Mechanizmy bezpieczeństwa systemów operacyjnych
oraz
VPN

dr inż. Krzysztof Cabaj

Plan wykładu

- Wstęp – podstawowe mechanizmy bezpieczeństwa systemów operacyjnych
- Kontrola dostępu
- Zaawansowane mechanizmy bezpieczeństwa
- Podsumowanie

Bezpieczeństwo na przykładzie systemu operacyjnego DOS

- System jedno-zadaniowy, jedno-użytkownikowy (ang. single-tasking, single-user)
- Brak jakichkolwiek zabezpieczeń
- Możliwość wykonywania jednego programu (*), który ma pełny dostęp do wszystkich zasobów komputera
- (*) Możliwość pisania prostych programów, TSR (ang. Terminate and Stay Resident) „podczepianych” pod rozmaite przerwania

„Nowoczesne” systemy operacyjne

- Są wielozadaniowe/wieloprocesowe (ang. Multi-tasking) oraz wielodostępne (ang. Multi-user)
- Wymusza to odpowiedni projekt oraz implementację, który musi chronić
  - procesy przed innymi procesami – tak aby jeden proces nie mógł (bez zgody) zmodyfikować danych innego procesu
  - użytkowników między sobą, ich procesy oraz zasoby/dane
  - pewne kluczowe struktury systemu operacyjnego przed użytkownikami/ich procesami
- Przykłady tego typu systemów: Windows NT/200X/7/8, Unix, Linux

„Nowoczesne” systemy operacyjne

- Ochrona w „nowoczesnych” systemach operacyjnych często związana jest ze współpracą oprogramowania z mechanizmami sprzętowymi, między innymi
  - Pierścieniami ochrony procesora
  - Jednostką zarządzania pamięcią (ang. Memory Management Unit)

Pierścienie ochrony

- Model bezpieczeństwa, w którym wprowadzamy odseparowane domeny bezpieczeństwa o różnych prawach, które tworzą hierarchię od domeny o najwyższym uprzywilejowaniu (mogącą wykonać dowolną operację) do domeny o najniższym poziomi uprzywilejowania
- Wykonanie akcji o wyższym poziomie uprzywilejowania wymaga kontaktu między domenami, która podlega i zapewnia odpowiednią ochronę

Pierścienie ochrony

- Mechanizm najczęściej opiera się na mechanizmach sprzętowych, pozwalających wykonywać pewne instrukcje tylko w wybranych pierścieniach
- Najczęściej systemy operacyjne są zaprojektowane w ten sposób, że jądro systemu działa na najbardziej uprzywilejowanym pierścieniu (ang. Ring 0) a aplikacje użytkownika na pierścieniu najmniej uprzywilejowanym (przykładowo dla procesorów rodziny x86, posiadającym 4 pierścienie na pierścieniu nr. 3)
- Wszystkie operacje wymagające komunikacji z urządzeniami są wykonywane za pośrednictwem systemu operacyjnego

Jednostką zarządzania pamięci - Wirtualna przestrzeń adresowa

- Jednostka zarządzania pamięcią dokonuje translacji adresów wykorzystywanych przez aplikację (wirtualnych) na adresy fizyczne
- W razie niemożności dokonania translacji zgłaszany jest odpowiedni wyjątek sprzętowy – pozwala to zapewnić ochronę oraz zrealizować pamięć wirtualną na dysku
- Dzięki temu każdy proces użytkownika widzi ciągły obszar pamięci tylko do jego dyspozycji
- Bez pomocy specjalnych mechanizmów systemu operacyjnego procesy nie mogą zmieniać danych innego procesu

Jednostką zarządzania pamięci – dodatkowe mechanizmy ochrony

- Mapowanie adresu wirtualnego na fizyczny wykonywane jest z pomocą struktury danych – tablicy stron
- Wszelkie manipulacje strukturami MMU wykonywane są przez system operacyjny w uprzywilejowanym pierścieniu bezpieczeństwa
- Dodatkowo z każdą stroną można skojarzyć dodatkowe flagi, przykładowo
  - No execution
  - Read only

Plan wykładu

- Wstęp – podstawowe mechanizmy bezpieczeństwa systemów operacyjnych
- Kontrola dostępu
  - Listy kontroli dostępu
- Zaawansowane mechanizmy bezpieczeństwa
- Podsumowanie

Kontrola dostępu

- Użytkownicy korzystający w sposób interaktywny z komputera podczas procesu logowania są uwierzytelniani
- W dalszych krokach z każdym uruchomionym procesem skojarzony jest zestaw informacji pozwalających określić użytkownika i na ich podstawie zweryfikować jakie akcje może on wykonać
- Dodatkowo współczesne systemy posiadają pewne procesy działające w tle (Unix/Linux – demony, Windows – usługi (ang. Services)), które są uruchamiane podczas startu systemu z prawami określonymi w konfiguracji

Kontrola dostępu

- Kontrola dostępu do obiektu związana jest z prawami, rodzajami operacji jakie dany użytkownik może wykonać
- Najczęściej używane prawa
  - Możliwość czytania danych
  - Możliwość pisania/modyfikowania danych
  - Możliwość uruchomienia

Kontrola dostępu

- Możliwe sposoby realizacje
  - Macierz dostępu
  - Lista kontroli dostępu
  - Lista możliwości (ang. capabilities)

Macierz dostępu

- Macierz w której kolumny oznaczają poszczególne zasoby a wiersze odpowiadają użytkownikom
- W każdej komórce zapisane są przysługujące danej osobie prawa do danego zasobu

Macierz dostępu

- Przykład (z R. Anderson, Inżynieria Bezpieczeństwa)

	System operacyjny	Program księgowy	Dane księgowości	Ślad rewizyjny
Sam	rwx	rwx	rw	r
Alice	x	x	rw	-
Bob	rx	r	r	r

- Główna wada, słaba skalowalność. Przy dużej liczbie użytkowników i zasobów szybko wzrasta wielkość co wpływa na wydajność i możliwość konfiguracji

Lista kontroli dostępu

- Lista kontroli dostępu (ang. Access Control List, ACL)
- Sposób przechowywania fragmentu macierzy kontroli, kolumny w połączeniu z obiektem
- W efekcie każdy obiekt posiada listę określającą, jaki rodzaj praw do danego obiektu ma określony podmiot

ACL – Unix/Linux

- Uproszczona lista kontroli dostępu, gdzie z każdym plikiem skojarzone są trzy wpisy określające prawa dla
  - Właściciela (user)
  - Grupy (group)
  - Pozostałych użytkowników (other)
- Możliwe prawa to
  - Czytanie (r, 4)
  - Pisanie (w, 2)
  - Wykonanie (x, 1)

ACL – Unix/Linux

- Prawa wyświetlane są jako trzy literowe grupy odpowiednio dla właściciela, grupy i reszty użytkowników, znak ‚-’ oznacza brak danego prawa
- Prawa można sprawdzić np. za pomocą programu ls z opcją -l
- Przykład

```
kcabaj@debian~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 1353 2012-03-31 11:47 /etc/passwd
kcabaj@debian:~$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 34052 2009-12-06 06:20
/usr/bin/passwd
```

ACL – Unix/Linux

- Modyfikacja praw możliwa jest za pomocą narzędzia *chmod <prawa> <pliki….>*
- Praw można zmienić wybiórczo podają wyrażenia <u/g/o> +/- prawo
- Albo za jednym razem podając dodane w postaci liczby ósemkowej
- Przykład

```
kcabaj@debian:~$ chmod 777 test.txt
kcabaj@debian:~$ chmod g-w test.txt
kcabaj@debian:~$ chmod o-rwx test.txt
kcabaj@debian:~$ ls -l test.txt
-rwxr-x--- 1 root root 0 2014-01-22 10:38 test.txt
```

ACL - Windows

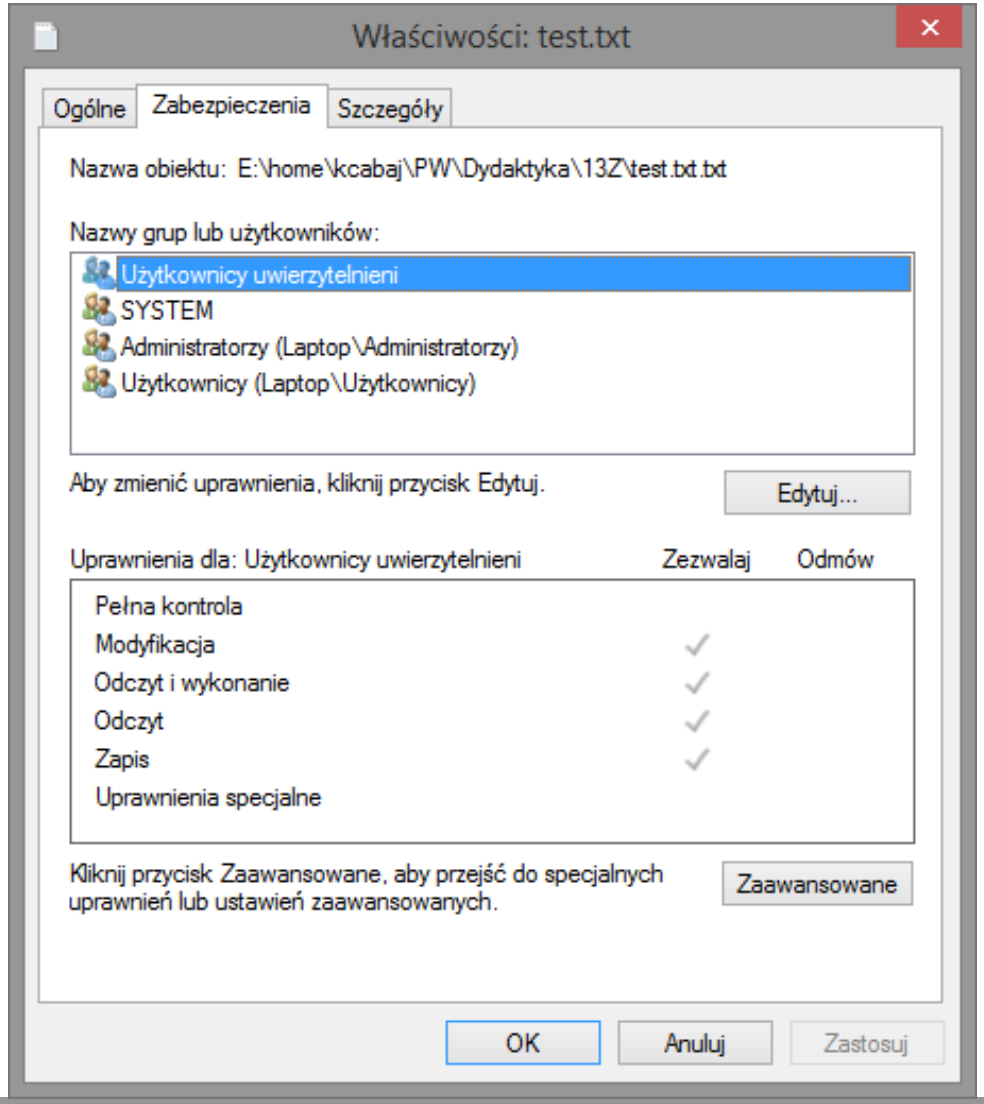
- Z obiektem (nie tylko plik, ale np. klucz rejestru, obiekt w Active Directory) związana jest lista kontroli dostępu (DACL), składająca się z dowolnej liczby wpisów (ang. Access Control Entry) które zezwalają lub zabraniają prawa do wykonania danej akcji dla danego użytkownika, lub grupy użytkowników
- W systemie Windows istnieje 13 różnych rodzajów praw
- Dodatkowo istnieje możliwość skonfigurowania listy SACL (system ACL), która służy do konfigurowanie jakie akcje mają podlegać audytowi – być logowane

ACL - Windows

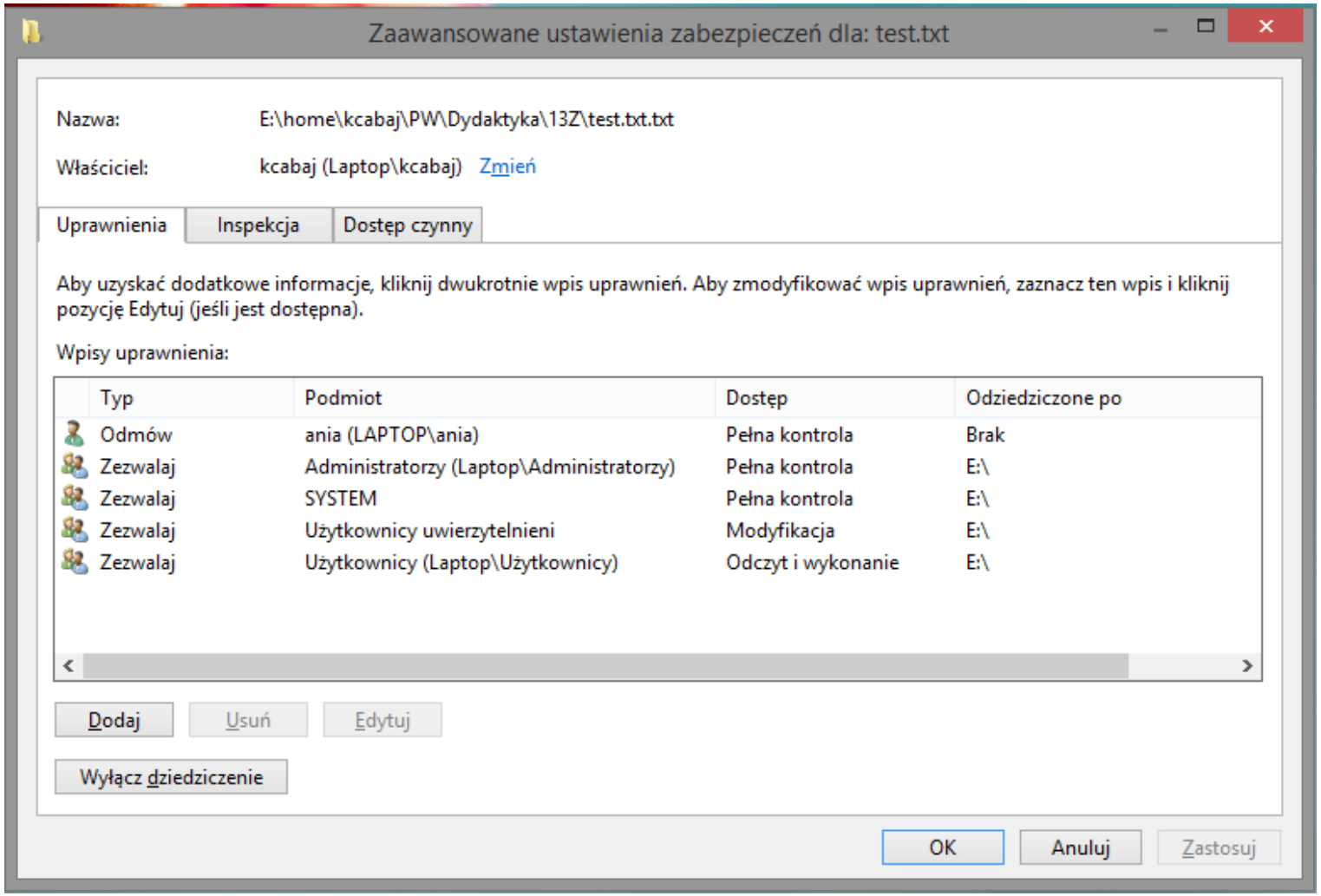
Na menu kontekstowym obiektu

-> Właściwości

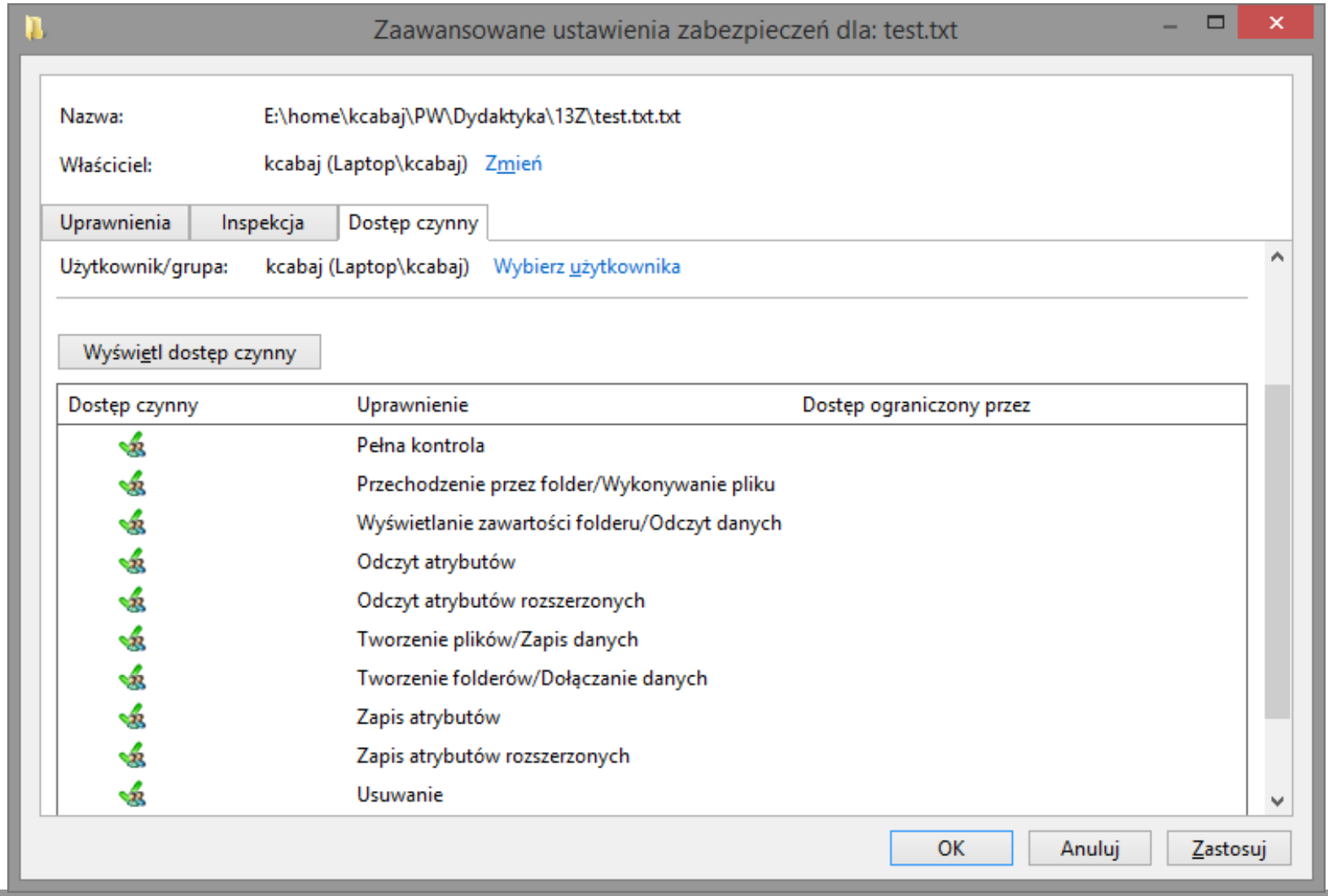
-> Zabezpieczenia



ACL - Windows


Zaawansowane ustawienia zabezpieczeń dla: test.txt
Nazwa: E:\home\kcabaj\PW\Dydaktyka\13Z\test.txt.txt
Właściciel: kcabaj (Laptop\kcabaj) Zmień
Uprawnienia
Inspekcja
Dostęp czynny
Aby uzyskać dodatkowe informacje, kliknij dwukrotnie wpis uprawnień. Aby zmodyfikować wpis uprawnień, zaznacz ten wpis i kliknij pozycję Edytuj (jeśli jest dostępna).
Wpisy uprawnienia:
Typ
Podmiot
Dostęp
Odziedziczone po
Odmów
ania (LAPTOP\ania)
Pełna kontrola
Brak
Zezwalaj
Administratorzy (Laptop\Administratorzy)
Pełna kontrola
E:\
Zezwalaj
SYSTEM
Pełna kontrola
E:\
Zezwalaj
Użytkownicy uwierzytelnieni
Modyfikacja
E:\
Zezwalaj
Użytkownicy (Laptop\Użytkownicy)
Odczyt i wykonanie
E:\
Dodaj
Usuń
Edytuj
Wyłącz dziedziczenie
OK
Anuluj
Zastosuj

ACL - Windows


Zaawansowane ustawienia zabezpieczeń dla: test.txt
Nazwa: E:\home\kcabaj\PW\Dydaktyka\13Z\test.txt.txt
Właściciel: kcabaj (Laptop\kcabaj) Zmień
Uprawnienia
Inspekcja
Dostęp czynny
Użytkownik/grupa: kcabaj (Laptop\kcabaj) Wybierz użytkownika
Wyświetl dostęp czynny
Dostęp czynny
Uprawnienie
Dostęp ograniczony przez
Pełna kontrola
Przechodzenie przez folder/Wykonywanie pliku
Wyświetlanie zawartości folderu/Odczyt danych
Odczyt atrybutów
Odczyt atrybutów rozszerzonych
Tworzenie plików/Zapis danych
Tworzenie folderów/Dołączanie danych
Zapis atrybutów
Zapis atrybutów rozszerzonych
Usuwanie
OK
Anuluj
Zastosuj

Rodzaje List kontroli dostępu

- Rodzaje list kontroli dostępu
  - DACL
  - MAC
  - RBAC

DACL

- Nieobowiązkowa lista ACL, uznaniowa ACL (ang. Discretionary Access Control, DAC)
- To użytkownik sam decyduje jakie prawa, komu nadaje
- Może to prowadzić do nieumyślnego lub celowego ujawnienia pewnych informacji osobą niepowołanym
- Wcześniej omawiane mechanizmy z systemów Unix/Linux oraz Windows są tego rodzaju

MAC

- Obowiązkowa lista ACL (ang. Mandatory Access Control List)
- Prawa dostępu są ustalane przez dedykowany podmiot, a użytkownik nie może ich zmienić
- Implementacja w systemie Linux to SELinux lub SMACK, wprowadzona w systemach Windows od wersji Vista i Server 2008 jako mechanizm Mandatory Integrity Control

RBAC

- Dostęp oparty o role (ang. Role Based Access Control)
- Analiza większości instytucji pokazuje, że większość użytkowników można zaklasyfikować do kilkunastu-kilkudziesięciu grup
- W tym modelu prawa przypisuje się do grup/ról i niezależnie grupy/role odpowiednim użytkownikom

Plan wykładu

- Wstęp – podstawowe mechanizmy bezpieczeństwa systemów operacyjnych
- Kontrola dostępu
- Zaawansowane mechanizmy bezpieczeństwa
- Podsumowanie

Set uid bit

- Ustawienie tego bitu pozwala na uruchomienie programu z prawami właściciela (lub grupy)
- W ten sposób działa przykładowo program passwd służący do zmiany hasła w systemach Unix/Linux
- Należy uważać aby plik nie miał prawa „w” co umożliwia podmianę programu pozostawiając bit suid

```
kcabaj@debian:~$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 34052 2009-12-06 06:20
/usr/bin/passwd
```

Mechanizm sudo

- Administratorem w systemie Unix/Linux jest użytkownik o identyfikatorze (ang. User ID, UID) o wartości 0
- Można stworzyć kilku użytkowników o tym samym UID
- Lepszym sposobem jest wykorzystanie mechanizmu sudo, który pozwala uprawnionym użytkownikom wykonać programy z uprawnieniami administratora
- Konfiguracja użytkowników uprzywilejowanych do wykorzystania sudo znajduje się w pliku /etc/sudoers

Chroot

- Mechanizm bezpieczeństwa wprowadzony pod koniec lat 70 pozwalający podmienić katalog główny na inny katalog, i w ten sposób uniemożliwić w razie wystąpienia błędu lub ataku dostęp do rzeczywistego systemu plików

- Aktualnie zastępowany dedykowanymi rozwiązaniami typu sandbox lub wirtualizacją

Ochrona plików systemu Windows

- Ochrona plików systemu Windows (ang. Windows File Protection)
- Mechanizm nasłuchuje na zdarzenie związane ze zmianami plików w chronionych katalogach
- W momencie wykrycia zmiany dotyczącej chronionego pliku zostaje on zastąpiony „poprawną kopią”, przechowywaną domyślnie w katalogu %systemroot%\system32\dllcache
- Od systemu Windows Vista mechanizm został zastąpiony przez Windows Resource Protection

Plan wykładu

- Wstęp – podstawowe mechanizmy bezpieczeństwa systemów operacyjnych
- Kontrola dostępu
- Zaawansowane mechanizmy bezpieczeństwa
- Podsumowanie
  - Zasada najmniejszych uprawnień
  - Zasada rozdzielenia obowiązków
  - Rzeczywistość

Zasada najmniejszych uprawnień

- Zasada najmniejszych uprawnień (ang. principle of least privilege, principle of minimal privilege, the principle of least authority) zakładająca, że każdy podmiot (użytkownik, proces) posiada minimalny zestaw uprawnień pozwalający wykonywać powierzone obowiązki/zadania

Zasada rozdzielenia obowiązków

- Ważne operacje wymagają współpracy co najmniej dwóch osób
- Przykład wykonane przelewu na dużą kwotę wymaga uzyskania akceptacji drugiego pracownika – czasem nawet kierownika

Rzeczywistość

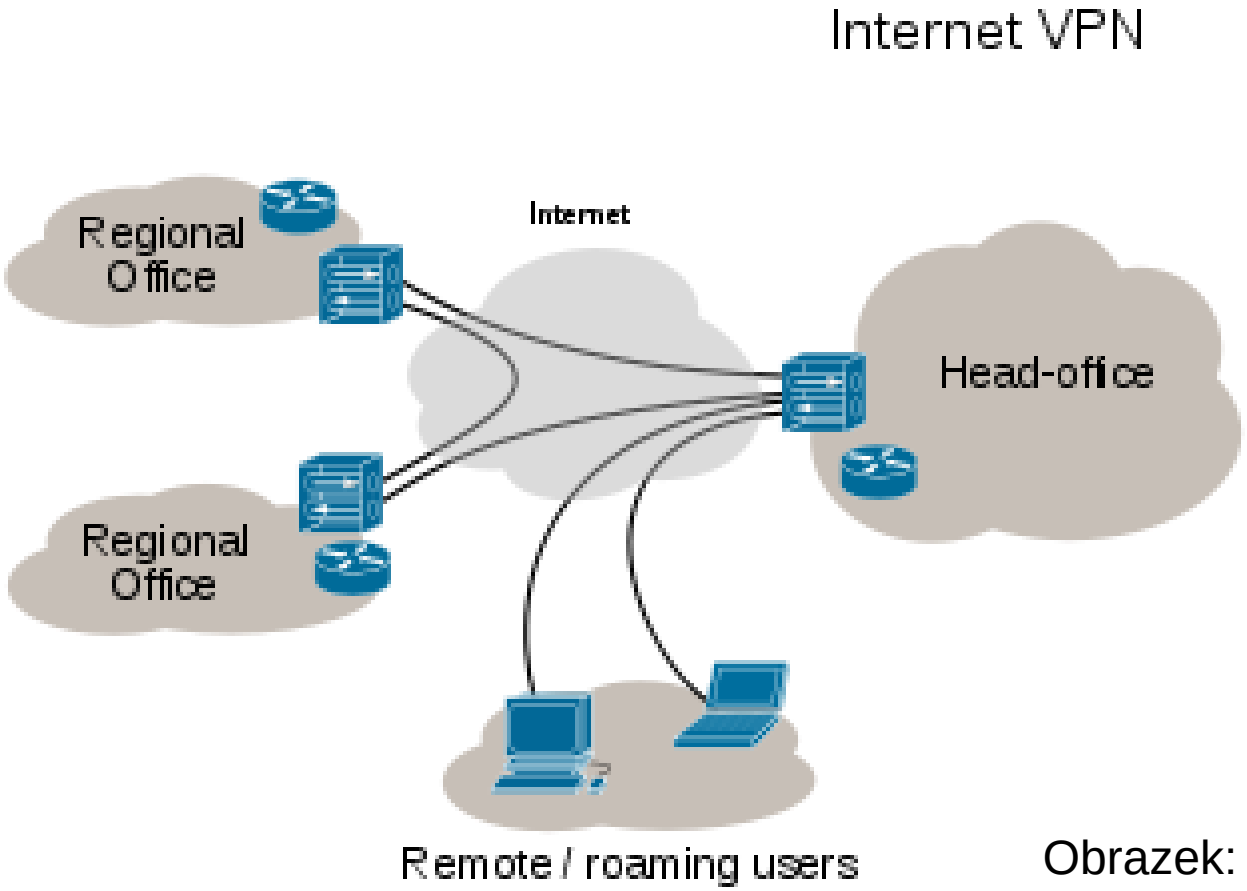
- Niestety obserwowana jest tendencja do pracy programów z wyższymi prawami niż potrzeba
- Mimo wielu mechanizmów dużo aplikacji wymaga działania z uprawnieniami administratora mimo, że potrzebują tego tylko do wykonywania znikomej części swojej pracy

VPN

dr inż. Krzysztof Cabaj

Wprowadzenie

- VPN (ang. Virtual Private Network)



Obrazek: Wiki

Protokoły VPN

- GRE (ang. Generic Routing Encapsulation)
- PPTP (ang. Point-to-point Tunneling Protocol)
- IPSec

IPSec

- IPSec to „framework” umożliwiający wybór dostępnych mechanizmów aby zabezpieczyć komunikację użytkowników
- Protokoły
  - AH (ang. Authentication Header)
  - ESP (ang. Encapsulated Security Payload)
  - IKE/ISAKMP

Protokół AH

- AH (ang. Authentication Header), protokół IP numer 51
- Zapewnia integralność pakietów oraz autentyczność źródła
- Zabezpiecza dane wraz z nagłówkiem (bez zmieniających się pól ToS, TTL, flag, offset fragmentu i sumy kontrolnej)
- Problemy jeśli na trasie jest zastosowany NAT lub urządzenia modyfikujące nagłówki

Protokół ESP

- ESP (ang. Encapsulated Security Payload), protokół IP numer 50
- Zapewnie poufność – chroni jedynie zawartość pakietu, bez nagłówków

Asocjacja bezpieczeństwa 1/2

- Asocjacja bezpieczeństwa (ang. Security Association, SA) byt w pamięci urządzenia sieciowego przechowujący wszystkie istotne informacje dotyczące zabezpieczanego połączenia, takie jak:
  - Wynegocjowany algorytm
  - Wektory inicjalizacyjne
  - Klucze sesyjne
  - Numery sekwencyjne
  - Identyfikację ruchu do zabezpieczenia

Asocjacja bezpieczeństwa 2/2

- SA przechowywane w SADB i identyfikowane poprzez numer SPI (ang. Security Parameter Index) umieszczany w nagłówkach protokołów AH i ESP
- Jedno SA dotyczy jednego protokołu (AH lub ESP) i jednego kierunku, czyli dla połączenia zabezpieczonego AH i ESP na każdym urządzeniu będą znajdowały się cztery Asocjacje Bezpieczeństwa

Protokół IKE/ISAKMP

- IKE (ang. Internet Key Exchange) wykorzystuje protokoł ISAKMP (ang. Internet Security Association and Key Management Protocol), UDP port 500
- Służy do zestawienia tunelu IPSec, wynegocjowania wspólnych parametrów oraz wypełnienie danymi struktur SA

Topologie

- Site-to-Site – topologia wykorzystywana do podłączeniu wielu użytkowników (np. biuro lokalne do głównej siedziby organizacji), w Internecie widać komunikację między dwoma urządzeniami dostępowymi (rutery, zapory ogniowe, koncentratory VPN)
- Remote Access – tryb wykorzystywany do podłączenia pojedynczego użytkownika, realizowane najczęściej w dodatkowym oprogramowaniu

Tryby Pracy IPSec

- Tryby pracy
  - Tunelowy (najczęściej używany w topologii site-to-site), cały pakiet użytkownika wraz z nagłówkami IPSec jest umieszczany w nowym pakiecie IP

  - Transportowy (najczęściej używany w topologii remote-access, pomiędzy nagłówek a dane użytkownika umieszczane są nagłówki IPSec

Uwierzytelnienie

- Aktualnie są używane dwa sposoby uwierzytelniania stron
  - Współdzielony sekret (ang. pre-shared secret/key)
  - Certyfikaty - wykorzystanie PKI

Działanie 1/2

- Klient wysyła tak zwany interesujący ruch sieciowy – taki, który powinien być zabezpieczony
- Urządzenie terminujące lub aplikacja na komputerze dla połączenia remote access sprawdza czy jest aktywny tunel IPSec
- Jeśli tunel IPSec nie jest aktywny rozpoczyna się proces negocjacji protokołem IKE, który tworzy własny zabezpieczony tunel zarządzania (a także własne SA)

Działanie 2/2

- Wykorzystując zabezpieczony tunel następuje negocjacja parametrów właściwego tunelu IPSec
- Po zestawieniu tunelu IPSec jest on wykorzystywany do przesyłania ruchu użytkownika