rocławska

Politechnika Wrocławska

Bazy Danych

dr inż. Roman Ptak
Katedra Informatyki Technicznej
roman.ptak@pwr.edu.pl

Plan wykładu 3.

- Modelowanie obiektowe (UML)
- Narzędzia CASE
- Bezpieczeństwo
  - Ochrona danych przed utratą
  - Ochrona przed niepowołanym dostępem

Modelowanie obiektowe

JĘZYK UML

Obiektowy model danych

- Język modelowania UML
- Mapowanie obiektowo-relacyjne (ORM)

ORACLE

HIBERNATE

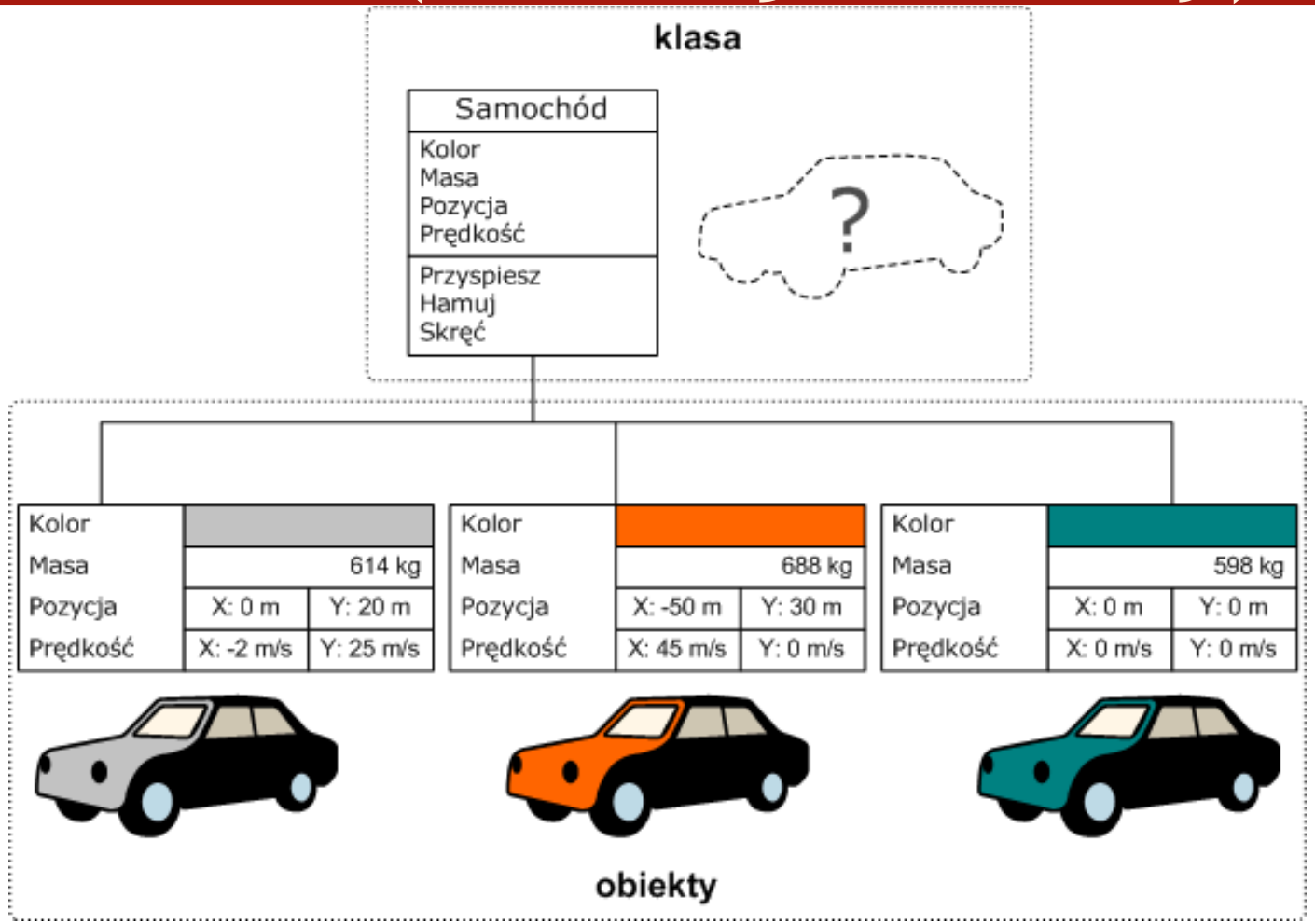
Modelowanie obiektowe

- Modelowanie systemów informacyjnych z wykorzystaniem podejścia **obiektowego** i języka **UML**.
- Zastosowania języka UML w różnych obszarach, od projektowania systemów czasu rzeczywistego poprzez projektowanie baz danych aż po modelowanie systemów biznesowych.

Klasa a obiekt klasy

- Klasa
  - opis zbioru obiektów, które mają takie same **atrybuty**, **operacje**, **związki** i znaczenie
  - częściowa lub całkowita definicja dla obiektów
  - zbiór wszystkich obiektów mających wspólną strukturę i zachowanie
- Obiekt
  - konkretne wystąpienie abstrakcji
  - byt o dobrze określonych granicach i tożsamości
  - obejmuje stan i zachowanie
  - egzemplarz klasy

Definicja klasy wraz z kilkoma obiektami (instancjami klasy)



Źródło: http://www.egrafik.pl/kurs-c-plus-plus/6.1.php

UML

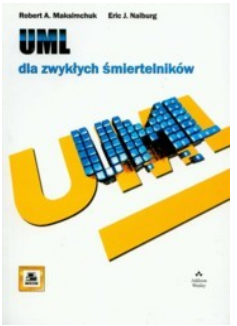
- UML (ang. *Unified Modeling Language)* - Ujednolicony Język Modelowania
- Najnowsza wersja: 2.5.1

UML

- Graficzny język do obrazowania, specyfikowania, tworzenia i dokumentowania elementów systemów informatycznych.
- Diagramy UML to schematy przedstawiające zbiór bytów i związków między nimi.

Literatura (wybór)

- G. Booch, J. Rumbaugh, I. Jacobson, *UML przewodnik użytkownika*, WN-T, Warszawa 2002.
- R. A. Maksimchuk, E. J. Naiburg, *UML dla zwykłych śmiertelników*, Warszawa 2007.
- http://www.uml.org/
- http://www.omg.org/spec/UML/



Historia UML

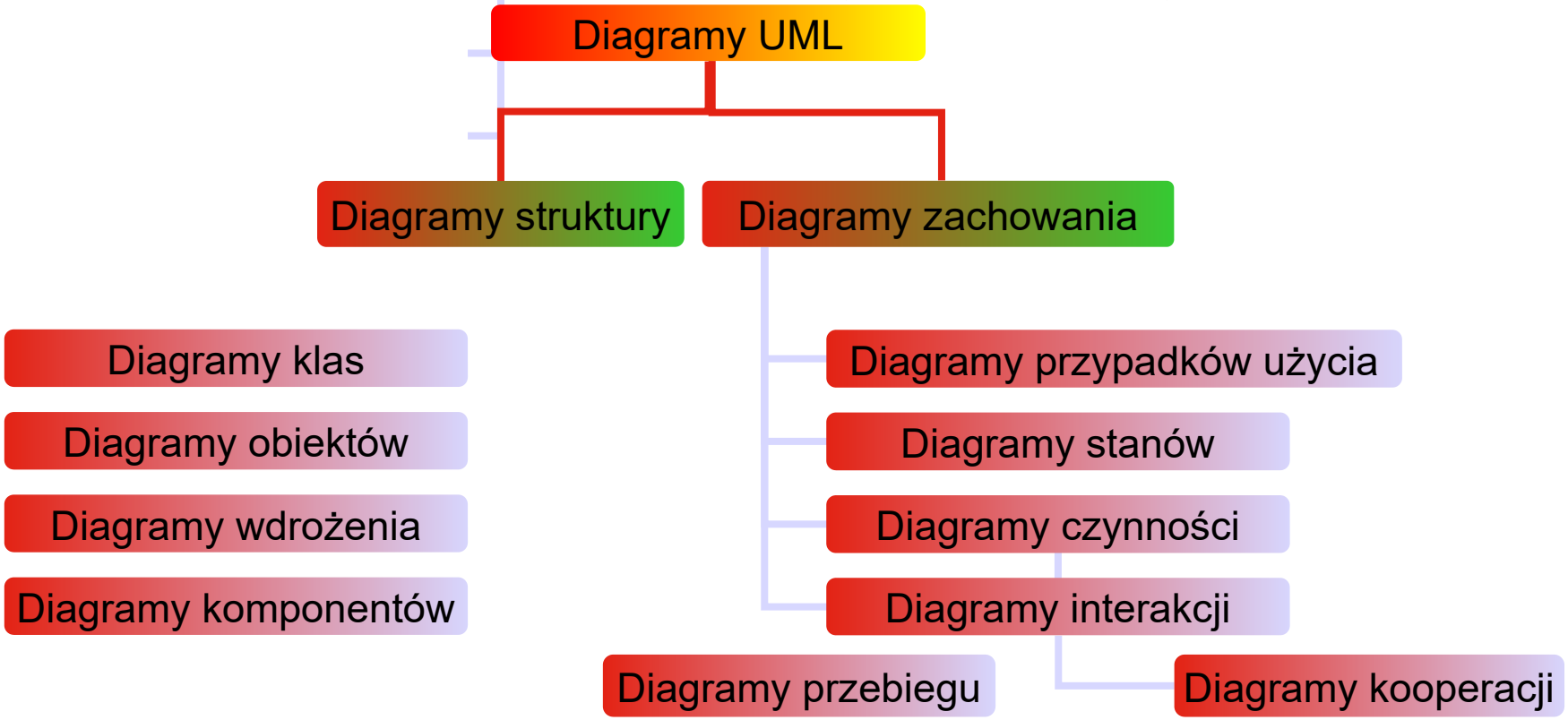
- Modelowanie obiektowe w latach 70. i 80.
- 1996 r. – dokumentacja wersji 0.9
- 1997 r. – UML 1.0 w gestii Object Management Group (OMG)
- Wersje: 1.1, 1.2, 1.3, 1.4, 1.4.2 (ta została poddana standaryzacji ISO/IEC 19501), 1.5, 2.1.1, 2.1.2, 2.4.1 (ISO/IEC 19505-1 i 19505-2)
- 2017 r. – najnowsza wersja: 2.5.1

Zastosowania UML:

- tworzenie systemów informacyjnych przedsiębiorstw,
- usługi bankowe i finansowe,
- przemysł obronnym i lotniczy,
- rozproszone usługi internetowe,
- telekomunikacja,
- transport,
- sprzedaż detaliczna,
- elektronika w medycynie,
- nauka itd.

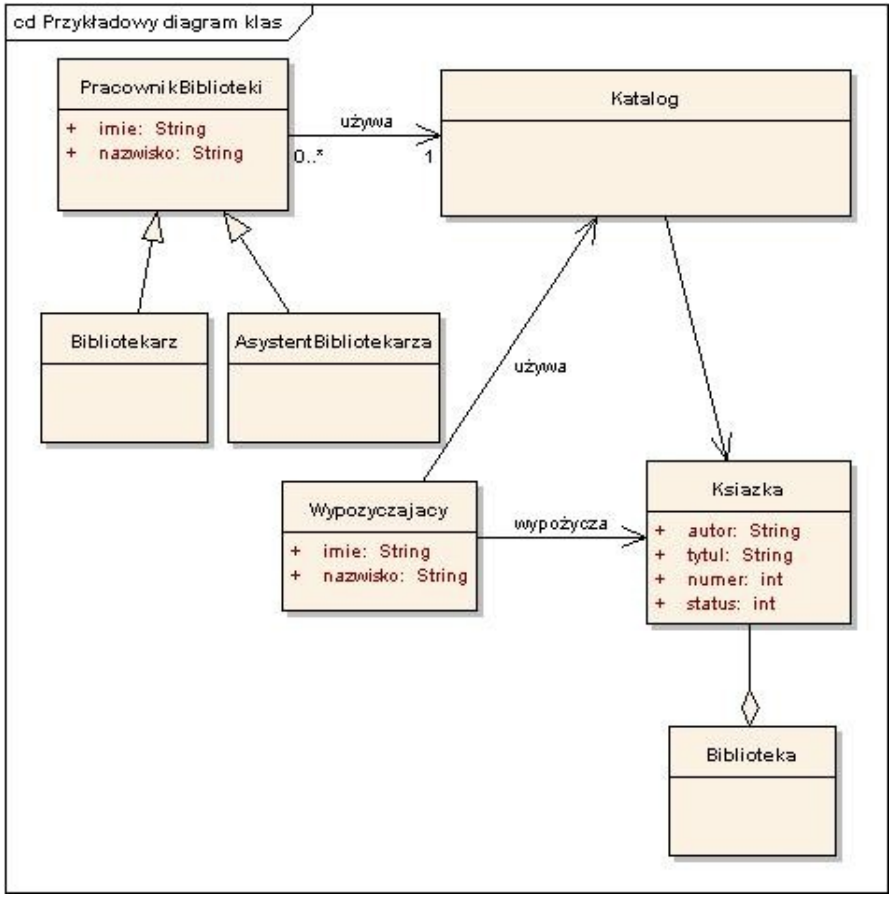
Diagramy UML

- Diagramy struktury
- Diagramy zachowania (dynamiki)



Diagramy struktury UML

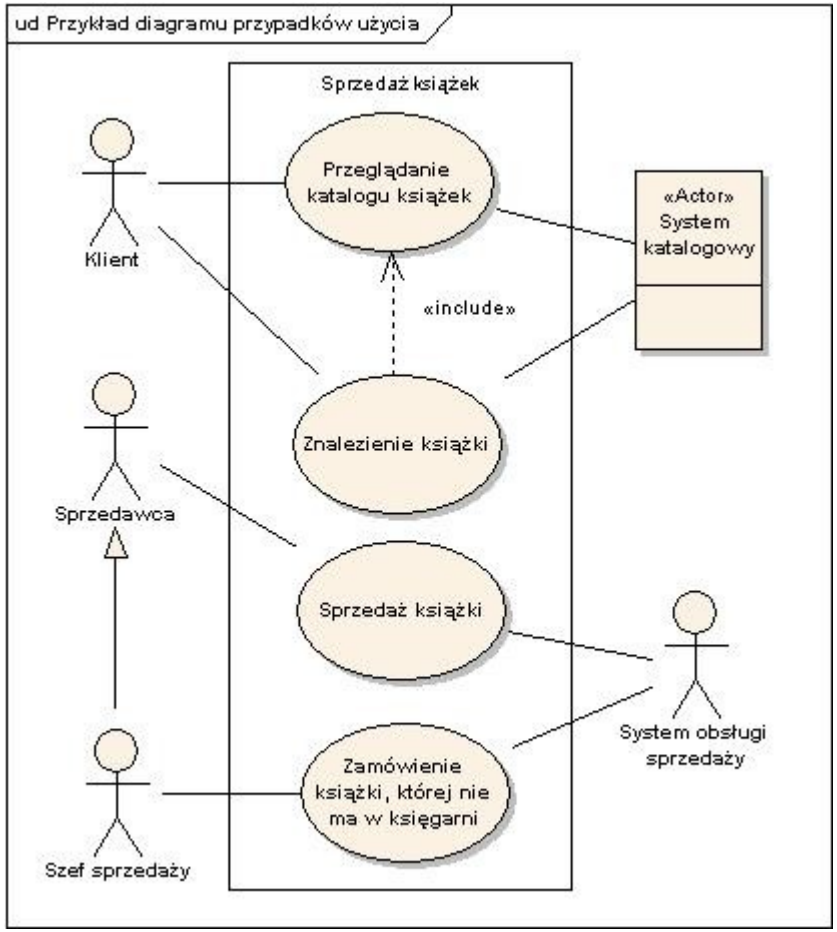
- **Klas**
- Obiektów
- Wdrożeniowy
  - Komponentów
  - Rozlokowania
- Pakietów
- Struktur połączonych



źródło: http://www.erudis.pl/pl/node/93

Diagramy dynamiki UML

- **Przypadków użycia**
- Czynności
- Interakcji
  - Sekwencji
  - Komunikacji
  - Harmonogramowania
  - Sterowania interakcją
- Maszyny stanowej



źródło: http://www.erudis.pl/pl/node/93

Zastosowania w projektowaniu systemów informatycznych

- Projektując system informatyczny, rozpoczyna się przeważnie od tworzenia diagramów w następującej kolejności:
  1. Przypadków użycia,
  2. Klas,
  3. Czynności,
  4. Sekwencji.
- Są to najczęściej wykorzystywane diagramy. Pozostałe z nich bywają pomijane, zwłaszcza przy budowaniu niedużych systemów informatycznych.

ang. *Use Case Diagrams*; DPU

DIAGRAM PRZYPADKÓW UŻYCIA

Definicja DPU

- Diagramy służące do modelowania zachowania systemu.
- Opisują co system powinien robić z punktu widzenia obserwatora z zewnątrz.
- Przedstawiają scenariusze realizacji określonych zachowań (funkcji systemu).

DPU - zawartość

- **przypadki użycia** (ang. *use case*) - opisy zdarzeń,
- **aktorzy** - osoby/rzeczy inicjujące zdarzenia,
- powiązania między aktorami i przypadkami użycia,
- zależności, uogólnienia i powiązania między przypadkami użycia,
- pakiety, notatki i ograniczenia.

Aktor

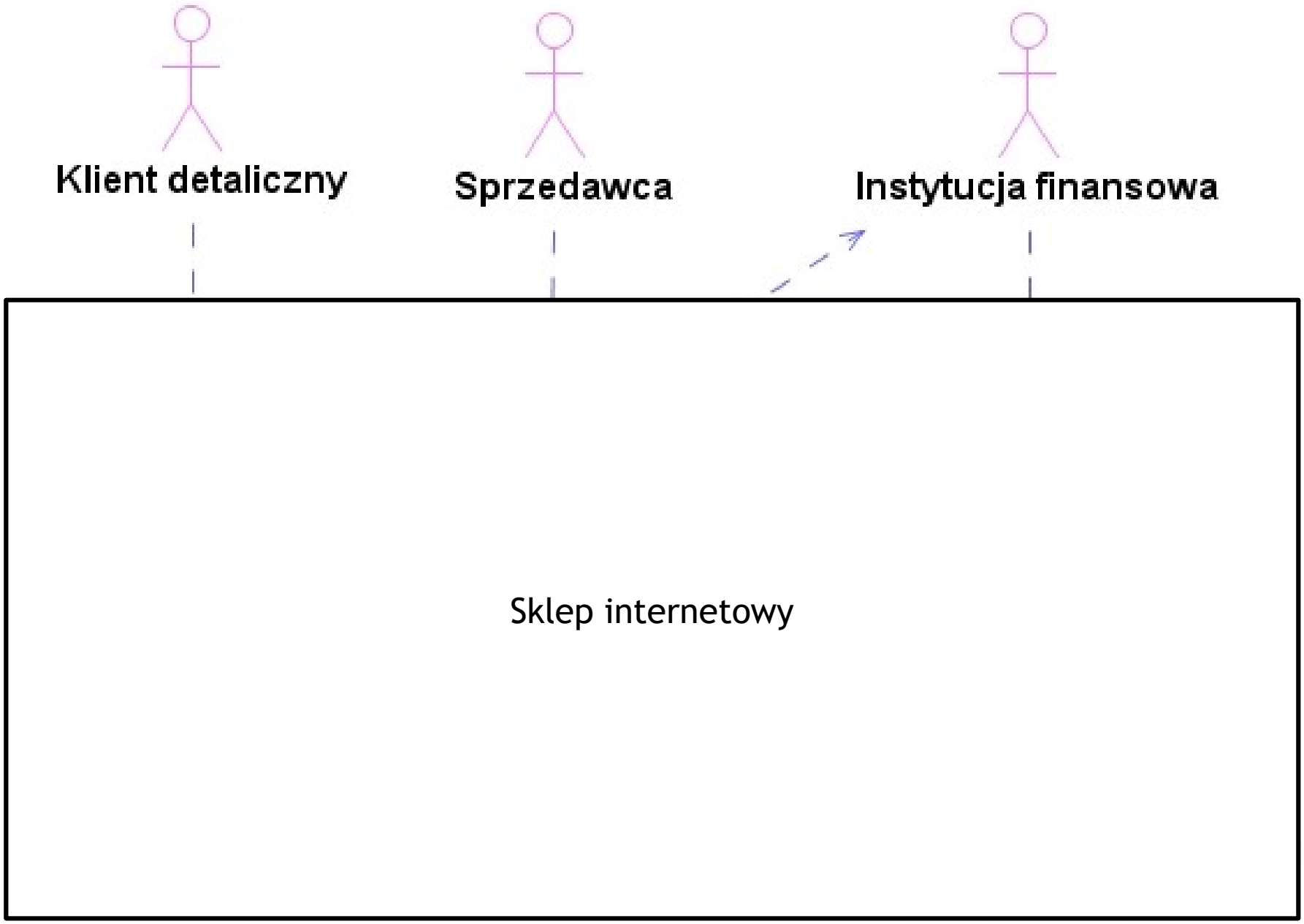
- Aktor – ktoś lub coś co wchodzi w interakcję z systemem: osoba identyfikowana przez rolę, system, urządzenie lub organizacja.
- **Aktor główny** inicjujący interakcję chce osiągnąć określony cel.
- **Aktor pomocniczy** dostarcza systemowi informacji lub usług niezbędnych do realizacji przypadku użycia.

Przypadek użycia

- Opisuje zachowanie systemu podczas interakcji z aktorem
- W zależności od szeregu warunków interakcja może potoczyć się w różny sposób, mogą wydarzyć się różne scenariusze.
- Przypadek użycia jest zbiorem możliwych scenariuszy.

DPU - zastosowania

- modelowanie zachowania bytów - opis ciągu akcji zmierzających do realizacji danej funkcji systemu,
- modelowanie otoczenia systemu - definiowanie aktorów i ich ról,
- modelowanie wymagań stawianych systemowi – określenie co system powinien robić,
- testowanie systemu.


Klient detaliczny
Sprzedawca
Instytucja finansowa
Sklep internetowy

DIAGRAMY KLAS

Diagramy klas (ang. *Class Diagrams*)

- Definicja:

  Schemat przedstawiający zbiór klas, interfejsów, kooperacji oraz związki między nimi.

➔Używa się ich do modelowania struktury systemu.

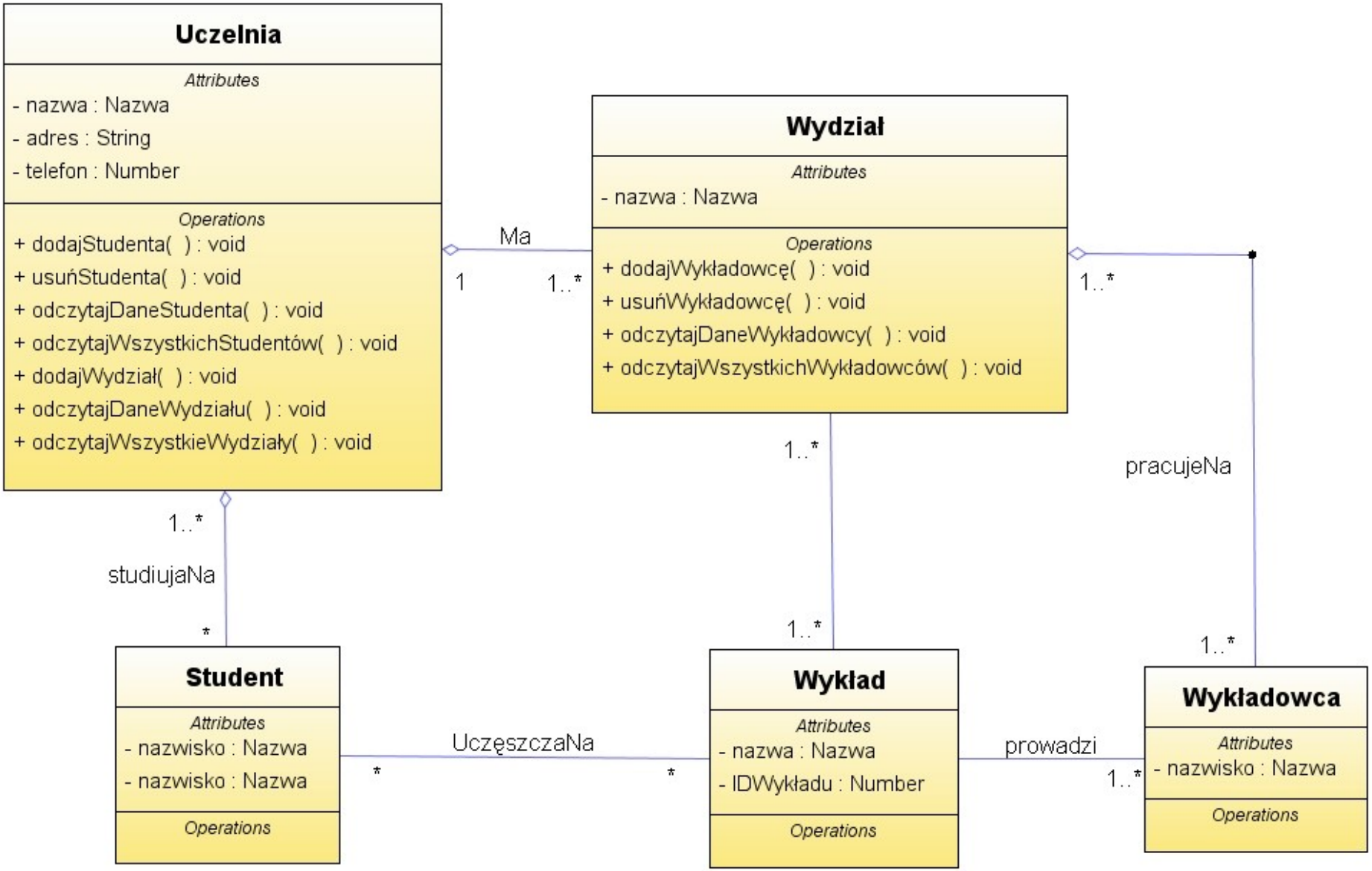
➔Stanowią bazę wyjściową dla diagramów komponentów i diagramów wdrożenia.

➔Szczególnie przydatne do tworzenia systemów (inżynieria do przodu i wstecz).

Diagramy klas (ang. *Class Diagrams*)

- Zawartość:
  - klasy,
  - interfejsy,
  - kooperacje,
  - zależności, uogólnienia, powiązania,
  - notatki, ograniczenia, pakiety, podsystemy.
- Zastosowania:
  - modelowanie słownictwa systemu (struktura systemu),
  - modelowanie prostych kooperacji,
  - modelowanie schematu logicznej bazy danych.

Przykład: Diagram klas



Rodzaje widoczności

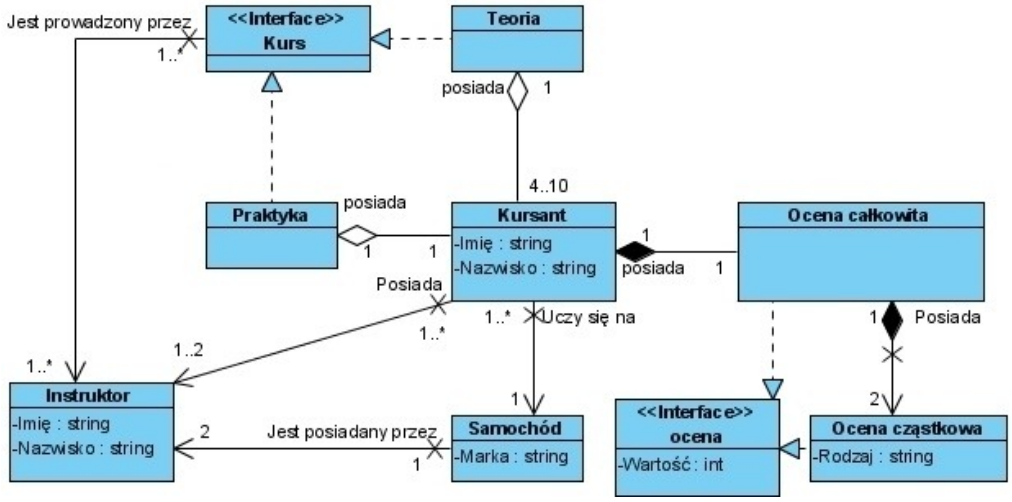
Widoczność atrybutu	Symbol	Znaczenie
Prywatny (*private*)	-	Tylko klasa zawierająca atrybut ma do niego dostęp
Chroniony (*protected*)	#	Dostęp do atrybutu mają również klasy potomne
Publiczny (*public*)	+	Wszystkie klasy mają dostęp do atrybutu
Pakiet (*package*)	~	Wszystkie klasy z danego pakietu mają dostęp do atrybutu

Związki między klasami

źródło: http://brasil.cel.agh.edu.pl/~09sbfraczek/diagram-klas,1,11.html

Liczebność asocjacji w UML

- 0..* - zero lub więcej (opcjonalność, wiele)
- 0..1 – zero lub jeden (opcjonalność, jeden)
- 1..* - co najmniej jeden (obligatoryjność, wiele)
- * - zero lub więcej (opcjonalność, wiele)
- 2..6 – co najmniej 2, co najwyżej 6
- 1, 5-7 – jeden, pięć, cześć lub siedem
- brak – 1..1 (obligatoryjność, jeden)



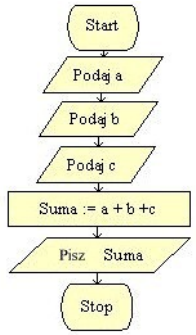
INNE DIAGRAMY

Diagramy czynności (ang. *Activity Diagrams*)

- Definicja:

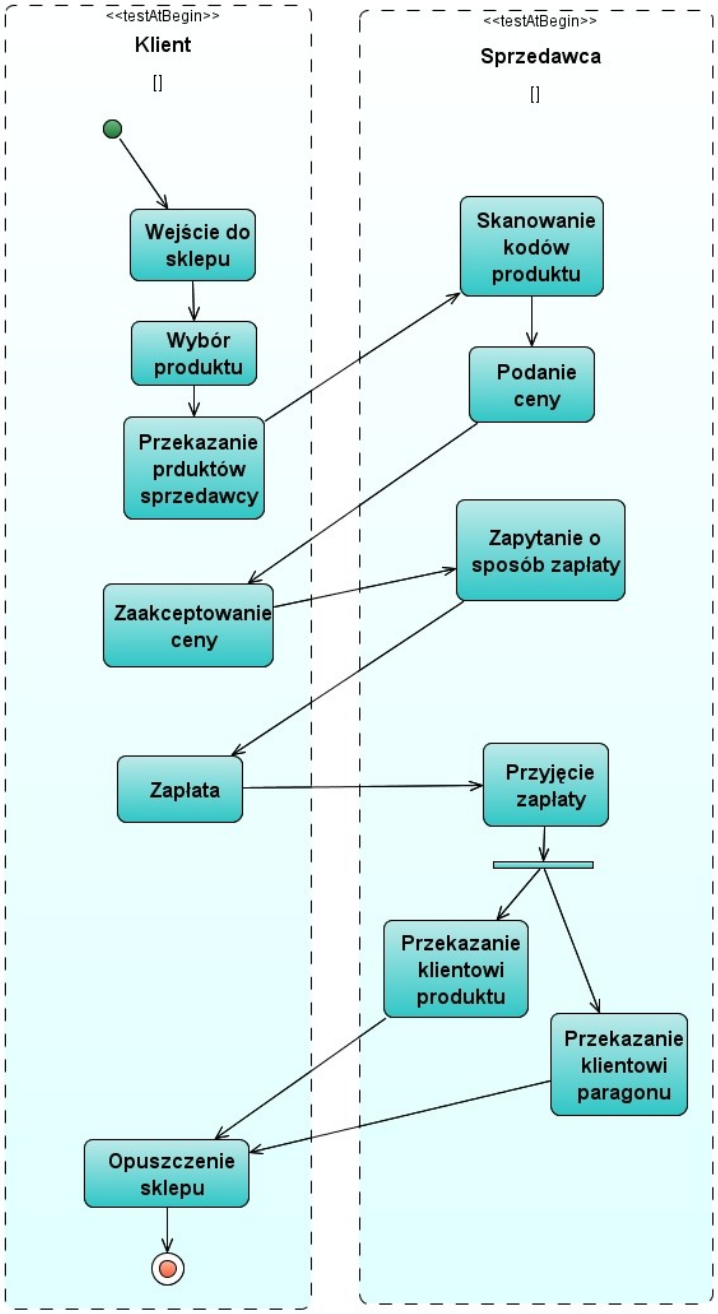
  Diagramy czynności przedstawiają przepływ sterowania od czynności do czynności. Większość diagramów czynności przedstawia kroki procesu obliczeniowego.

➔ Schematy blokowe



Diagramy czynności (ang. *Activity Diagrams*)

- Zawartość:
  - stany akcji i stany czynności,
  - przejścia,
  - obiekty,
  - notatki i ograniczenia.
- Zastosowania:
  - modelowanie przepływu czynności
  - modelowanie operacji


<<testAtBegin>>
Klient
[]
Wejście do sklepu
Wybór produktu
Przekazanie prduktów sprzedawcy
Zaakceptowanie ceny
Zapłata
Przekazanie klientowi produktu
Opuszczenie sklepu
<<testAtBegin>>
Sprzedawca
[]
Skanowanie kodów produktu
Podanie ceny
Zapytanie o sposób zapłaty
Przyjęcie zapłaty
Przekazanie klientowi paragonu

Diagramy interakcji

- Definicja:
  Diagramy interakcji (ang. *Interaction Diagrams*) służą do modelowania zachowania systemu. Ilustrują kiedy i w jaki sposób komunikaty przesyłane są pomiędzy obiektami.

➔Diagramy przebiegu (ang. *Sequence Diagrams*)
➔Diagramy kooperacji (ang. *Collaboration Diagrams*)

Diagramy interakcji

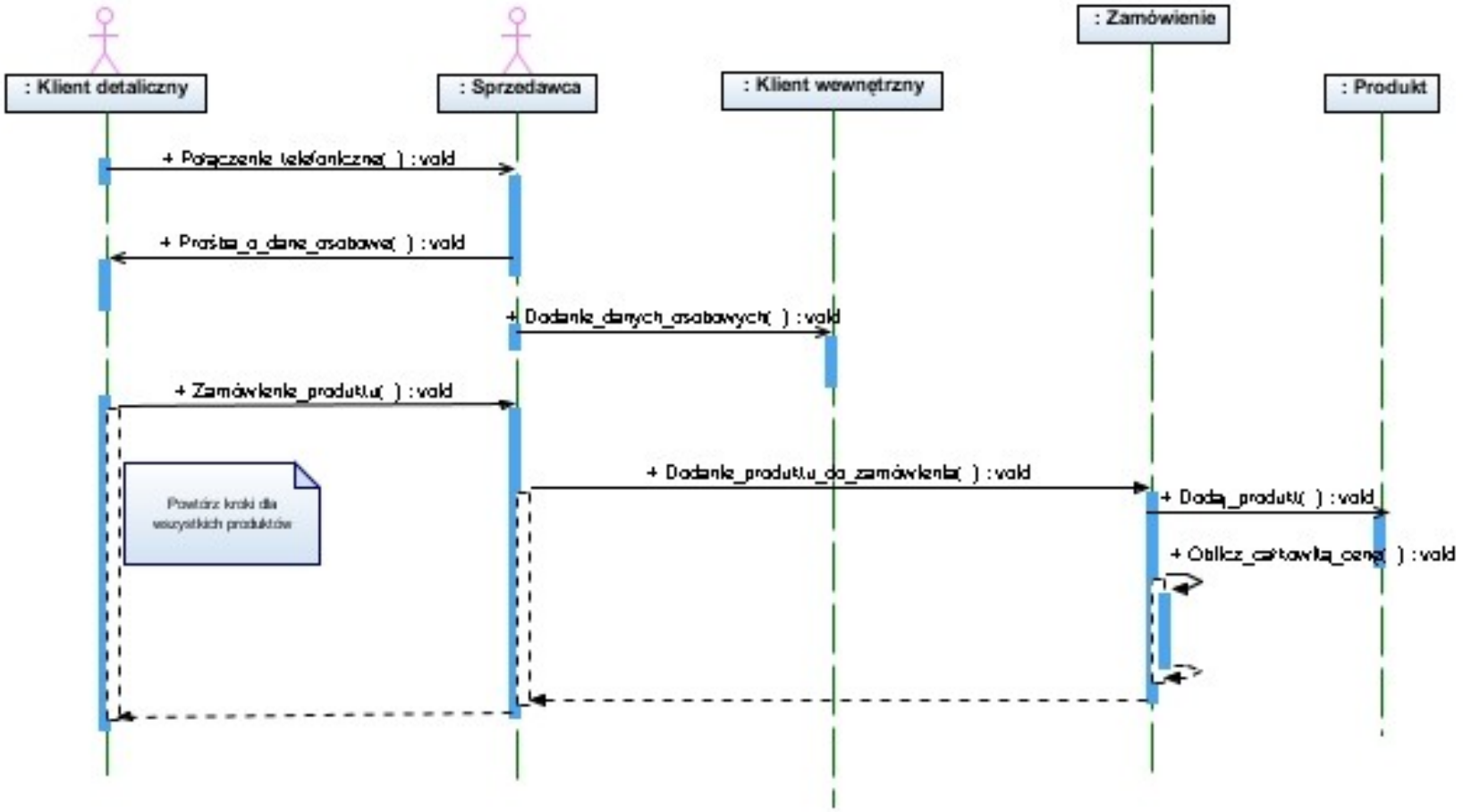
Na **diagramie przebiegu** uwypukla się kolejność wysyłania komunikatów w czasie.

Na **diagramie kooperacji** kładzie się nacisk na związki strukturalne między obiektami wysyłającymi i odbierającymi komunikaty.

Diagramy interakcji

- Zawartość:
  - obiekty,
  - wiązania,
  - komunikaty,
  - notatki i ograniczenia.
- Zastosowania:
  - modelowanie przepływu sterowania z uwzględnieniem kolejności
  - komunikatów w czasie,
  - modelowanie przepływu sterowania z uwzględnieniem organizacji strukturalnej obiektów

Przykład: Diagram interakcji (sekwencji)



Inne elementy

- Język OCL (ang. *Object Constraint Language*)
  - Język zapisu ograniczeń w modelu obiektowym;
  - Jest on częścią języka UML.
- OCL pozwala uzupełnić opis modelu o informacje, które umożliwiają:
  - nakładanie ograniczeń na elementy modelu (reguły, warunki)
  - poprawę precyzji oraz jednoznaczności modelu
  - definiowanie kwerend w celu uzyskania dostępu do elementów modelu i ich wartości

OCL - przykład

Klient
nazwisko: String tytuł: String jestMężczyzną: Boolean dataUrodzenia: Data wiek: Integer
wiek(): Integer

```
Klient
Wiek >= 18
```

Formalizmy definiowania bazy danych

1. Model Encja-Związek (*Entity-Relationship Model*) (ERM):
   - Najbardziej naturalny, modelowanie semantyczne
2. Języki modelowania obiektowego (ODL):
   - UML (*Unified Modeling Language*)
   - ODL (*Object Definition Language*)
   - inne: CWM (*Common Warehouse Metamodel*), …

Transformacja modeli

- Model konceptualny (E/R) → model relacyjny
  - Modele E/R są tworzone po to, by przekształcić je w model implementacyjny rzeczywistej bazy danych
- UML → model relacyjny
  - Przekształcenie modelu obiektowego do postaci relacji
- ODL → model relacyjny

Wybrane aplikacje wspomagające tworzenie diagramów (darmowe)

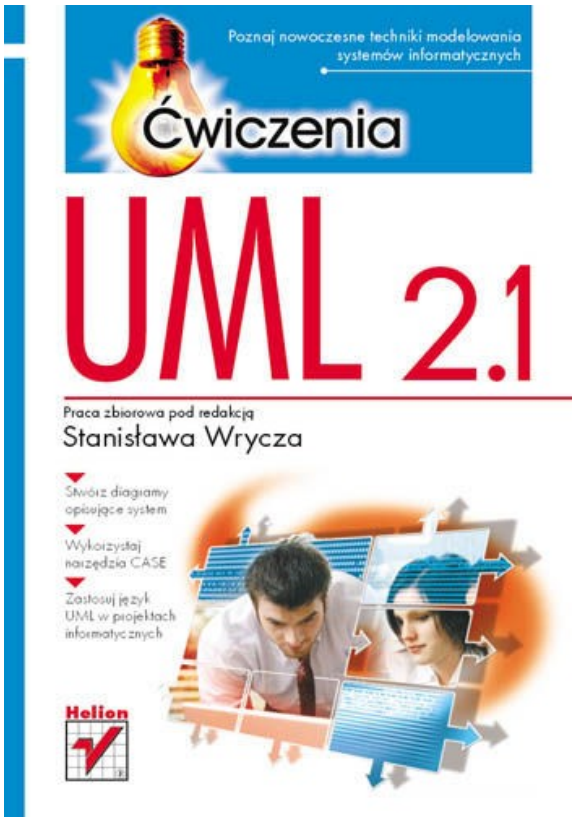
- ArgoUML - napisany w Javie, zaawansowane generowanie kodu i podpowiedzi, ciągle tworzony,
- StarUML - środowiska modelowania pod platformę Windows,
- Dia - ogólne narzędzie do rysowania diagramów,
- UML Sculptor - prosty, łatwy w użyciu program do tworzenia diagramów klas,
- Umbrello UML Modeller - program dla Linuksa, część KDE,
- UMLpad - Notepad with UML,
- Astah Community (wcześniej JUDE Community),
- NetBeans Enterprise Pack.

Wybrane aplikacje wspomagające tworzenie diagramów (komercyjne)

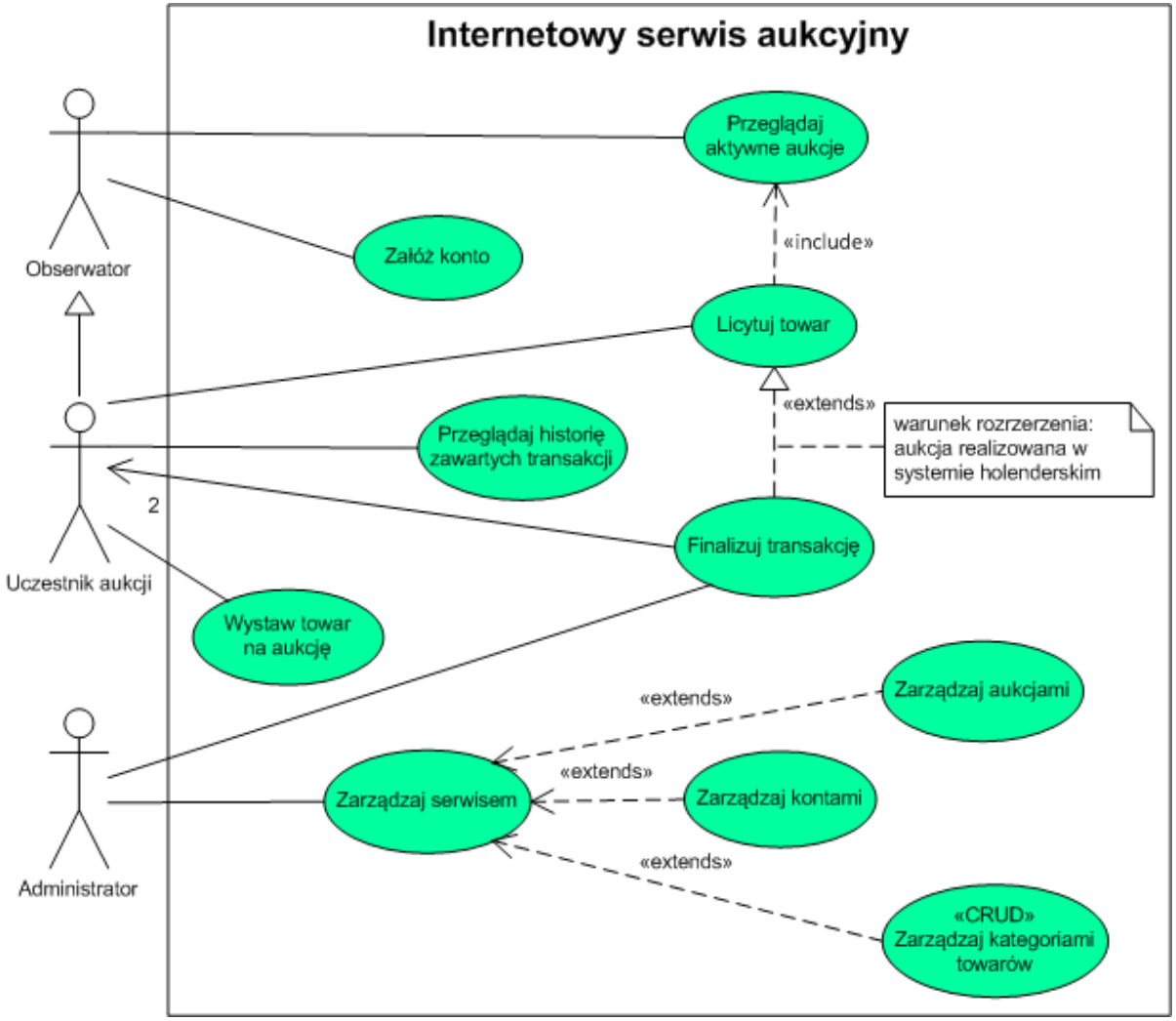
- Borland Together - rodzina programów integrujących się z różnymi IDE, jest wersja darmowa,
- Poseidon for UML - zaawansowane narzędzie bazujące na ArgoUML, darmowa edycja Community,
- Enterprise Architect - Profesjonalne narzędzie w przystępnej cenie o wygodnym interfejsie działające na platformach Windows i Linux. Wspiera UML 2.0,
- Rodzina programów iGrafx - narzędzia począwszy od iGrafx FlowCharter wspierają tworzenie diagramów UML. Wersja testowa na witrynie iGrafx,
- Visual Paradigm for UML,
- IBM Rational Rose,
- Telelogic Tau G2,
- Visio.

Przykłady

- Stanisław Wrycza (red.), UML 2.1, Ćwiczenia, Helion 2006.



DPU (ang. *Use Case*)



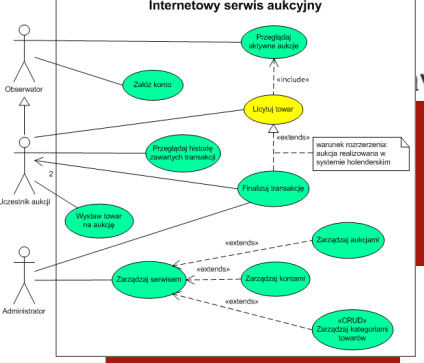


Tabela 2.1. *Licytuj towar — dokumentacja przypadku użycia*

Nazwa	*Licytuj towar*
Numer	1
Twórca	Tomasz Nowak — Analityk
Poziom ważności	Wysoki
Typ przypadku użycia	Ogólny, niezbędny
Aktorzy	*Uczestnik aukcji [kupujący]*
Krótki opis	Licytacja wskazanego towaru
Warunki wstępne	*Uczestnik aukcji* posiada niezablokowane konto
Warunki końcowe	Oferta została zarejestrowana lub został wyświetlony komunikat o błędzie, a stan systemu nie uległ zmianie
Główny przepływ zdarzeń	1) *Uczestnik aukcji* wskazuje aukcję, w której chce uczestniczyć

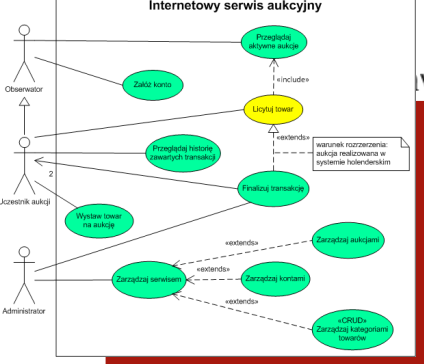
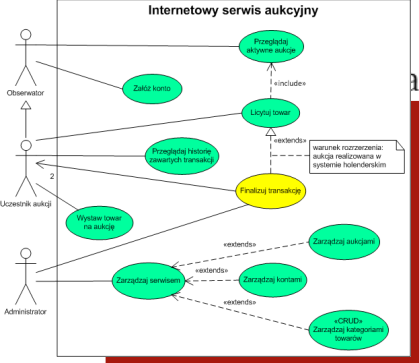


Tabela 2.1. *Licytuj towar — dokumentacja przypadku użycia — ciąg dalszy*

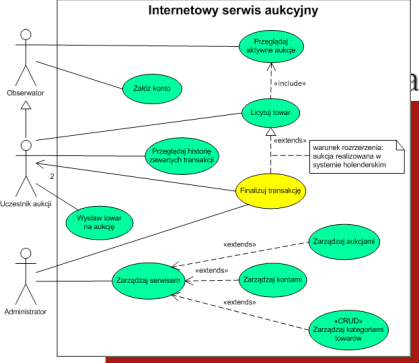
	2) System wyświetla formularz do wpisania oferty
	3) *Uczestnik aukcji* wpisuje ofertę, a następnie wybiera opcję *licytuj*
	4a) System rejestruje ofertę i informuje o tym *Uczestnika aukcji*
	5) Jeżeli aukcja realizowana jest w systemie holenderskim, następuje rozszerzenie o przypadek *Finalizuj transakcję*
Alternatywne przepływy zdarzeń	4b) Jeżeli w kroku 3) *Uczestnik aukcji* wprowadził kwotę niezgodną z regułami licytacji, system informuje o błędzie i następuje przejście do kroku 2)
Wyjątki w przepływach	4c) Jeżeli z powodu awarii technicznej lub zakończenia aukcji system nie może zarejestrować oferty, informuje o tym *Uczestnika aukcji* i następuje zakończenie przypadku
Specjalne wymagania	brak
Notatki i kwestie	Po zakończeniu aukcji system informuje kupującego i sprzedającego o wyniku licytacji W dowolnym momencie *Uczestnik aukcji* może zrezygnować z licytacji i następuje zakończenie przypadku



awska

Tabela 2.2. *Finalizuj transakcję — dokumentacja przypadku użycia*

Nazwa	*Finalizuj transakcję*
Numer	2
Twórca	Tomasz Nowak — Analityk
Poziom ważności	Wysoki
Typ przypadku użycia	Ogólny, niezbędny
Aktorzy	*Uczestnik aukcji [kupujący], Uczestnik aukcji [sprzedający]*



awska

Tabela 2.2. *Finalizuj transakcję — dokumentacja przypadku użycia* — ciąg dalszy

Krótki opis	Finalizacja rozstrzygniętych aukcji
Warunki wstępne	1) *Uczestnik aukcji* posiada niezablokowane konto 2) *Uczestnik aukcji [sprzedający]* był oferentem aukcji 3) *Uczestnik aukcji [kupujący]* wygrał licytację
Warunki końcowe	Transakcja została zakończona lub aukcja została unieważniona
Główny przepływ zdarzeń	1) System informuje *Uczestników aukcji* o zakończeniu licytacji 2a) Kupujący określa sposób płatności oraz wybiera formę dostarczenia towaru 3) System wysyła do sprzedającego informację o sposobie płatności oraz wybranej przez kupującego formie dostarczenia towaru 4) Sprzedający wystawia ocenę kupującemu 5) W przypadku negatywnej oceny system wysyła informację do *Administratora* 6) Kupujący wystawia ocenę sprzedającemu 7) W przypadku negatywnej oceny system wysyła informację do *Administratora* 8) *Administrator* w przypadku uzasadnionych skarg uczestników transakcji i (lub) naruszenia regulaminu może unieważnić transakcję
Alternatywne przepływy zdarzeń	2b) Jeżeli w ciągu 3 dni od zawarcia transakcji kupujący nie poinformował sprzedawcy o wyborze sposobu płatności, sprzedawca może unieważnić transakcję
Specjalne wymagania	brak
Notatki i kwestie	Pomiędzy kolejnymi zdarzeniami mogą wystąpić kilkudniowe odstępy czasowe Kroki 6) i 7) mogą wystąpić przed krokami 4) i 5)

Podsumowanie

- UML może być **stosowany na różnych etapach** realizacji projektu informatycznego;
- oferuje **wiele perspektyw modelowania** (poziomów szczegółowości).
- Istotnym jest wybór tych elementów, które w danym przypadku **ułatwiają przejście od wymagań do działającego systemu**.

CASE (ang. *Computer-Aided Software Engineering*)

NARZĘDZIA DO MODELOWANIA BAZ DANYCH

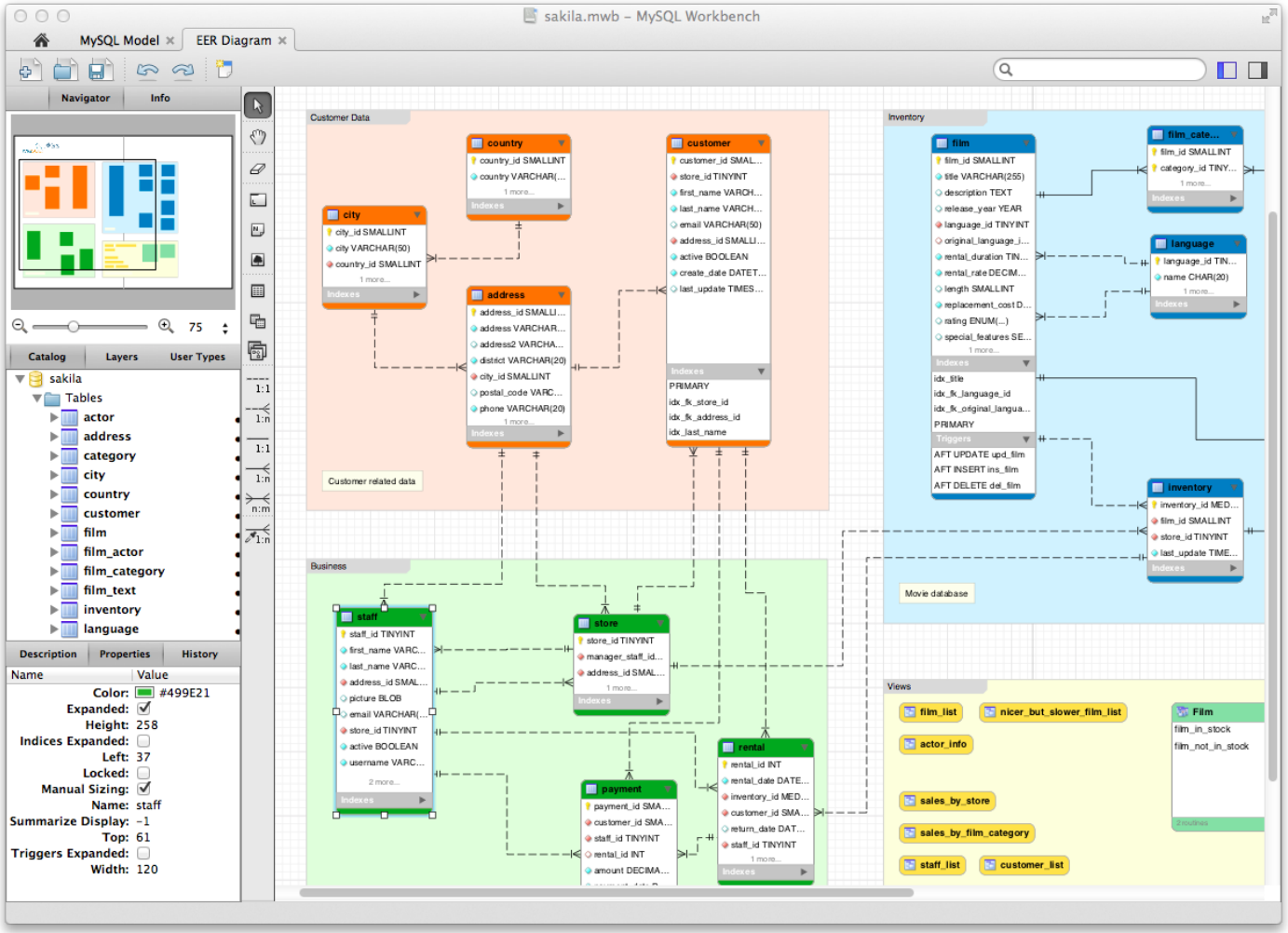
Wybrane narzędzia do modelowania

- Oracle MySQL **Workbench**
- Oracle SQL **Developer** Data Modeler
- SAP Sybase **PowerDesigner** DataArchitect
- IBM Rational Data Architect
- Microsoft Visio

Oracle MySQL **Workbench**

- Narzędzie do zarządzania i modelowania baz danych MySQL
- Wsparcie dla projektowania baz na poziomach koncepcyjnym, logicznym i fizycznym
- Wsparcie dla procesów reverse-engineeringu
- Możliwość generowania skryptów SQL
- Wersja: 8.0.15 (I 2019 r.)
- Licencja: GNU GPLicense lub zamknięta EULA
- http://www.mysql.com/products/workbench

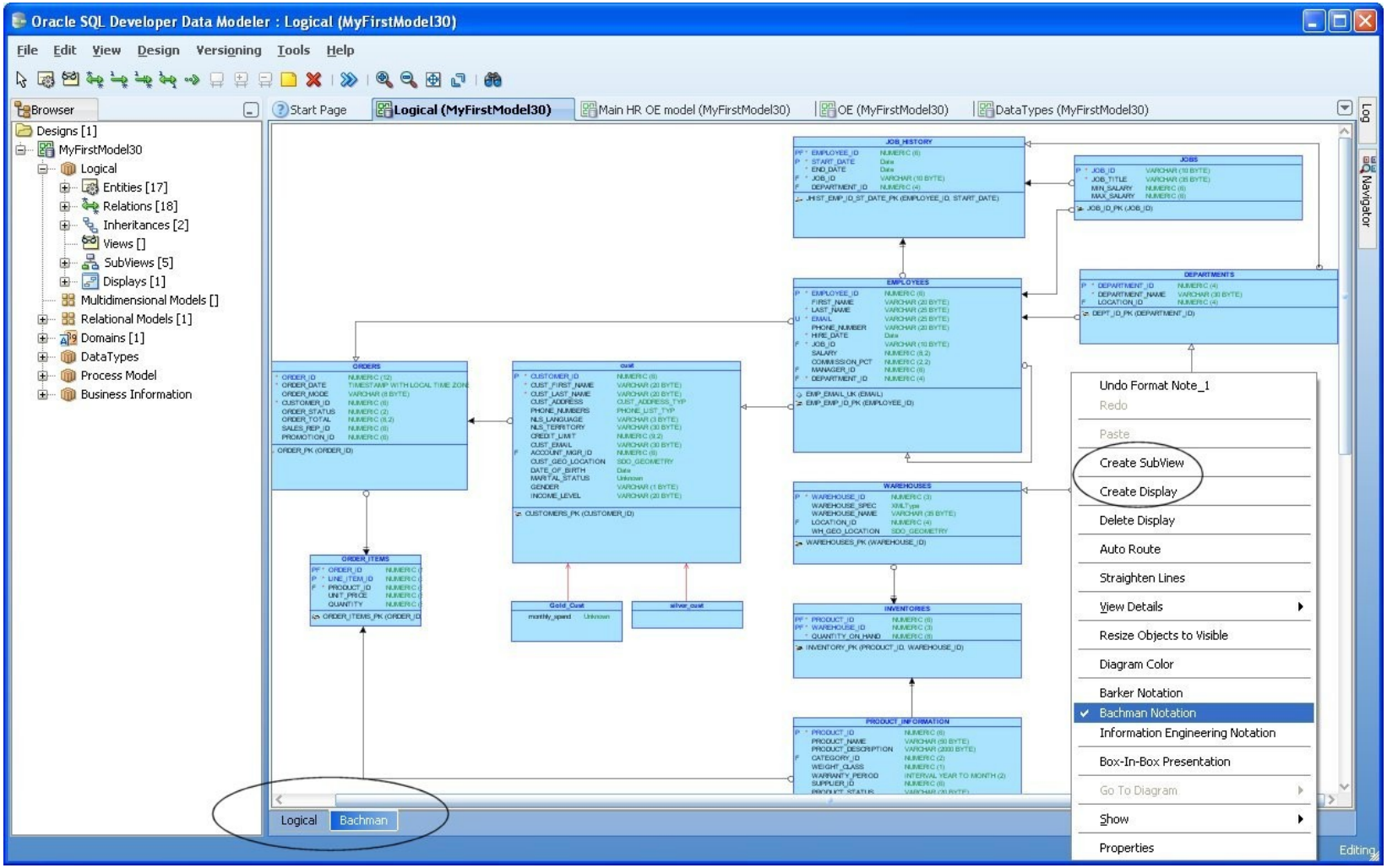
MySQL Workbench



Oracle SQL Developer Data Modeler

- Zintegrowane środowisko programistyczne dla użytkowników zajmujących się programowaniem baz firmy Oracle
- Wersja: 18.4 (I 2019 r.)
- Licencja: zamknięta
- http://www.oracle.com/technetwork/developer-tools/datamodeler/overview/index.html
- http://www.oracle.com/technetwork/developer-tools/datamodeler/downloads/datamodeler-087275.html

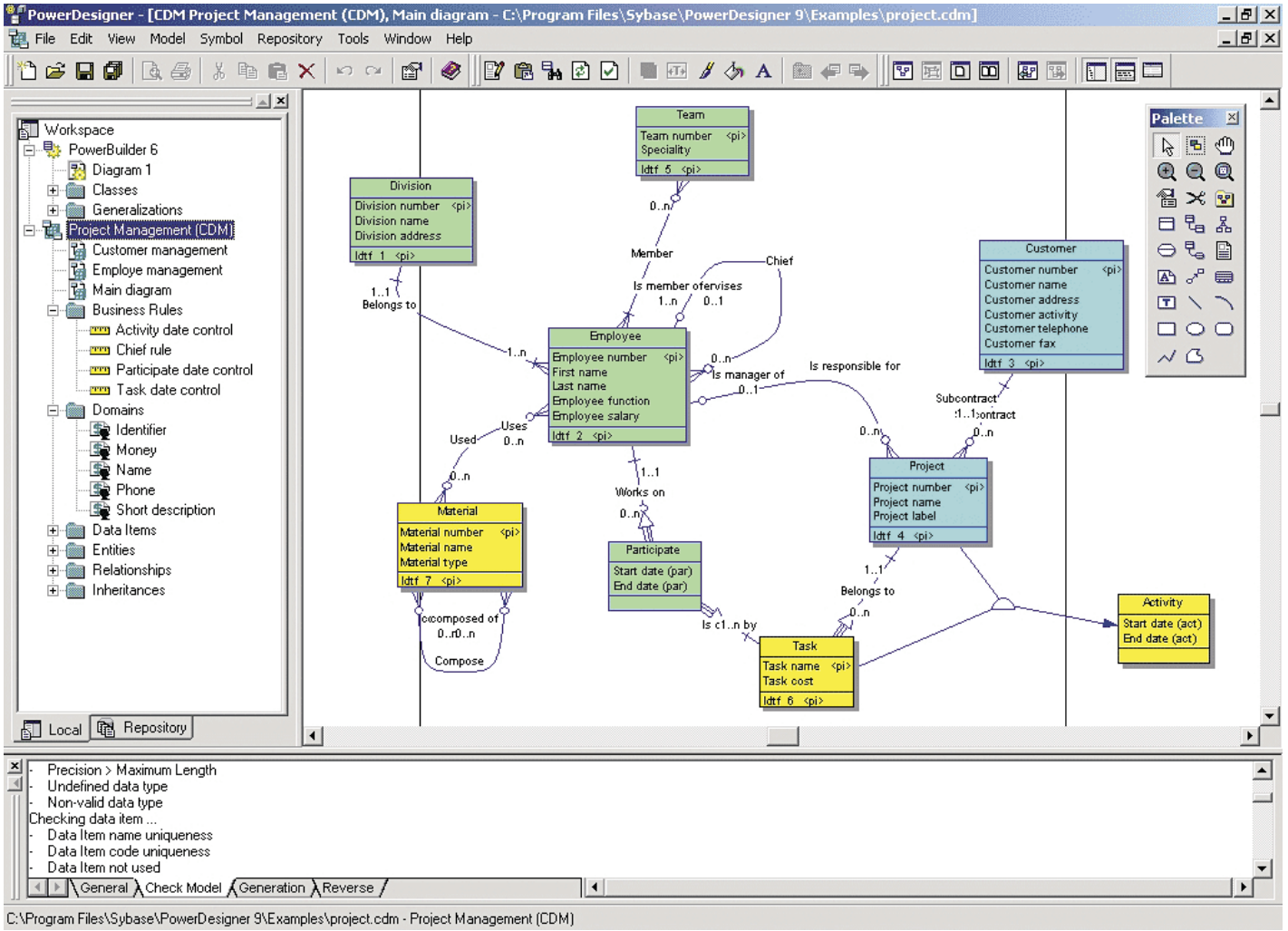
Oracle SQL Developer Data Modeler



SAP Sybase PowerDesigner DataArchitect

- Narzędzie do modelowania systemów: baz danych, hurtowni danych, modelowanie obiektowe, modelowanie procesów biznesowych i in.
- Wersja: 16.6 (III 2016 r.)
- Licencja: zamknięta
- Cena: ~2000 € - ~10000 €
  źródło: www.powerdesigner.de/en/pricing/

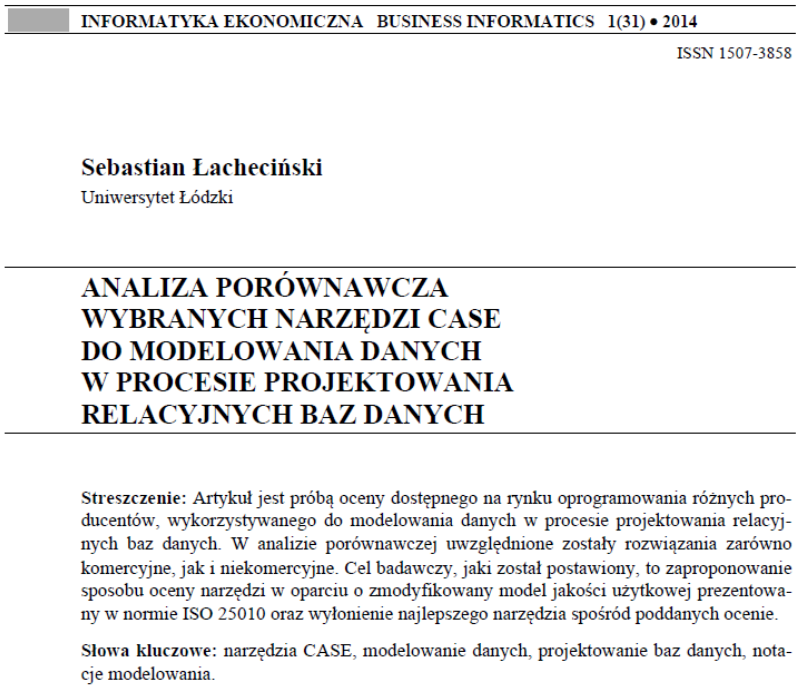
SAP Sybase PowerDesigner DataArchitect



Porównanie narzędzi

Sebastian Łacheciński, *Analiza porównawcza Wybranych narzędzi CASE do modelowania danych w procesie projektowania relacyjnych baz danych*, (w:) Informatyka Ekonomiczna Business Informatics, nr 1 (31), 2014, s. 239-258.

http://www.dbc.wroc.pl/dlibra/doccontent?id=25198



INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 1(31) • 2014

ISSN 1507-3858

Sebastian Łacheciński
Uniwersytet Łódzki

ANALIZA PORÓWNAWCZA WYBRANYCH NARZĘDZI CASE DO MODELOWANIA DANYCH W PROCESIE PROJEKTOWANIA RELACYJNYCH BAZ DANYCH

Streszczenie: Artykuł jest próbą oceny dostępnego na rynku oprogramowania różnych producentów, wykorzystywanego do modelowania danych w procesie projektowania relacyjnych baz danych. W analizie porównawczej uwzględnione zostały rozwiązania zarówno komercyjne, jak i niekomercyjne. Cel badawczy, jaki został postawiony, to zaproponowanie sposobu oceny narzędzi w oparciu o zmodyfikowany model jakości użytkowej prezentowany w normie ISO 25010 oraz wyłonienie najlepszego narzędzia spośród poddanych ocenie.

Słowa kluczowe: narzędzia CASE, modelowanie danych, projektowanie baz danych, notacje modelowania.

Testom poddane zostały:

- ER Studio XE5 Data Architect 9.7
- CA ERWin 9.5 Workgroup
- **SAP Sybase Power Designer 16.5 Data Architect RE**
- **Oracle SQL Developer Data Modeler 4.0.1**
- **MySQL Workbench 6.1.4**
- **MS Visio 2010/2013 Professional**
- IBM InfoSphere Data Architect 9.1

Wyniki

- Najlepszy: SAP Sybase PowerDesigner 16.5
- Dla darmowych narzędzi najlepszy wynik osiągnął: Oracle SQL Developer Data Modeler v. 4
- Dla wdrożeń w oparciu o serwer MySQL rozsądnym wyborem jest: MySQL Workbench 6.1.4.

rocławska

Politechnika Wrocławska

Bezpieczeństwo

Poziomy bezpieczeństwa:

1. bezpieczeństwo fizyczne danych,
2. bezpieczeństwo sieci,
3. bezpieczeństwo domeny,
4. bezpieczeństwo maszyny lokalnej,
5. bezpieczeństwo serwera baz danych,
6. bezpieczeństwo bazy danych,
7. bezpieczeństwo aplikacji bazodanowej.

Ryzyko i zagrożenia

- Zmiana polityki rządowej
- Awarie sprzętu komputerowego
- Awarie sieci elektrycznych, komunikacyjnych, komputerowych
- Błędy w oprogramowaniu
- Ograniczenie pojemności systemów
- Crackerzy

1. Kategorie zagrożeń

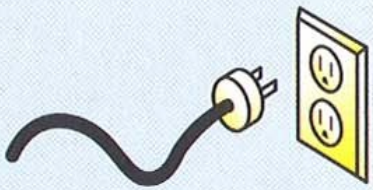
ZAGROŻENIA BEZPIECZEŃSTWA

Związane z postępowaniem człowieka

- **Złe intencje**
  - Napastnicy zewnętrzni, np. krakerzy i hakerzy
  - Napastnicy wewnętrzni, np. niezadowoleni pracownicy
- **Bez złych intencji**
  - Nieprzeszkoleni pracownicy

Niezwiązane z postępowaniem człowieka

(sprzęt/oprogramowanie/sieć)
Błędy i furtki w oprogramowaniu
Awarie produktów (MTBF)
Awarie zasilania
(mogą tworzyć luki w bezpieczeństwie)



Katastrofy naturalne

Powodzie, pożary, trzęsienia ziemi, huragany

2. Profile napastników

Napastnicy	Umiejętności	Znajomość celu	Środki	Motywy
Wywiad gospodarczy	Średnie-wysokie	Średnia-wysoka	Średnie-duże	Finansowe, konkurencja
Szpiedzy (agencje wywiadu)	Wysokie	Średnia-wysoka	Duże	Interesy narodowe
Napastnicy wewnętrzni (personel, kontrahenci)	Średnie	Wysoka	Średnie	Finansowe, zemsta
	UWAGA: Zwykle dysponują pewnymi prawami dostępu			
Terroryści	Wysokie	Średnia	Średnie-duże	Fanatyzm religijny i polityczny
Karierowicze łamiący prawo	Średnie-wysokie	Średnia	Średnie	Finansowe, zdobycie władzy
Hakerzy				
• Nowicjusze (Script Kiddie, Wannabe)	Niskie	Niska	Małe	Ciekawość, chęć wyróżnienia się
	UWAGA: Mają mnóstwo wolnego czasu i są niebezpieczni, bo nie zawsze zdają sobie sprawę, co robią			
• Black Hat (źli)	Średnie-wysokie	Wysoka	Średnie	Chęć wyróżnienia się, rzekome zwiększanie bezpieczeństwa
• Grey Hat	Średnie-wysokie	Średnia	Średnie	Działający jako Black i White Hat, do wynajęcia lub nie
• White Hat (dobrzy)	Średnie-wysokie	Brak celu	Średnie	Zwiększanie bezpieczeństwa (ale tworzą narzędzia, które są wykorzystywane przez nowicjuszy)
• Hacktivist	Średnie-wysokie	Średnia-wysoka	Małe-średnie	Polityczni aktywiści, którzy chcą coś zademonstrować

3. Techniki zdobywania informacji

- **Metody socjotechniczne (Social Engineering) do zdobycia numerów kont, haseł itp.**
- **Dostęp do materiałów publicznych:**
  1. Strony internetowe władz państwa, wyszukiwarki, InterNIC i inne serwisy online
  2. Fora dyskusyjne, ekrany logowania, książki telefoniczne, artykuły i wycinki prasowe, wyniki finansowe
  3. Usługi detektywistyczne

- **Skanowanie adresów IP:** ping, TJping, traceroute
- **Skanowanie portów:** Ultrascan, NMAP, Slow Scan Attack (w celu uniknięcia wykrycia)
- **Programy narzędziowe i instrukcje Unix/NT:** Finger, Netstat, Rpcinfo, nslookup, whois, przeglądarka do śledzenia źródła, Telnet do połączenia z dostępnym portem i zdobycia jakichś danych (np. numeru wersji oprogramowania), expn root @foo.com, rlogin, rsh, rexecd, próby znalezienia plików: /etc/shadow, /etc/passwd, /etc/aliases i przesłania ich do siebie
- **Man-in-the-middle:**

  Przechwytywanie pakietów za pomocą analizatorów protokołów (np. ethfind, sniff, netmon, tcpdump), wykorzystując:

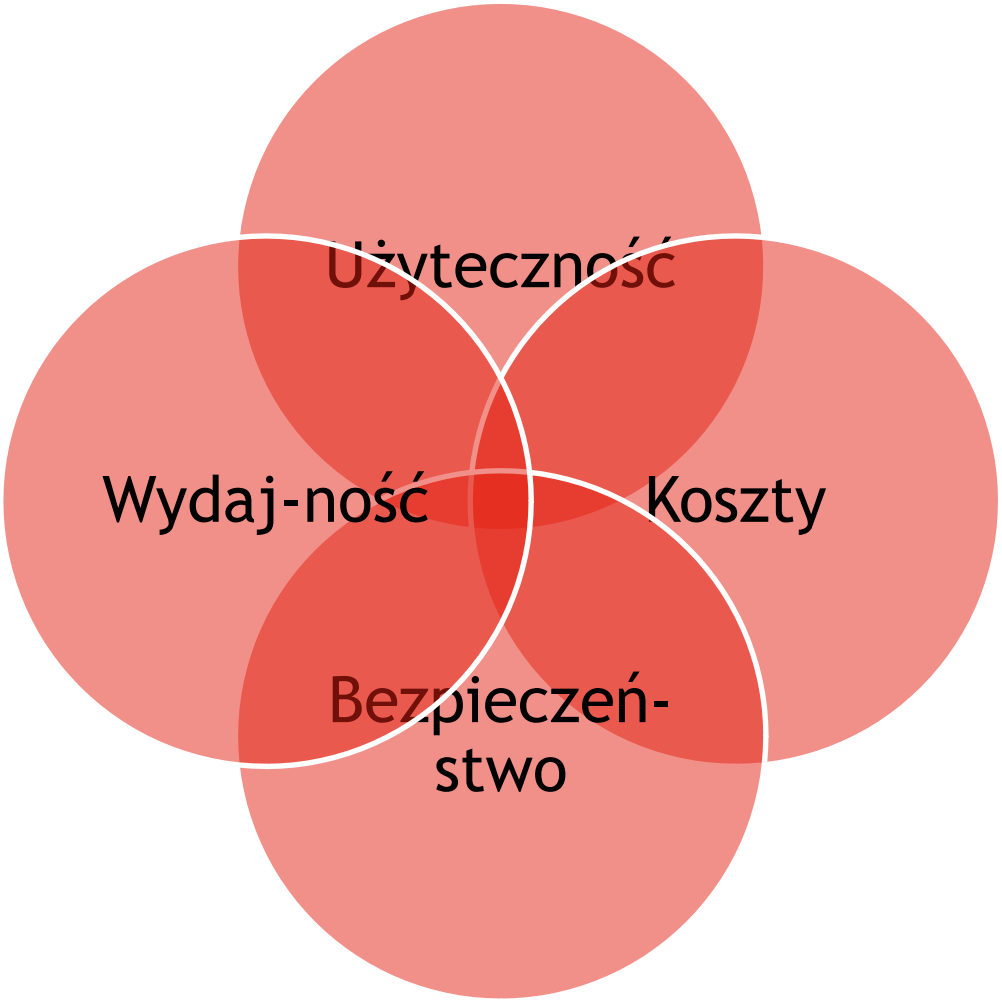
  1. Fizyczny dostęp do sieci: podsłuch przez szafkę telefoniczną, wolne gniazdko sieciowe lub modem kablowy
  2. Kontrolę przejętą nad hostem w sieci
  3. Przekierowywanie danych przy użyciu podrobionych pakietów RIP, DNS lub ICMP Redirect

- **War Dialing:** zautomatyzowana technika skanowania linii telefonicznych w poszukiwaniu niezabezpieczonych modemów. Inne przykłady to ToneLOC, AIO, Modem Hunter i Demon Dialer
- **Wrogie aplikacje:** GetAdmin, NetBus, BackOrifice do zdobycia informacji, haseł itp.
- **Przeszukiwanie śmieci:** firmowe odpadki są cennym źródłem informacji
- **Informacje podejrzane lub podsłuchane:** podczas rozmowy w samolocie, restauracji i innych miejscach publicznych
- **Użycie internetowych robotów wyszukiwawczych:** do znalezienia źle zabezpieczonych stron internetowych (luki w cgi bin)

Zagrożenia bezpieczeństwa

- Ujawnienie poufnych danych
- Modyfikacja lub zniszczenie danych
- Uniemożliwienie świadczenia usług
- Nieuznawanie transakcji

Konieczność kompromisu



Metody socjotechniczne (Social Engineering)

Atak z podszywaniem się
Wykorzystywanie fałszywego identyfikatora, ubioru służb porządkowych itp. do zdobycia informacji lub dostępu; wykorzystanie informacji o pewnych osobach w celu podania się za ich przyjaciół lub znajomych; podawanie się za osobę uprawnioną i żądanie informacji

Atak „na ignoranta"
Nakłonienie kogoś, by wyjaśnił, zaprzeczył lub uzupełnił „pseudowiedzę" napastnika;

Atak z podpuszczaniem
Wypowiadanie wyjątkowych kłamstw i niedorzeczności, by zdobyć informacje w odpowiedzi

Atak nieustający
Ciągłe nękanie ofiary poczuciem winy, onieśmielanie i inne negatywne oddziaływania, by zdobyć informacje

Atak przez obserwację
Rejestrowanie aktywności i działań ludzi w czasie, dostaw towarów itp.

Atak z przynętą
Wykorzystanie atrakcyjności seksualnej w celu zdobycia informacji lub dostępu

Atak brutalny
Atak z użyciem siły, zastraszenie, grożenie bronią, szantaż

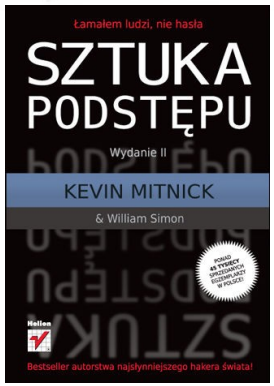
Atak przez łapówkę
Użycie zwykłego przekupstwa

Atak z fałszywym alarmem
Wszczynanie serii fałszywych alarmów, by ofiara wyłączyła swój system alarmowy

Atak z Help Desk
Podszycie się pod obecnego lub nowego użytkownika potrzebującego pomocy, by zdobyć dostęp do sieci lub serwera

Atak z „wmieszaniem się w tłum"
Spotkania i imprezy firmowe są znakomitym miejscem zdobycia informacji i dostępu. Wmieszanie się w grupę pracowników i udawanie jednego z nich

Atak z fałszywą ankietą
Obietnica wygrania wycieczki do egzotycznych krajów po udzieleniu odpowiedzi na kilka pytań dotyczących firmowej sieci



Działania hakerskie

1. Wykorzystanie złego administrowania

- Użycie odgadniętego lub wykradzionego hasła do zdobycia dostępu do konta, wykorzystując dziurę w zaporze ogniowej lub modem
- Wykorzystanie pozostawionych niebezpiecznych usług: TFTP itp.
- Wykorzystanie do zdobycia dostępu pozostałości po debugowaniu: phf.cgi, files.pl

2. Wykorzystanie błędów programowych

- Doprowadzenie do przepełnienia bufora, by uruchomić złośliwy kod
- Wstawienie specjalnych znaków do aplikacji lub strony internetowej ofiary
- Użycie opcji debugowania lub furtek programowych w oprogramowaniu bez poprawek
- Użycie "wyścigu" (race condition) do zwiększenia zakresu dostępu (zdobycia uprawnień root lub administratora)

3. Skłonienie ofiary do uruchomienia konia trojańskiego (pod postacią gry lub atrakcyjnego obrazka), instalującego tylne drzwi

NetBus, BackOrifice, dające napastnikowi dostęp

4. Wykorzystanie funkcji dostępnych z zewnątrz lub na hostach klienckich

- Złośliwy kod osadzony w aktywnym/mobilnym kodzie
- JavaScript (np. wykorzystanie funkcji CALL w Excelu)
- ActiveX - Java
- NTFS Streams - PostScript
- Przygotowanie płyty CD z funkcją AutoPlay, która instaluje wirusa lub program tylnych drzwi

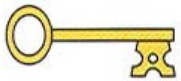
5. Różne narzędzia hakerskie

- Analizator pliku Core dump
- Hex editor
- Modem Jammer: zapobiega wykrywaniu połączeń modemowych
- Netcat: doskonałe narzędzie do połączeń TCP/UDP, autorzy: „The Hobbit" i Weld Pond

6. E-shoplifting

- Zmodyfikowany html przesłany z powrotem do strony dostawcy

Cracking



Lekki
(Mały wysiłek umysłowy)

- Dostęp nie zabezpieczony hasłami
- Hasło zapisane w miejscu łatwym do znalezienia
- Konto, w którym nazwa użytkownika = hasło
- Hasło wywodzące się z nazwiska lub imienia użytkownika (efektywność 5-10%)
- Tylne drzwi pozostawione przez poprzedniego napastnika

Pracochłonny
(Pochłaniający dużo czasu)

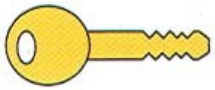
- Ataki słownikowe oparte na:
  1. Słowniku wyrazów powszechnie używanych
  2. Słowniku wyrazów danego języka
  3. Słownikach wyrazów i wzorów w innych językach
  4. Filtry podstawień; o=0, 1=!, dla=4, do=2, E=3
- Przykłady narzędzi wykorzystywanych przy odgadywaniu haseł

  Crack v5.0
  L0pht Crack v2.0 for NT
  NetBUS
  FastZip Password
  Jack the Ripper

Średni
(Wymaga zarówno wysiłku umysłowego, jak i zasobów obliczeniowych)

- Wyczerpujące wyszukiwanie klucza
- Złamanie szyfru asymetrycznego/ symetrycznego może zabrać wiele czasu w zależności od długości użytego klucza
- 40-bitowy: minuty
- 56-bitowy: godziny/dni
- 128-bitowy: nie do złamania!
- SSL PKCS#1

  Saltine Cracker



Ciężki
(Najbardziej zaawansowane metody kryptoanalityczne)

- Kryptoanaliza linearna
- Kryptoanaliza różnicowa
- Łamanie z kryptogramami
- Łamanie ze znanym tekstem jawnym
- Łamanie z wybranym tekstem jawnym
- Łamanie z adaptacyjnie wybranym tekstem jawnym
- Łamanie z wybranymi kryptogramami
- Łamanie z wybranym kluczem

Ataki hybrydowe

- Istnieje nieskończona liczba ataków hybrydowych wykorzystujących dowolną kombinację rozmaitych metod w różnych sekwencjach, zależnie od celu, poziomu wiedzy i doświadczenia napastnika.
- Ataki hybrydowe stanowią zdecydowaną większość wszystkich ataków.
- Uwaga! 80% włamań obejmuje działania wykorzystujące:
  1) znane, niezałatane luki,
  2) łatwe do odgadnięcia hasła.

Ataki hybrydowe

- Kilka przykładów …

Gromadzenie informacji
- Skanowanie portów
- Przechwytywanie pakietów
- Metody socjotechniczne
- War Dialing

Włamanie i przejęcie kontroli
- Wykorzystanie dobrze znanych słabych punktów
- Wykorzystanie złej konfiguracji systemu operacyjnego
- Odgadywanie haseł/Cracking
- Instalowanie narzędzi „rootkit”
- Dodawanie użytkownikom przywilejów by przejąć zdalnie

Przestępstwa
- Zmienić, ukraść, zniszczyć ….
- DDoS, przerobienie strony internetowej
- Manipulowanie danymi
- Kopiowanie własności intelektualnej (bazy danych HR, listy płac, karty kredytowe…)

TYPY ATAKÓW

1. Buffer overflow

- zapisanie łańcuchów danych przekraczających rozmiar bufora, przy niedopracowanych aplikacjach może spowodować uzyskanie uprawnień do wykonywania swoich programów
- zapobieganie: instalacja łatek
- przykład: błędy ODBC w serwerze webowym Microsoft (Windows NT)

2. Wirusy, robaki i konie trojańskie

- znane z życia codziennego ☹
- zapobieganie: aktualne oprogramowanie antywirusowe, wyłączanie zbędnych usług

Wirusy komputerowe

Klasyfikacja wirusów

Wirus właściwy Złośliwy program, który dokleja część lub cały swój kod do innego pliku. Zarażone pliki to zwykle pliki wykonywalne lub pliki danych z częścią wykonywalną.
Robak (Worm) Złośliwy program, który ma zdolność do rozprzestrzeniania się do komputerów innych użytkowników. Najczęściej spotykaną formą dystrybucji jest e-mail.
Koń trojański Złośliwy program, który kamufluje się jako oprogramowanie użyteczne lub służące do rozrywki, ale w rzeczywistości przeprowadza szkodliwe działania, np. niszczy dane.

Chociaż podział obejmuje trzy klasy złośliwych programów, to zdarza się, że autorzy wirusów piszą programy, które można zaliczyć do więcej niż jednej klasy. Przykładem są konie trojańskie, które usuwają dane i mogą rozprzestrzeniać się za pośrednictwem poczty elektronicznej.

Złośliwa działalność	Opis	Symptomy	Przykłady
Infekcja sieci	Znajduje dostępne w sieci serwery z plikami i infekuje znajdujące się tam pliki.	Zainfekowane pliki wykryte na serwerach i komputerach ze współdzielonymi zasobami. Wirusy takie mogą bardzo szybko się rozprzestrzeniać w sieci.	W32.Funlove, W32.HLLW.Bymer, Worm.ExploreZip
Masowy mailing	Wysyła e-maile do innych użytkowników, zwykle zawierające złośliwy kod osadzony w treści lub załączony do przesyłki.	Serwery pocztowe zaczynają pracować wolniej i załamują się. Wykorzystanie tego typu programu może być uważane za atak typu Denial of Service.	VBS.LoveLetter, Wscript.Kakworm, W32.Prolin.Worm, Worm.ExploreZip
Niszczenie plików	Różne pliki są usuwane z systemu lub uszkadzane. Usuwane pliki mogą obejmować określone typy lub wszystkie pliki atakowanego systemu.	Programy nie startują, pliki z danymi nie są dostępne, ogólna niestabilność systemu.	W32.Kriz, Worm.ExploreZip, VBS.NewLove.A
Eksport danych	Znajduje osobiste informacje, takie jak hasła i numery kart kredytowych, i wysyła je pod ustalony adres e-mailowy lub internetowy.	Zwykle nie ma zauważalnych od razu objawów działania, ewentualnie wyższe rachunki za dostęp do Internetu.	Buddylist, PWSteal.Trojan
Przejęcie systemu	W różnych składnikach systemu są instalowane punkty zaczepienia, pozwalające monitorować lub unieruchamiać te składniki, ewentualnie zmieniać sposób ich działania. Czasami punkty zaczepienia są wykorzystywane do uruchamiania złośliwych programów.	Z normalną pocztą mogą być wysyłane dodatkowe e-maile; funkcjonowanie przeglądarki może być ograniczone lub zmienione.	W95.MTX, W32.Navidad, Happy99.Worm
Niszczenie sprzętu	Próbuje wymazać BIOS lub usunąć ustawienia CMOS.	Wewnętrzny test po włączeniu urządzenia może nie startować; dyski twarde mogą nie być właściwie rozpoznawane.	W32.Kriz, W95.CIH W32.Navidad, KeyPanic.Trojan
Wizualne treści	Wyświetla komunikaty lub grafikę.	Mogą się pojawiać różne komunikaty lub obrazki. W paskach narzędziowych mogą się pojawić nowe ikony.	Happy99.Worm
Tylne drzwi/ zdalna kontrola	Po zainstalowaniu w systemie programy te „nasłuchują" instrukcji z innych komputerów, a następnie je wykonują.	Zwiększony ruch sieciowy. Nietypowa aktywność na portach IP/UDP. Napastnicy przeprowadzający atak typu Denial of Service często wykorzystują mechanizmy tylnych drzwi.	Backdoor.SubSeven, BackOrifice, NetBus
Socjotechnika	Metody, jakimi twórcy wirusów posługują się, by fałszywie przedstawić swój program użytkownikom i zachęcić ich do uruchomienia go.	Użytkownik może otrzymać e-mail, który ma intrygujący, zachęcający temat lub treść. Czasami można natknąć się na pliki wysłane do grup dyskusyjnych, które są rzekomymi zdjęciami o treściach seksualnych itp.	W32.Funlove, PrettyPark.Worm, Mypics.Worm

Uwaga: *Informacje o tych i innych złośliwych programach można znaleźć na stronach Symantec AntiVirus Research Center, http://www.sarc.com*

3. Spoofing (podszywanie się)

- podrabianie wiarygodnej tożsamości,
  - fałszowanie adresu IP (zaufanie serwera lub udawanie kogoś innego),
  - podrabianie zaufanej witryny (może klient się „zaloguje”),
  - inne;
- zapobieganie: zabezpieczenia firewall’a, podpisy cyfrowe, urządzenia.

4. Podszywanie się/Spoofing

Rodzaj	Scenariusz	Jak to możliwe	Jak zapobiegać
E-mail	Wysłanie podrobionego e-maila z fałszywym wierszem „Od:" do serwera SMTP	Brak uwierzytelniania w SMTP	Sprawdzać źródłowy adres IP komunikatu lub używać podpisów cyfrowych
Przekaźnik poczty anonimowej	Napastnik wysyła e-mail z konta na przekaźniku poczty anonimowej	Brak uwierzytelniania w SMTP	Używać podpisów cyfrowych
Login	Wykorzystanie czyjejś nazwy użytkownika i hasła do dostania się do hosta	Brak ostrożności przy hasłach	Chronić hasła lub używać silnego uwierzytelniania
Rutowanie	Wysłanie podrobionych pakietów RIP lub ICMP do routera lub pakietu w trybie source routed do hosta	Brak uwierzytelniania w protokołach RIP, przekierowanie ICMP, trybie source routed	Nie używać tych protokołów w komunikacji z niezaufanymi sieciami
Partner	Wysłanie podrobionego e-maila do InterNIC z prośbą o zmianę nazwy domeny internetowej lub podmianę adresu IP	InterNIC nie stosuje pełnego uwierzytelniania, chyba że żąda tego klient	Zapewnić uwierzytelnianie zmian domeny w InterNIC
Spoofing DNS	Wysłanie nieproszonej odpowiedzi z podrobioną nazwą domeny i adresem do serwera DNS ofiary	Brak uwierzytelniania w DNS	Używać zmodyfikowanego DNS, który nie buforuje wpisów
Adres IP	Wysłanie pakietu z podrobionym źródłowym adresem IP do „ufającego" hosta	Adres źródłowy jest rzadko sprawdzany	Zablokować dostęp z zewnątrz przez zaufane wewnętrzne adresy
Przejęcie kontroli nad sesją	Napastnik wstawia podrobione pakiety do zestawionej sesji; przykładowe narzędzia: HUNT i Juggernaut	Uwierzytelnienie już było	Szyfrować sesje
Spoofing www http://www.cs.princeton.edu/sip/pub/spoofing.html	Napastnik sporządza kopię całej strony internetowej, ruch przechodzi przez komputer napastnika, co pozwala mu śledzić działania ofiary, przechwytywać hasła i numery kont	W ataku "man-in-the-middle" napastnik przepisuje wszystkie adresy URL ze strony internetowej, tak że kierują one ofiarę na serwer napastnika	Wyłączyć obsługę JavaScript, zwrócić uwagę, by w przeglądarce była wyświetlana linia adresu, kontrolować wyświetlany adres URL

5. Denial of Service (DoS); DDoS

- DoS (odmowa świadczenia usługi) przy użyciu standardowych protokołów lub procesów blokuje usługi, np. „ping śmierci”, otwierająca się ogromna liczba okienek,
- zapobieganie: właściwa konfiguracja firewall’a oraz zabezpieczenia po stronie komputera klienta, a także np. monitorowanie sieci.

Denial of Service (DoS)

Atak	Dysk	Pasmo	Wewnętrzna struktura danych lub przepełnienie bufora	Cykle CPU lub załamanie	Uwagi
Przesłanie dużych plików przez FTP	X				Wypełnia dysk danymi-śmieciami
Spowodowanie wpisu obszernych komunikatów o błędach do dziennika	X		X	X	Przepełnia dysk lub bufor
SYN Flood			X		Zamyka port na krótki czas
Teardrop			X	X	Wykorzystuje nachodzące na siebie fragmenty pakietów IP
Smurf		X			Przekierowuje broadcast, jako źródło podaje adres IP ofiary
Snork		X			Wysyła fałszywy komunikat o błędzie do portu 135 w NT
Bomba UDP		X		X	Fałszywy pakiet pomiędzy portami echo i chargen
Atak OOB			X	X	Użycie podrobionych wartości istotnych wskaźników danych
Ping of Death			X	X	Przepełnienie bufora datagramami IP
Flood Ping		X		X	Zalewa sieć
WinNuke			X	X	Wysyła śmieci do portu 139 w NT
Land			X	X	Podaje jako źródło adres ofiary
Bomby e-mailowe, spam	X			X	Zapycha serwer/bramkę pocztową lub skrzynkę użytkownika

Przykłady: Mailbombs, SYN FLOOD, Aenima 2.0, WIN NUKE, ZERO LENGTH, Wnuke5, WinGenocide, Avalanche 3.0 4.0, Nuker, LiquidNuker

Atak Distributed Denial of Service (DDos) Przykłady: Trinoo, TFN, TFN2K, Stacheldraht

Bardzo poważne zagrożenie, wykorzystujące wiele komputerów w skoordynowanym ataku mającym na celu wyczerpanie przepustowości routera i zasobów stosu sieciowego, a w rezultacie zerwanie łączności

1) Stworzenie sieci komputerów do ataku DDoS przez włamanie się do tych komputerów, zdobycie uprawnień root, zapewnienie zdalnej kontroli i zainstalowanie oprogramowania służącego do ataku
2) Wysłanie do wszystkich przejętych komputerów pakietów z instrukcjami o typie ataku, czasie jego trwania i adresie celu
3) Sieć komputerów DDoS wysyła strumienie pakietów (z fałszywymi adresami źródłowymi) do ofiary (np. atak Smurf, wysyłanie do ofiary dużej ilości pakietów echo)

6. Session Hijacking

- przejęcie istniejącego połączenia i odgrywanie roli jednej ze stron,
- zapobieganie: instalacja łatek, właściwe projektowanie i implementacja oprogramowania.

ATAKI BAZODANOWE

Ataki bazodanowe

- Wstrzyknięcia kodu SQL (ang. *SQL Injection*)
- DoS (odmowa usługi) za pomocą SQL Injection
- *Cross Site Scripting* (XSS),
- *Wildcard attack*
- *Account lockout attack*

Uzyskiwanie dostępu do systemu

- Uzyskiwanie dostępu do systemu

```
SELECT * FROM USERS WHERE USERNAME LIKE 'POBRANY_LOGIN' AND
PASS LIKE 'POBRANE_HASLO';
```

- Przykład ataku

```
SELECT * FROM USERS WHERE USERNAME LIKE ' ' OR 1 = 1; --
```

- Przekazywanie wielu zapytań (modyfikacja bazy danych)

```
SELECT * FROM USERS WHERE USERNAME = 'x'; DROP TABLE USERS;
SELECT '1';
```

DoS za pomocą SQL Injection

```
SELECT * FROM USERS WHERE USERNAME = 'x' OR
BENCHMARK(9999999,
BENCHMARK(999999,
BENCHMARK(999999, MD5(NOW()))))) = 0;
```

Inne ataki bazodanowe - Wildcard attack

```
SELECT * FROM TABLE WHERE COLUMN LIKE '%something%,
_[^!_%/%a?F%_D)_(F%)_%([)({}%){()}£$&N%_)$*£()$*R"_)]
   [%](%[x])%a][$*„£$-9]_
```

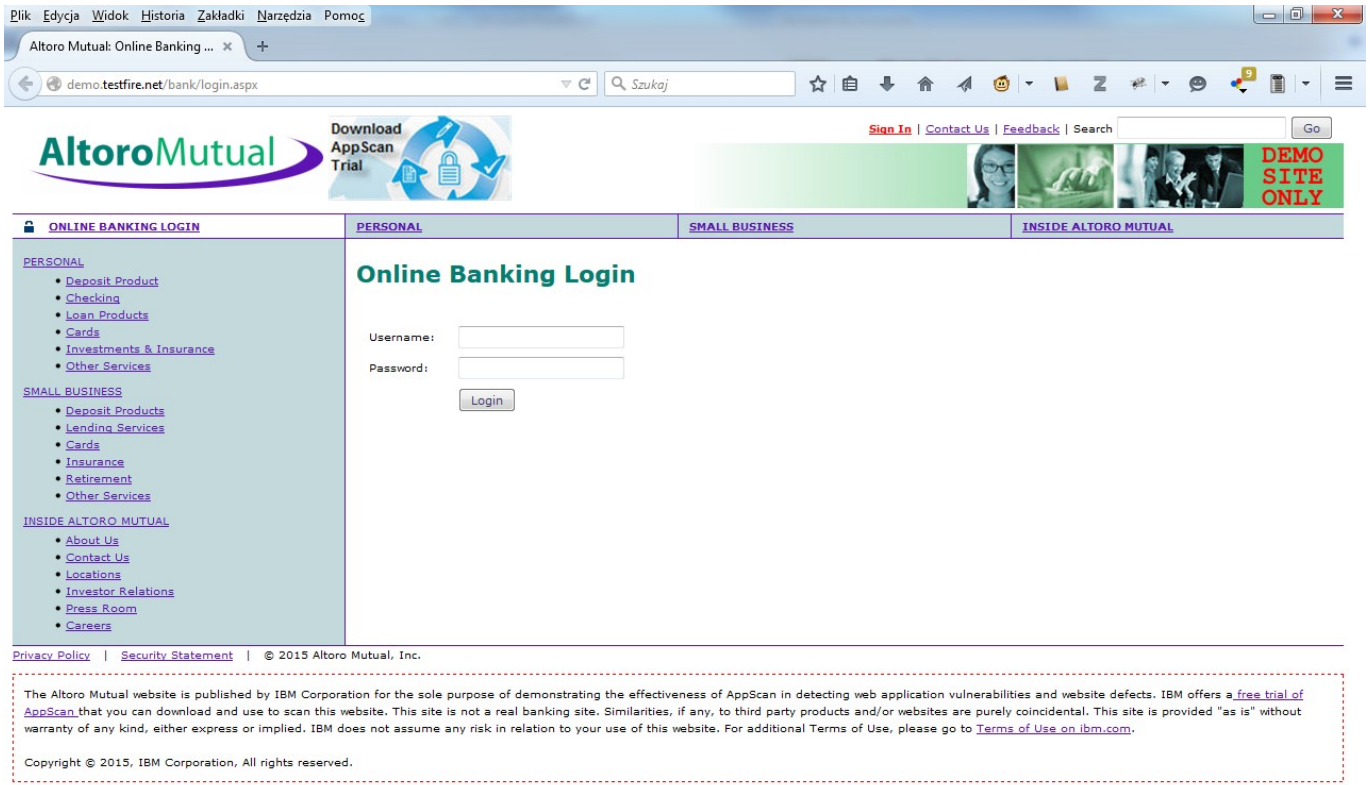
Jak chronić swoje aplikacje przed SQL Injection?

- Na poziomie aplikacji
  - Niedopuszczenie do przekazania znaku ’ do zapytania
  - „Zaślepki”
  - Rzutowanie łańcucha znaków na wartość liczbową.
  - Wyłączenie komunikatów o błędach lub ich zastąpienie.
- Na poziomie bazy danych
  - Ograniczenie uprawnień aplikacji
- Na poziomie serwera aplikacji
  - Odfiltrowywanie podejrzanych zapytań

Przykład

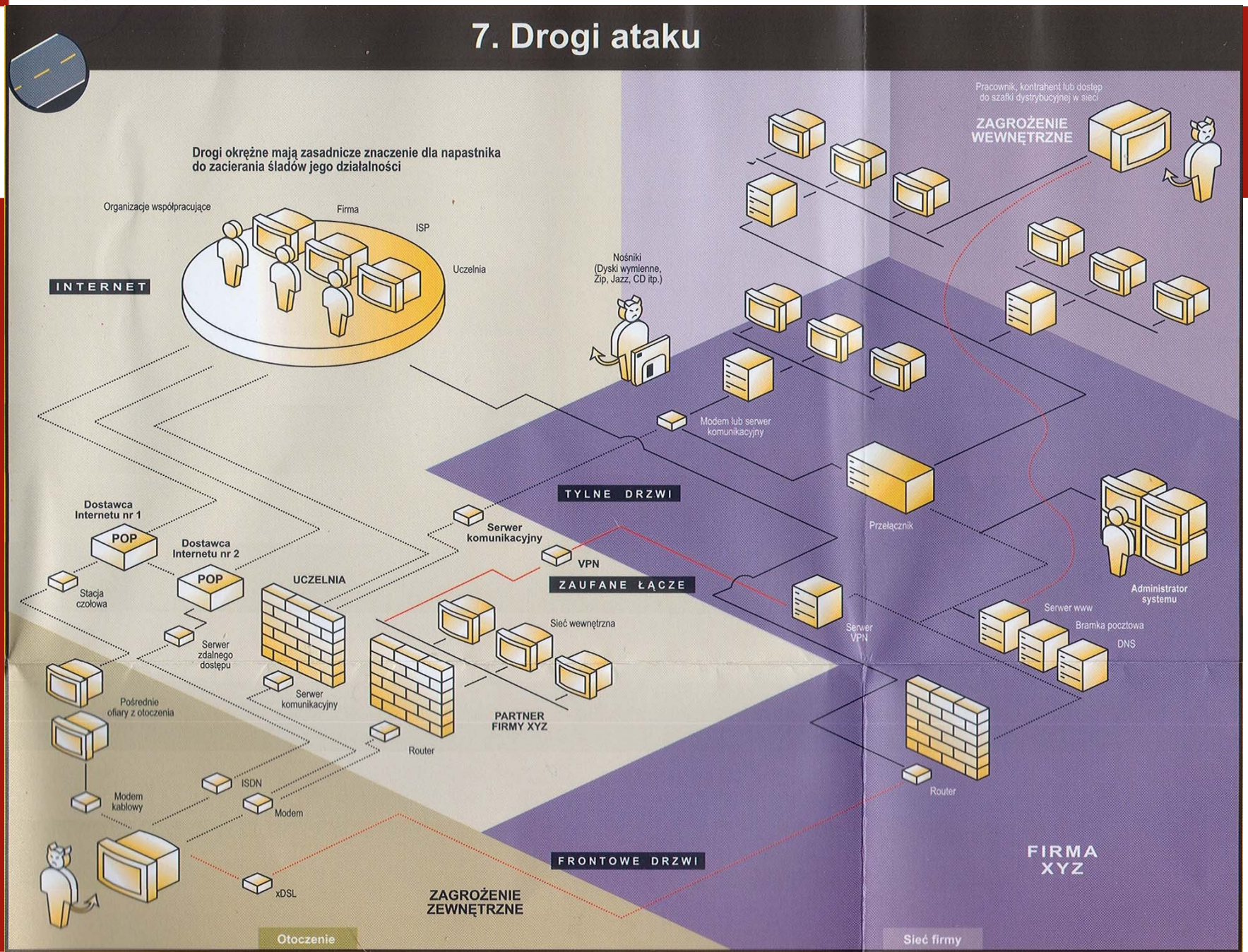
- AltoroMutual Bank – strona

http://demo.testfire.net/bank/login.aspx



UMIEJSCOWIENIE BAZY DANYCH W ARCHITEKTURZE SIECI FIRMOWEJ

7. Drogi ataku



8. Luki w zabezpieczeniach

1. Łatwe do odgadnięcia hasła

- Zbyt krótkie
- Zbyt proste (niewykorzystujące cyfr, małych i wielkich liter oraz znaków specjalnych)
- Wykorzystujące pospolite wyrazy (słownikowe)
- Oparte na prostych trikach (dodanie cyfry do nazwy użytkownika lub odwrócenie nazwy użytkownika)

2. Nieaktualne oprogramowanie (niezainstalowane poprawki programowe bezpieczeństwa)

3. Złe administrowanie systemem

- Niewyłączone usługi (każdy system operacyjny ma dużo ustawień domyślnych)
- Konta niezamknięte lub zbyt wiele kont
- Pozostawione konta domyślne
- Niedostatecznie kontrolowane usługi zaufane

4. Złe obchodzenie się z informacjami poufnymi

- Zapisywanie haseł (w miejscach dostępnych dla innych)
- Przesyłanie poufnych danych w e-mailu (to jak na pocztówce)
- Użycie protokołów przesyłających jawnie hasła (FTP, HTTP, POP3, Telnet, SNMP)
- Przesyłanie poufnych informacji przez FTP lub HTTP

5. Nieprzeszkolony personel bez świadomości zagrożeń bezpieczeństwa

- Podatny na metody socjotechniczne
- Nieznający powodów i metod ochrony prywatności informacji

6. Wykorzystanie zaufanych usług w niezaufanych sieciach

- NFS
- Współdzielenie dysków w Windows
- Komendy „r" (rsh, rlogin, rexec)
- X Window

7. Brak ostrożności przy protokołach bez uwierzytelniania

- DNS
- SMTP
- RIP
- ICMP Redirect
- Tryb source routing

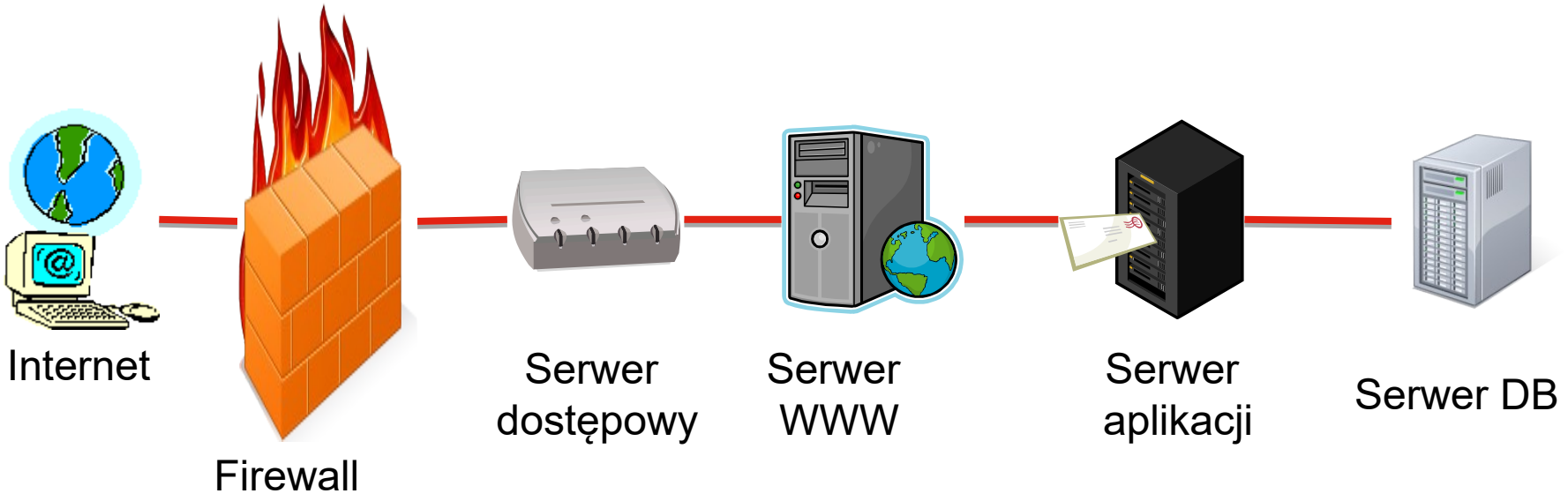
8. Brak ostrożności w obchodzeniu się z otrzymanym od innych oprogramowaniem

- Kod wykonawalny (konie trojańskie, wirusy)
- Aktywna zawartość (szczególna forma kodu wykonawczego, np. JavaScript, ActiveX, Java, makra, PostScript)
- Wstawianie danych do swoich skryptów (mogą zawierać specjalne znaki, ukryte komendy lub doprowadzać do przepełnienia bufora)

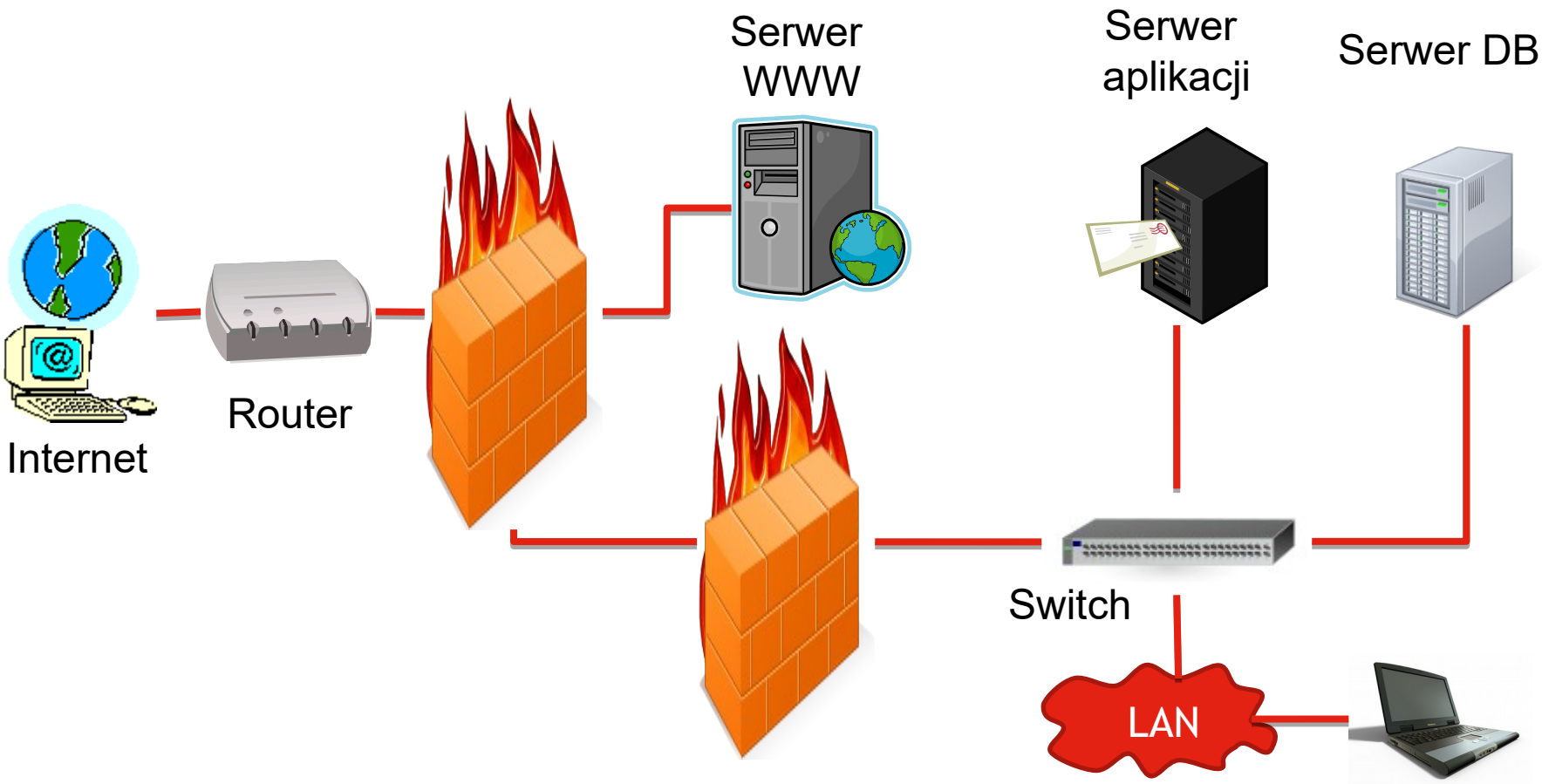
9. Nieodpowiedzialność producenta

- Pozostawione furtki w oprogramowaniu
- Brak wbudowanych zabezpieczeń
- Słaba kryptografia, wykorzystanie kluczy 40-bitowych

Umiejscowienie BD - przykład 1.



Umiejscowienie BD - przykład 2.



Umiejscowienie BD – sieci wirtualne

Tunelowanie:

1. z wykorzystaniem IPSec,
2. z wykorzystaniem SSL (przezroczyste dla zapory).

VPN (Virtual Private Network) – wirtualna sieć prywatna korzysta z publicznej infrastruktury telekomunikacyjnej, protokołów tunelowania i procedur bezpieczeństwa danych (Uwaga: wykorzystywana również w ramach LAN do odseparowania fragmentu sieci).

Fizyczne zagrożenia

	1. Zdobycie fizycznego dostępu	2. Atak
Podstawowe	- Włamanie przez wyważenie drzwi, użycie łomu... - Przeczołganie się pod podniesioną podłogą, wzdłuż duktów kablowych lub przez przestrzeń międzysufitową - Otwarcie mechanicznego zamka, zdobycie lub skopiowanie kluczy - Aktywacja wewnętrznego przycisku otwierającego drzwi lub wsunięcie pod drzwi płytki w celu uaktywnienia sensora ruchu	Kradzież komputera, laptopa (np. na lotnisku), taśmy z kopią zapasową, dysków i zastąpienie ich niezapisanymi nośnikami - Użycie dysku startowego do zabezpieczonego systemu, hack NTFS2DOS.exe - Włamanie do szafek dystrybucyjnych w miejscach publicznych, a następnie podsłuchiwanie/ zniszczenie/inne działania - Przeszukiwanie śmieci w celu znalezienia dokumentacji papierowej - Odzyskiwanie dokumentów z niszczarek - Podglądanie, wykorzystanie dużych powiększeń fotograficznych, podsłuchiwanie wprowadzania numerów PIN
Zaawansowane	- Pokonanie systemu alarmowego, wrażliwego na ruch, z pasywnym detektorem IR (zmiany temperatury), mikrofalami (odbicia) - Wykorzystanie systemu identyfikatorów/czytnika kart/FOBS/ataku man-in-the-middle ze strojonymi obwodami LC pomiędzy „panelem" a „maszyną kontrolną" - Złamanie czytnika kart lub zduplikowanie kart relatywnie łatwe (12-bitowy kod osobisty, 8-bitowy kod instalacyjny) - Wykorzystanie błędnej weryfikacji przez system biometryczny (wady projektowe), złamanie czytnika odcisków palców, użycie powtórzeń	- Podsłuchiwanie łączy przewodowych oraz nagrywanie wideo i audio - Ataki z wykorzystaniem koni trojańskich (niewykrytych agentów) - Rejestrowanie użytkowania klawiatury, zastąpienie klawiatury podobnie wyglądającą klawiaturą rejestrującą lub przesyłającą sygnał radiowy - Fałszowanie kart elektronicznych, może być bardzo trudne - Wykorzystanie nadajnika radiowego, efektu van Ecka, przechwytywanie obrazu z monitora - Wykorzystanie wad BIOS-u (specjalne hasło, pewne kombinacje klawiszy) - Zdobycie prywatnych kluczy szyfrujących - z CA lub lokalnych, a następnie złamanie ich

SKŁADOWANIE, ARCHIWIZACJA I OCHRONA DANYCH

Zagrożenia

- Zagrożenia miejsca (budynku, pojazdu itp.)
  - huragan, trzęsienie ziemi, powódź itp.,
  - utrata zasilania, wojna terroryzm;
- Awarie sprzętu
  - uszkodzenia pamięci masowej (np. dysku),
  - błąd procesora,
  - niedziałająca infrastruktura sieciowa;
- Awaria logiczna
  - błędy oprogramowania,
  - wirusy, robaki, itp.
  - przypadkowe usunięcia danych.

Zagrożenia miejsca - wybrane techniki zapobiegania utratom danych:

- redundancja sprzętu – replika bazy danych wraz ze sprzętem na serwerze zapasowym (np. 30 km dalej),
- zasilacze UPS, własne generatory,
- monitorowanie i zabezpieczenie obiektów, systemy alarmowe itp.

Awarie sprzętu - wybrane techniki zapobiegania utratom danych:

- redundancja sprzętu,
- macierze RAID 1 (mirroring), RAID 5,
- backup i archiwizacja.

Błędy w oprogramowaniu - wybrane techniki zapobiegania utratom danych:

- takie, jak poprzednio,
- ochrona antywirusowa, aktualizacja oprogramowania, zapory sieciowe, itp.
- projektowanie, implementacja, testowanie i walidacja oprogramowanie metodami formalnymi

Archiwizacja

- Rodzaje backupów
  - pełny (ang. *full backup*),
  - przyrostowy (ang. *incremential backup*),
  - różnicowy (ang. *differential backup*)

  - lokalny
  - sieciowy

Przykłady urządzeń wykorzystywanych do archiwizacji:

- macierze dyskowe RAID,
- urządzenia taśmowe (ang. *streamer*)
- nośniki optyczne i magnetooptyczne

Macierze dyskowe

- pojemności dysków: do 14 TB
- macierze dyskowe RAID
  - RAID 0 (stripping)
  - RAID 1 (lustrzany)
  - RAID 2
  - RAID 3
  - RAID 4
  - RAID 5
  - RAID 6
  - RAID 0+1
  - RAID 1+0

RAID

Poziom RAID	Minimalna liczba dysków (N)	Dostępna przestrzeń	Max liczba dysków, które mogą ulec awarii
0	2	N	0
1	2	1	N-1
2	3	N-log N	1
3	3	N-1	1
4	3	N-1	1
5	3	N-1	1
6	4	N-2	2
0+1	4	zależnie od konfiguracji	zależnie od konfiguracji
1+0	4	zależnie od konfiguracji	zależnie od konfiguracji

Urządzenia taśmowe

- Strimer (ang. *streamer*);
- DDS (ang. *Digital Data Storage*) zapis skośny na taśmach muzycznych DAT (ang. *Digital Audio Tape*),
- DLT (ang. *Digital Linear Tape*),
- LTO (ang. *Linear Tape-Open*),
- AIT (ang. *Advanced Intelligent Tape*),
- QIC (ang. *Quarter Inch Cartridge*).

Urządzenia taśmowe - przykłady

- DAT (ang. *Digital Audio Tape*), np. DDS-6 80 GB, 5MB/s
- DLT (ang. *Digital Linear Tape*), np. SDLT600 300GB/600 GB, 36 MB/s
- LTO (ang. *Linear Tape-Open*), np. LTO-2 200/400GB; LTO-3 400/800 GB; LTO-4 800/1600 GB; LTO-5 1600/3200 GB; LTO-6 2500/6250 GB, 160 MB/s
- przyszłościowe: LTO-7 … LTO-10 do 48 TB,

Nośniki optyczne

- CD
  - pojemności: ok. 700 MB
- DVD
  - pojemności: 4,7 GB – 17,08 GB
- HD DVD
  - pojemności: 15 GB, 20 GB
- Blu-ray Disc (BD)
  - pojemności: 25 GB, 50 GB, 100/128 GB (BDXL)

Nośniki magnetooptyczne (MO)

- pojemności: 5,2 GB, 9,1 GB
- dysk z danymi jest umieszczony w specjalnej kasecie co pozwala na wydłużenia okresu archiwizacji nawet do 100 lat,
- dostępne także w wersji WORM (ang. *Write Once, Read Many*) – do jednorazowego zapisu; RW – wielokrotnego zapisu.

UWIERZYTELNIENIE I AUTORYZACJA

Uwierzytelnienie i autoryzacja

- **Uwierzytelnienie** – proces mający na celu identyfikację klientów aplikacji, np. użytkowników końcowych, usług, procesów lub komputerów
- **Autoryzacja** – proces mający na celu ustalenie, które zasoby i operacje powinny być dostępne danemu uwierzytelnionemu klientowi. Dotyczy to zasobów takich jak pliki, bazy danych, zasoby systemowe.

Uwierzytelnienie i autoryzacja (2)

- Mechanizmy uwierzytelnienia i autoryzacji są różne i zależą od konkretnego SZBD
- Zazwyczaj użytkownicy dzieleni są na **grupy** natomiast grupom nadawane są określone **uprawnienia**
- Ponadto niezbędnym dobrym nawykiem administratora baz danych powinno być rejestrowanie i monitorowanie zdarzeń na serwerze w poszukiwaniu nietypowych zdarzeń

Podstawy szyfrowania

- Szyfrowanie z kluczem prywatnym
- Szyfrowanie z kluczem publicznym
- Podpis cyfrowy
- Certyfikaty cyfrowe

Pytania?

DZIĘKUJĘ ZA UWAGĘ