciem transmisji i uzgodniony z użyciem innego kanału komunikacyjnego. Inaczej system z kluczem symetrycznym.
- Systemy z kluczem prywatnym są znacznie szybsze niż systemy z kluczem publicznym, ale nie mogą być użyte w celu utworzenia bezpiecznego kanału komunikacyjnego jeśli nie dysponujemy innym bezpiecznym kanałem w celu wymiany kluczy.



Systemy z kluczem publicznym:

- Korzystając z klucza publicznego (który może być ogólnie znany, opublikowany) w celu szyfrowania danych i klucza prywatnego w celu deszyfracji. Zwane również systemami z kluczem asymetrycznym.
- Systemy z kluczem publicznym mogą zostać użyte do utworzenia bezpiecznego kanału komunikacyjnego nawet wtedy, gdy nie możemy wymienić kluczy w sposób tajny. Są przez to znacznie wolniejsze niż systemy z kluczem prywatnym.



Systemy hybrydowe:

- Ze względu na zalety obu poprzednich systemów zaczęto stosować systemy hybrydowe. Wolniejszy w działaniu system z kluczem publicznym jest używany w celu nawiązywania komunikacji iw wymiany losowo wygenerowanego klucza sesji, który jest następnie używany jako klucz symetryczny, znany przez obie strony i obowiązujący tylko na czas trwania tego połączenia.
- Obecnie prawie wszystkie systemy są systemami hybrydowymi.

Systemy z kluczem prywatnym – rodzaje:

- Crypt – tradycyjna metoda szyfrowani w systemach UNIX
- DES (Data Encryption Standard) – 56 bitowe klucze, nie jest bezpieczny
- Potrójny DES – DES zastosowany trzy razy pod rząd z innymi kluczami
- RC2,RC4 i RC5 – RC2 i RC5 szyfry blokowe, RC4 to szyfr strumieniowy
- IDEA (International Data Encryption Algorithm) – 128-biotwy klucz, używane przez SSH.
- Skipjack – 80-bitowy klucz, nie dostępny do użytku publicznego.

- Blowfish – alternatywa algorytmu Skipjack, dostępny do użytku publicznego
- AES (Advanced Encryption Standard) – następca DES, używa 128,192 lub 256 bitowych kluczy

Systemy z kluczem publicznym – rodzaje:

- Diffie-Hellman – System wymiany kluczy pomiędzy dwoma lub więcej stronami. Metoda bezpiecznej wymiany danych przez kanał publiczny. Używany jako metoda ustalania klucza sesji.
- RSA (Rivesta,Shamir,Adleman)– używany do szyfrowania danych lub podpisywania dokumentów
- ElGamal – używany podobnie jak RSA. Oparty na metodach wykładniczych i arytmetyce resztkowej
- DSA (Digital Signature Algoritm) – używany do generowania podpisów cyfrowych. Dowolna długość klucza (typowa 512-1024 bitów).

Kryptograficzne funkcje skrótu:

- Zwane takie funkcjami haszującymi lub kryptogamicznymi funkcjami sumy kontrolnej
- W powtarzalny sposób przetwarzają dane wejściowe dowolnej długości na łańcuch wynikowy o stałej, niewielkiej długości.
- Funkcje jednokierunkowe, tzn. te same dane dają ten 5am wynik, ale nie jest możliwe odtworzenie danych wejściowych na podstawie wyniku.
- Nawet drobna zmiana w danych wejściowych zmienia znacząco część lub całość wyniku, nie jest więc możliwe do przewidzenia jak zmienić dane wejściowe tak, by otrzymać ten sam wynik funkcji skrótu.
- Przy co najmniej 128 bitach wynikowych atak siłowy w celu znalezienia danych generujących zadany skrót jest poza zasięgiem jakichkolwiek systemów komputerowych (1.7 – 10^38 możliwości do sprawdzenia).
- Mogą być używane do sprawdzania spójności danych lub podpisów cyfrowych.

Zamiast podpisywać kryptograficznie całą wiadomość. co wymagałoby kosztownego szyfrowania kilo-bajtów lub megabajtów danych metodą asymetryczną, można wyliczyć jej skrót MD5 i podpisać wyłącznie-nie skrót

Skrót MD5 lub SHA ważnych plików może zostać wygenerowany i zapamiętany gdzieś poza systemem, aby
w razie wątpliwości przekonać się, czy pliki nie zostały zmodyfikowane.

Algorytmy funkcji skrótu:

- MD2, MD4 i MD5 – najczęściej używane funkcje, produkujące 128-bitowy wynik. Funkcja MD2 nie ma żadnych ułomności lecz jest bardzo wolna. MD4 jest szybsza, ale krótko po opublikowaniu wykryto pewne metody ataku, co w rezultacie zaowocowało utworzeniem funkcji MD5 – nieco wolniejszej, ale bezpieczniejszej i najszerzej obecnie stosowanej.
- SHA(SHA-1,SHA-2) – Działa podobnie jak algorytm MD4/MD5, ale produkuje 160-bitowe wyniki. Zaprojektowany przez NSA.

- HAVAL – Modyfikacja algorytmu funkcji MD5, dla danych wyjściowych od 92 do 256 bitów z możliwością regulacji wewnętrznych iteracji algorytmu. Można używać jako szybki i mało bezpieczny lub wolny i bezpieczny algorytm.
- SNEFRU – produkuje 128 lub 256 bitowe wyniki. Umożliwia regulację wewnętrznych iteracji, jednak przy 4 przebiegach występują pewne słabości, a rekomendowana 8-przebiegowa funkcja jest wolniejsza od MD5 czy HAVAL.

Zastosowania kryptografii:

Aplikacje użytkownika końcowego korzystają z funkcji kryptograficznych w celu ochrony danych przechowywanych w systemie komputerowym:

- PGP, używane do szyfrowania/deszyfrowania danych;
- PGP, używane do ręcznej weryfikacji podpisów cyfrowych;
- SSH, używane do zdalnego logowania w bezpieczny sposób;
- Różnorakie programy szyfrujące zawartość plików lub dysków;
- Możliwości szyfrowania wbudowane w wiele aplikacji (edytory tekstu, bazy danych, arkusze kalkulacyjne, itp.)

Warstwy oprogramowania sieciowego korzystają z funkcji kryptograficznych, stanowiących odrębną warstwę (sytuowaną zwykle w okolicach warstwy transportowej lub sesji), dostarczając tym samym mechanizmów nieobecnych w niższych warstwach.

- SSL. używane do nawiązywania szyfrowanych połączeń, wbudowane w wielu aplikacjach klienckich takich jak Netscape. MSIE. lynx. pine, etc.
- SSH, używane w celu zestawiania tuneli i forwardowania portów;
- PGP, używane jako automatyczna warstwa dokonująca szyfrowania/deszyfrowania;
- wszystkie programy VPN (Virtual Private Networks).

Metody łamania szyfrów:

- Metoda prób i błędów - metoda prób i błędów polega na podstawianiu różnych kombinacji klucza i poszukiwaniu sensownego tekstu jawnego. Metoda łamania klucza w wyniku wypróbowania wszystkich możliwych jego kombinacji nazywa się atakiem brutalnym.
- Analiza statystyczna - analiza statystyczna sprowadza się do określenia prawdopodobieństwa rozkładu liter w kryptogramie i tekście jawnym. Ponieważ rozkład liter jest charakterystyczną cechą każdego języka, informacje takie można wykorzystać do łamania niektórych szyfrów, np. szyfrów podstawieniowych.
- Wyszukiwanie prawdopodobnych słów - każdy dokument lub program zawiera pewne słowa i zwroty pojawiające się w określonych miejscach. W dokumentach takimi słowami są np. nazwy miejscowości i zwroty grzecznościowe, a w programach słowa kluczowe. Za pomocą prawdopodobnych słów można znaleźć fragmenty klucza.
- Analiza matematyczna - metoda ta polega na napisaniu układu równań na podstawie znanych algorytmów, którego rozwiązanie da wartości zmiennych, reprezentujących

fragmenty wiadomości lub klucza. W ten sposób można również uzyskać wyrażenia generujące klucze kryptograficzne.

Inne techniczne sposoby zabezpieczania danych:

Kryptografia w sprzęcie

Przykład: Prosty zamek elektroniczny w oparciu o iButton

- Każdy iButton to urządzenie elektroniczne komunikujące się protokołem 1Wire i posiadające unikalny elektroniczny identyfikator wygrawerowany laserowo w krzemie
- Czytnik iButton otwiera drzwi na podstawie odczytanego 64-bitowego numeru przyłożonej pastylki iButton.

Problemy:

- Trywialne do podrobienia techniką nagraj-odtwórz (aktywny spoofing)
- Pojedynczy iButton może zostać sklonowany lub zaemulowany za pomocą innego urządzenia, dając efektywnie taki sam dostęp.

Kryptografia w sprzęcie (c.d.)

Rozwiązanie: Kryptograficzny iButton

- Pewne tajne dane są przechowywane w pamięci nieulotnej iButtona i nie są możliwe do odczytania wprost. Te same dane muszą być znane w systemie autoryzacji dostępu za pomocą iButtona.
- Czytnik iButton wysyła jakieś dane (mogą być losowe) do iButtona
- Odebrane dane są doklejane do pamiętanych danych tajnych i dopiero z nich razem wewnątrz iButtona liczony jest skrót kryptograficzny
- Do czytnika transmitowany jest wyliczony skrót. Jeśli taki sam skrót został wygenerowany w systemie autoryzacji dostępu, autoryzacja jest poprawna.
- Tajne dane nie są nigdy transmitowane pomiędzy iButtonem i czytnikiem, więc nie mogą zostać skradzione.

Analogiczny problem dotyczy identyfikacji za pomocą prostych tagów RFID lub "zwykłych" kart ATM (wyłącznie z paskiem magnetycznym) autoryzowanych PINem

Hasła zmienne w czasie

- hasło zmienia się automatycznie co minutę,
- centralny serwer autoryzacyjny,
- do zalogowania się potrzebne jest specjalne urządzenie – wielkości breloka do kluczy lub karty kredytowej,
- kod podawany na wyświetlaczu uzupełniany jest kodem PIN,
- po użyciu hasło traci ważność natychmiast i nie może zostać użyte do zalogowania się na inny system,
- problem synchronizacji serwera z tokenem.
- „gwarancja" lub raczej licencja udzielana na czas 2-3 lat.
- Istniejące rozwiązania: tokeny VASCO lub Secure ID
- Bardziej zaawansowane rozwiązania: klawiatura pozwalająca wpisać PIN, który uaktywnia urządzenie.

Hasła zmienne w czasie

Hasła zmienne w czasie

Tokeny RSA:

- standardowo: hasło zmienia się automatycznie co minutę,
- kod podawany na wyświetlaczu uzupełniany jest kodem PIN,
- po użyciu hasło traci ważność natychmiast i nie może zostać użyte do zalogowania się na inny system,

Tokeny VASCO:

- Klawiatura zabezpieczająca dostęp do tokena za pomocą kodu PIN
- 2 tryby pracy:
  - „standardowy" - generator haseł zmiennych w czasie
  - dodatkowy – challenge-response: kod podany na stronie WWW należy przepisać na klawiaturze w celu uzyskania odpowiedzi

Listy haseł

- Używane głównie przez banki jako podstawowa i najtańsza metoda implementacji haseł jednorazowych time keys.
- Losowo generowana lista haseł musi być przekazana klientowi w bezpieczny sposób (np. zwykłą pocztą)
- Hasła SMS-owe

Literatura:

1. **Wykłady dr inż. T. Surmacza, pt. Systemy Ochrony Informacji, Wrocław 2018 r.**
2. **https://www.bezpieczneit.com/metody-ochrony-systemow-teleinformatycznych/ [stan na dzień 24.05.2019]**
3. **https://pl.wikipedia.org/wiki/Kryptologia [stan na dzień 24.05.2019]**
4. **https://pl.wikipedia.org/wiki/Szyfr_strumieniowy [stan na dzień 24.05.2019]**
5. **https://pl.wikipedia.org/wiki/Szyfr_blokowy [stan na dzień 24.05.2019]**