Techniczne środki bezpieczeństwa

Kamil Breczko

06.12.2018

Plan prezentacji

1. Kopie bezpieczeństwa
   - Backup online
   - Backup offline
   - Porównanie
2. Szyfrowanie
   - Szyfrowanie asymetryczne
   - Szyfrowanie symetryczne
3. Identyfikacja, uwierzytelnianie i autoryzacja
4. Zasilanie awaryjne
5. Fizyczna ochrona informacji

Kopie bezpieczeństwa

Rodzaje

Wyróżnia się dwa rodzaje kopii bezpieczeństwa:

- Off-line (zwykle na nośnikach zewnętrznych)
- On-line (RAID, serwery backupowe, hot standby)

Definicja

Backup online polega na dzierżawieniu przestrzeni dyskowej i oprogramowania automatyzującego proces. Zapewnia także synchronizację danych, szyfrowanie oraz nadawanie praw dostępu.

Definicja

Backup offline to kopiowanie danych na określone nośniki pamięci takie jak: inny komputer (lub inna partycja dysku na naszym komputerze), płyty CD/DVD, pendrive, czy też dyski zewnętrzne.


Dropbox

Archiwizacja a kopia bezpieczeństwa

Rodzaje kopii off-line

- Archiwizacja
- Kopie zapasowe (backupy)

Definicja

Archiwizacja danych - czynność przeniesienia danych w inne miejsce w pamięci masowej, w celu ich długotrwałego przechowywania.

Definicja

Kopia bezpieczeństwa, kopia zapasowa (ang. backup copy) - dane, które mają służyć do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia.

W odróżnieniu od archiwizacji, kopia bezpieczeństwa obejmuje, oprócz danych, także oprogramowanie pozwalające na ich interpretację. Zazwyczaj pozwala na szybkie odtworzenie systemu informatycznego w przypadku jego uszkodzenia.

Kopia bezpieczeństwa

Czynniki wpływające na metody składowania danych:

- koszty nośników
- czas potrzebny na wykonanie kopii
- czas niezbędny do ich odtworzenia oraz niezawodność nośników, na jakich są one zapisane

Rodzaje nośników

Ze względu na technologię zapisu możemy wyszczególnić 5 rodzajów nośników:

- taśmy magnetyczne,
- dyski magnetyczne,
- dyski magnetooptyczne,
- dyski optyczne,
- pamięci typu „flash”,

Typy backupów

Wyróżniamy 4 typy backupów:

- Backup pełny (ang. Full backup) polega na całościowym zarchiwizowaniu danych
- Backup przyrostowy (ang. Incremental backup) archiwizuje jedynie pliki, które powstały lub uległy modyfikacji od czasu wykonania ostatniego backupu
- Backup różnicowy (ang. Differential backup) archiwizuje pliki utworzone lub zmienione po ostatnim backupie pełnym
- Backup typu delta (ang. Delta backup) jest właściwie podtypem backupu różnicowego lub przyrostowego. Archiwizowane są nie całe modyfikowane pliki, a jedynie ich fragmenty

Typ *backupu*	**Czas wykonywania**	**Czas odtwarzania**	**Wykorzystanie nośników**
Backup pełny	Długi	Krótki	Duże
Backup przyrostowy	Krótki	Długi	Małe
Backup różnicowy	Średni	Średni	Średnie

Backup online

Plusy:

- dane dostępne wszędzie tam gdzie jest połączenie z internetem
- kopie są przechowywane w innym miejscu - dzięki temu odporne są na zdażenia losowe

Minusy:

- dostęp do danych zapasowych, jeżeli brak dostępu do internetu
- brak możliwości tworzenia kopii zapasowych, jeżeli nie masz połączenia z internetem

Backup offline

Plusy:

- dane są zachowane na nośnikach niepołączonych z siecią – nikt nie może ich wykraść
- proces może być automatyczny jak w backupie online

Minusy:

- istnieje ryzyko, że w wyniku lokalnej katastrofy wszyskie dane zostaną stracone
- backup offline to realne zajęcie miejsca... fizycznego.

Szyfrowanie

Definicja

Szyfrowaniem określa się proces przekształcania tekstu czytelnego dla człowieka lub informacji w innej postaci (np. zarejestrowanego materiału dźwiękowego lub filmowego) na niezrozumiały ciąg znaków w celu jego utajnienia

Definicja

Deszyfrowanie - czynność odwrotna, która ma na celu przekształcenie tekstu tajnego na jawny.

Rodzaje szyfrowania (najważniejsze):

- szyfry symetryczne (całe systemy plików lub całe dyski)
- szyfry asymetryczne (szyfrowanie pojedynczych plików)

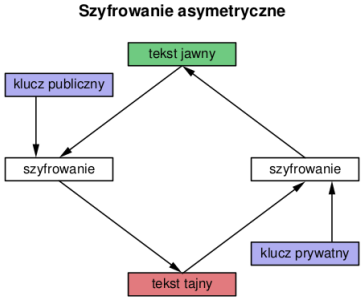
Szyfrowanie asymetryczne

W asymetrycznych metodach szyfrowania zarówno nadawca, jak i odbiorca dysponują oddzielną parą kluczy. Para ta składa się z:

- klucza publicznego (public key) - jawny i dostępny do publicznej wiadomości
- klucza prywatnego (private key) - musi być przechowywany w ukryciu

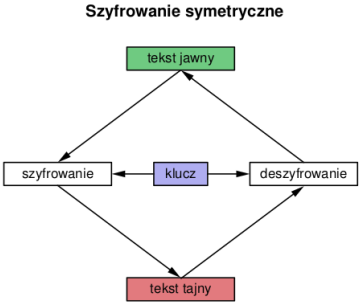
Wady:

- Każdy plik trzeba szyfrować osobno.
- Wiele programów przetwarzających pliki tworzy kopie zapasowe. Trzeba pamiętać, żeby je też szyfrować lub usuwać.
- Wolne działanie

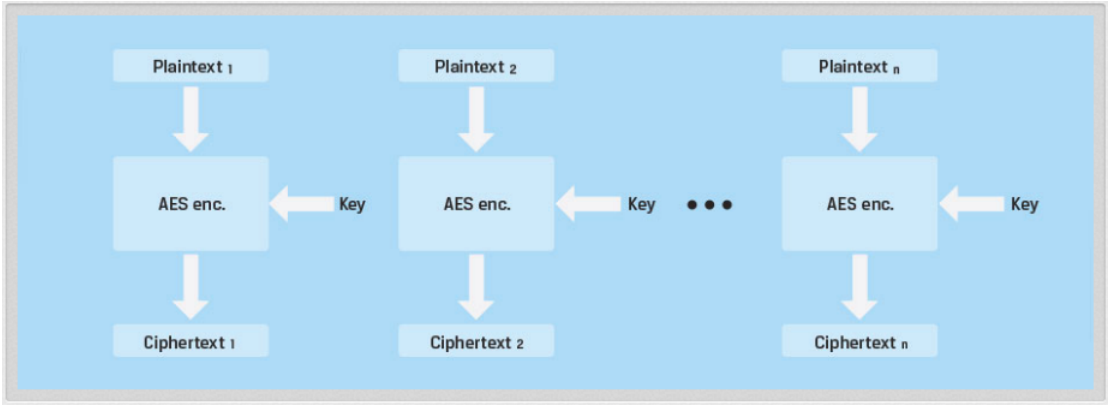


Szyfrowanie symetryczne

- W metodach symetrycznych używa się tego samego klucza do szyfrowania i deszyfrowania wiadomości
- Przed przekazaniem poufnych informacji nadawca i odbiorca muszą więc wspólnie ustalić tajny klucz i dostarczyć go sobie bezpiecznym kanałem
- Funkcje są szybko obliczalne w porównaniu do szyfrowania asymetrycznego



Tryby kodowania bloków - ECB (Electronic Codebook)



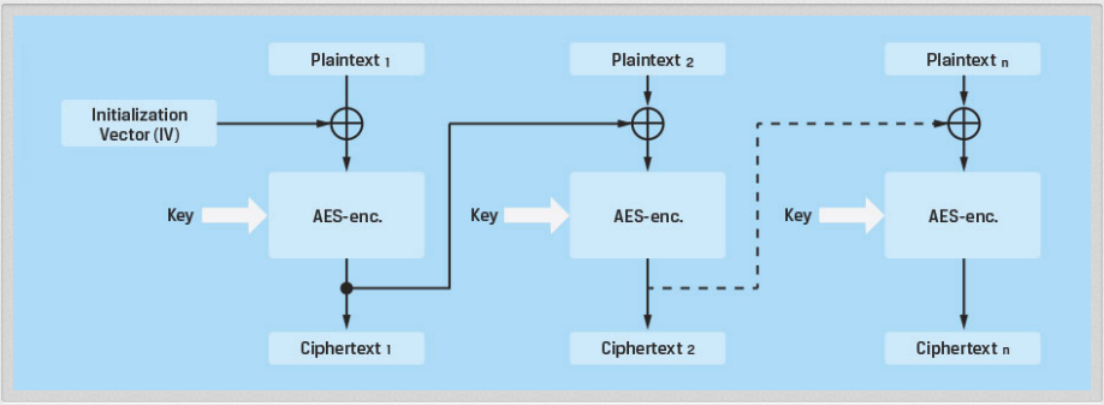
Tryby kodowania bloków - ECB (problem)

Oryginalny obraz

Szyfrowanie z użyciem trybu ECB

Szyfrowanie z użyciem innego trybu

Tryby kodowania bloków - CBC (Cipher Block Chaining)



Wady:

- konieczność wymiany tajnego klucza
- komunikacja pomiędzy obcymi jednostkami

Wady:

- konieczność wymiany tajnego klucza
- komunikacja pomiędzy obcymi jednostkami

Główny problem: jak ustalić wspólny klucz?

Wady:

- konieczność wymiany tajnego klucza
- komunikacja pomiędzy obcymi jednostkami

Główny problem: jak ustalić wspólny klucz?
Rozwiązanie: Przesłać innym, zabezpieczonym kanałem (zazwyczaj niepraktyczne / drogie)

Wady:

- konieczność wymiany tajnego klucza
- komunikacja pomiędzy obcymi jednostkami

Główny problem: jak ustalić wspólny klucz?
Rozwiązanie: Przesłać innym, zabezpieczonym kanałem (zazwyczaj niepraktyczne / drogie)

Lepiej zastosować inne podejście: szyfrowanie asymetryczne !

Wady:

- konieczność wymiany tajnego klucza
- komunikacja pomiędzy obcymi jednostkami

Główny problem: jak ustalić wspólny klucz?
Rozwiązanie: Przesłać innym, zabezpieczonym kanałem (zazwyczaj niepraktyczne / drogie)

Lepiej zastosować inne podejście: szyfrowanie asymetryczne !

Szyfrowanie sprzętowe - dyski samoszyfrujące?

Wady:

- konieczność wymiany tajnego klucza
- komunikacja pomiędzy obcymi jednostkami

Główny problem: jak ustalić wspólny klucz?
Rozwiązanie: Przesłać innym, zabezpieczonym kanałem (zazwyczaj niepraktyczne / drogie)

Lepiej zastosować inne podejście: szyfrowanie asymetryczne !

Szyfrowanie sprzętowe - dyski samoszyfrujące?
Samoszyfrujące dyski twarde, zwane SED (self-encrypting hard drive), automatycznie szyfrują wszystkie dane w czasie rzeczywistym, które znajdują sie na nośnikach. Oznacza to, że przy każdym dostępie do pliku, dane są szyfrowane i odszyfrowywane. Zabezpieczanie danych jest całkowicie niewidoczne dla użytkownika, co powoduje że użytkownik nie musi samodzielnie zabezpieczać danych. Wszystkim zajmuje się kontroler dysku.

Wady:

- konieczność wymiany tajnego klucza
- komunikacja pomiędzy obcymi jednostkami

Główny problem: jak ustalić wspólny klucz?
Rozwiązanie: Przesłać innym, zabezpieczonym kanałem (zazwyczaj niepraktyczne / drogie)

Lepiej zastosować inne podejście: szyfrowanie asymetryczne !

Szyfrowanie sprzętowe - dyski samoszyfrujące?
Samoszyfrujące dyski twarde, zwane SED (self-encrypting hard drive), automatycznie szyfrują wszystkie dane w czasie rzeczywistym, które znajdują sie na nośnikach. Oznacza to, że przy każdym dostępie do pliku, dane są szyfrowane i odszyfrowywane. Zabezpieczanie danych jest całkowicie niewidoczne dla użytkownika, co powoduje że użytkownik nie musi samodzielnie zabezpieczać danych. Wszystkim zajmuje się kontroler dysku.

Jak bezpieczne?

Wady:

- konieczność wymiany tajnego klucza
- komunikacja pomiędzy obcymi jednostkami

Główny problem: jak ustalić wspólny klucz?
Rozwiązanie: Przesłać innym, zabezpieczonym kanałem (zazwyczaj niepraktyczne / drogie)

Lepiej zastosować inne podejście: szyfrowanie asymetryczne !

Szyfrowanie sprzętowe - dyski samoszyfrujące?
Samoszyfrujące dyski twarde, zwane SED (self-encrypting hard drive), automatycznie szyfrują wszystkie dane w czasie rzeczywistym, które znajdują sie na nośnikach. Oznacza to, że przy każdym dostępie do pliku, dane są szyfrowane i odszyfrowywane. Zabezpieczanie danych jest całkowicie niewidoczne dla użytkownika, co powoduje że użytkownik nie musi samodzielnie zabezpieczać danych. Wszystkim zajmuje się kontroler dysku.

Jak bezpieczne?
Dyski samoszyfrujące to blackbox, nie wiemy co dokładnie znajduje się wewnątrz

Przykłady algorytmów

Szyfr	Klucz	Blok	Uwagi
AES	128, 192, 256	128	NIST Std 2001; "Rijndael" (Daemen & Rijmen)
Twofish	128, 256	128	Schneier 1998; AES finalist; 16-round Feistel
Blowfish	32–448	64	Schneier 1993; AES finalist; 16-round Feistel
Serpent	128, 192, 256	128	Anderson, Biham, Knudsen 1998; AES finalist
Camellia	128, 192, 256	128	Mitsubishi, NTT, 2000; 18–24-round Feistel
Anubis	128–320	128	Rijmen, Barreto 2000
CAST6	128–256	128	48-round generalized Feistel; 1998
3DES	56, 112, 168	64	16,32,48-round Feistel; 1998
Legacy			
KHAZAD	128	64	Rijmen, Barreto 2000
Tea	128	64	Needham, Wheeler 1994; Feistel network
RC4	40–2048	—	strumieniowy; Rivest 1994
CAST5	40–128	64	Adams, Tavares 1996; 12–16-round Feistel; GPG
DES	56	64	NIST standard 1979; 16-round Feistel

Identyfikacja, uwierzytelnianie i autoryzacja

W celu ochrony systemów informatycznych przed niebezpieczeństwem związanym z dostępem osób niepowołanych, stosowane są techniki:

- identyfikacji (ang. Identification)
- uwierzytelniania (ang. Authentication)
- autoryzacji (ang. Authorization)

Definicja

Identyfikacja - to proces umożliwiający rozpoznanie użytkownika w systemie.

Definicja

Uwierzytelnianie pozwala na weryfikację tożsamości użytkownika z danymi zawartymi w systemie.

Definicja

Autoryzacja - potwierdzenie, czy dany podmiot jest uprawniony do uzyskania dostępu do żądanego zasobu.

Uwierzyteleninie

„COŚ, O CZYM WIESZ”

PASSWORD 123

Hasła
Osobiste numery identyfikacyjne
Słowo kluczowe (nazwisko panieńskie matki)

„COŚ, CO POSIADASZ”

Klucze
Tokeny (sprzętowe lub programowe)
Karty szyfrujące
Karty inteligentne
Certyfikaty cyfrowe i klucze prywatne

„COŚ, CZYM SIĘ CHARAKTERYZUJESZ”

Odcisk palca
Obraz tęczówki lub siatkówki oka
Geometria dłoni, twarzy itp.
Głos
Sposób pisania

Token

- należy do kategorii "Coś, co posiadasz"
- urządzenie kryptograficzne generujące jednorazowe hasła
- działanie tokena opiera się na algorytmach oraz kluczach kryptograficznych
- generuje ciąg cyfr przy użyciu prywatnego klucza, bazując na czasie lub wprowadzonym wcześniej ciągu cyfr stanowiących hasło

Porównawcze wybranych technologii biometrycznych

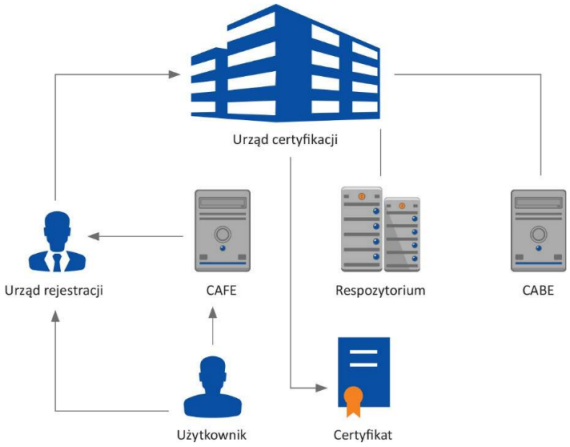
Cecha biometryczna	Przyczyny błędów	FAR	FRR	Poziom bezpieczeństwa	Stabilność w czasie
Odcisk palca	Uszkodzenia skóry, wiek użytkownika	Mały	Mały	Duży	Średnia
Twarz	Uszkodzenia, wiek, zarost, fryzura, mimika, oświetlenie	Mały	Duży	Mały	Mała
Tęczówka	Oświetlenie	Mały	Mały	Duży	Duża
Głos	Wiek, choroby, tło dźwiękowe	Średni	Duży	Mały	Mała

FRR (ang. False rejection rate) - współczynnik błędnych odrzuceń prawidłowych prób zalogowania
FAR (ang. False acceptance rate) - współczynnik błędnych akceptacji nieprawidłowych prób logowania

Bezpieczeństwo sieci

Infrastruktura klucza publicznego, w skrócie PKI (ang. Public Key Infrastructure), jest najbardziej kompleksowym rozwiązaniem problemów związanych z bezpieczeństwem sieci. Polega na szyfrowaniu asymetrycznym oraz kluczach kryptograficznych, wydawanych przez zaufaną, trzecią stronę, którą jest Główny Urząd Certyfikacji (ang. Root Certification Authority).

Proces certyfikacji



Przykłady

Uwierzytelnienie:

- personel banku prosi o podanie ustawionego wcześniej hasła telefonicznego, daty urodzenia, nazwiska panieńskiego matki; suma poprawnych odpowiedzi daje wysokie prawdopodobieństwo, że dana osoba jest tą, za którą się podaje;
- serwer prosi użytkownika o wpisanie hasła (lub wskazanie pliku klucza) i weryfikuje jego zgodność z wcześniej ustawioną wartością;

Identyfikacja:

- w rozmowie telefonicznej z centrum obsługi banku klient deklaruje swoje imię, nazwisko i numer konta (bank jest stroną ufającą);
- w procesie logowania do serwera użytkownik wpisuje nazwę (login) (serwer jest stroną ufającą);

Autoryzacja:

- serwer weryfikuje uprawnienia zalogowanego użytkownika do konkretnego pliku sprawdzając tablicę dostępu w systemie plików;
- przeglądarka sprawdza zapisane w certyfikacie serwera flagi keyUsage, weryfikując czy został on poświadczony przez uprawniony podmiot;

Zasilanie awaryjne

Podstawowymi urządzeniami, które podnoszą bezpieczeństwo energetyczne, są zasilacze awaryjne UPS (ang. Uninterruptable Power Supply). Możemy wyróżnić 2 rodzaje konfiguracji systemu zasilania:

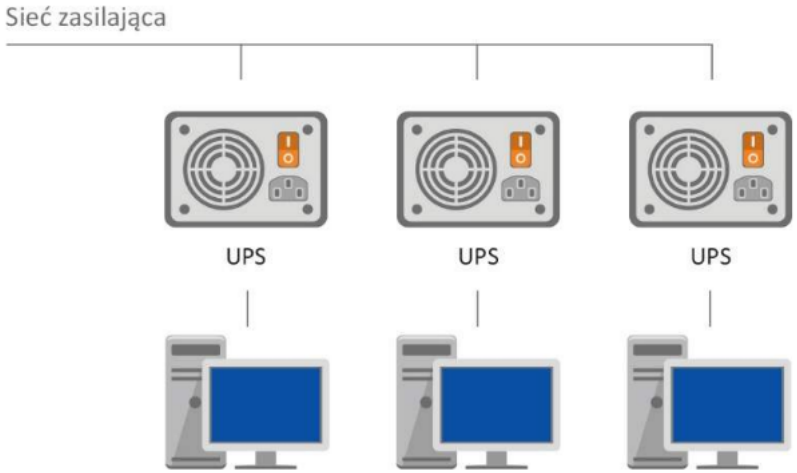
- centralny
- rozproszony

Centralny system

Centralny system zasilania awaryjnego jest rozwiązaniem kosztownym, projektowanym zazwyczaj już na etapie budowy budynku. Wymaga wydzielenia osobnych linii zasila- jących przeznaczonych wyłącznie dla sprzętu informatycznego. UPS zasila całą wydzieloną linię.

Rozproszony system

Rozproszony system zasilania awaryjnego stosowany jest ze względu na niewielkie koszty oraz łatwość wdrożenia. Każdy z UPS-ów zasila pojedyncze urządzenie.



Fizyczna ochrona informacji

Kasowanie danych

Rodzaje metod usuwania danych z nośników:

- skasowanie (deletion) - usunięcie dostępu do danych (skasowanie pliku, sformatowanie dysku); zwykle polega na modyfikacji metadanych (np. tablicy alokacji plików), a same dane pozostają na nośniku i mogą zostać odtworzone

  rm jawny.txt

- zamazanie (clearing) — faktyczne usunięcie danych z nośnika z wykorzystaniem normalnych funkcji urządzenia (np. zapisanie losowych wartości w miejsce usuwanych danych); dane lub ich fragmenty być może nadal mogą być odzyskane za pomocą technik serwisowych lub laboratoryjnych

  shred -vzun0 jawny.txt

- odkażanie (purging lub sanitization) — nieniszczące usunięcie danych z nośnika w sposób gwarantujący niemożność ich odzyskania za pomocą żadnych znanych metod. Dla wielu współczesnych nośników istnieją techniczne przesłanki by sądzić, że ze względu na dużą gęstość zapisu zamazywanie wystarcza do odkażania.
- zniszczenie (physical destruction) — fizyczne zniszczenie nośnika (spalenie, rozdrobnienie, sproszkowanie, zgniecenie itp.) w sposób gwarantujący niemożność odzyskania danych za pomocą żadnych znanych metod

Zniszczenie przykłady

Rodzaje metod usuwania danych z nośników:

- temperatura - wyższa od temperatury Curie, powyżej której ferromagnetyk traci właściwości magnetyczne, stając się paramagnetykiem,
- silne pole magnetyczne - generowane przez urządzenie zwane degausserem,
- fizyczne zniszczenie powierzchni nośnika - mechaniczne lub za pomocą kwasu.