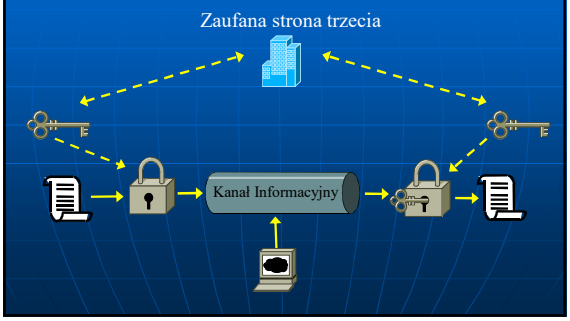
Dotychczasowe wykłady

- Poufność
- Integralność
- Dostępność
- Uwierzytelnianie
- Rozliczalność
- Niezaprzeczalność
- Kontrola dostępu
- Dystrybucja kluczy

Dystrybucja kluczy

Key distribution

Model ochrony danych w sieci komputerowej



Dystrybucja kluczy - symetryczne

W jaki sposób dostarczyć klucz drugiej stronie, tak aby nie wpadł w ręce osób postronnych ?

- Wręczyć osobiście (dyskietka, CD, USB)
- Wykorzystać zaufaną osobę/instytucję
- Przesłać nowy klucz szyfrując poprzednim
- Wykorzystać zaufaną osobę/instytucję, z którą obie strony mają szyfrowane łącze

Liczba kluczy w Szyfr. Sym.

- Dla *N* stron, liczba kluczy wynosi

$$\frac{N \cdot (N-1)}{2}$$

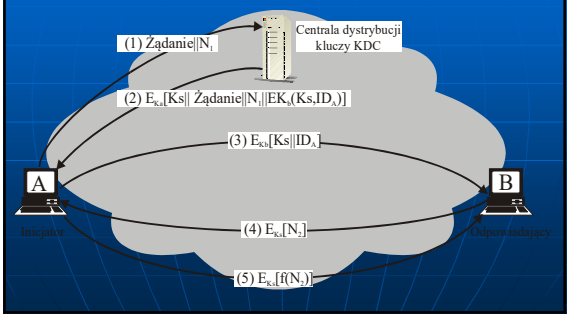
Liczba kluczy rośnie, jeśli strony komunikują się na poziomie programów.

- Hierarchia kluczy
  - Klucz sesji
  - Klucz główny

Dystrybucja tajnych kluczy w praktyce

1. Klucz główny – współdzielony klucz tajny (alg. symetryczny) lub komplet kluczy jawny-prywatny
   Klucz sesji – klucz tajny (alg. symetryczny)
2. Metoda Diffiego-Helmana (DH)

Key Distribution Center



Wymiana kluczy Diffiego-Hellmana

- Algorytm D-H umożliwia bezpieczną wymianę tajnego klucza bez żadnych warunków wstępnych (bezpiecznego kanału dystrybucji, kryptografii asymetrycznej, użycia poprzednich kluczy, współdzielonych sekretów)
- Tajny klucz jest obliczany niezależnie przez obie komunikujące się strony

Algorytm Diffiego-Hellmana

Globalne elementy jawne

q – liczba pierwsza,

$\alpha < q$ – pierwiastek liczby q

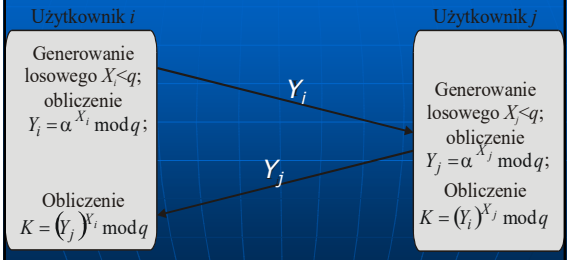
Generowanie kluczy użytkowników i oraz j

1. Wybór prywatnych $X_i < q$ $X_j < q$
2. Wyliczenie jawnych $Y_i = \alpha^{X_i} \bmod q$ $Y_j = \alpha^{X_j} \bmod q$

Generowanie klucza tajnego

$$K = (Y_j)^{X_i} \bmod q = (Y_i)^{X_j} \bmod q$$

Algorytm Diffiego-Hellmana



DK w schemacie asymetrycznym

- Klucza prywatnego nie przesyłamy
- Klucz jawny (publiczny) jest jawny, nie ma potrzeby utajniania podczas dystrybucji

Dystrybucja kluczy publicznych

W jaki sposób przekazać drugiej stronie klucz publiczny ?

- Wysłać e-mailem
- Umieścić na stronie WWW
- Wydrukować w gazecie
- …

Czy możemy 'ufać' tak otrzymanemu kluczowi ?

Dystrybucja kluczy publicznych

Metody:

- Publiczne ogłoszenie
- Ogólnie dostępny katalog
- Organ zarządzający kluczami jawnymi
- Certyfikaty kluczy jawnych
- Odcisk palca (fingerprint)

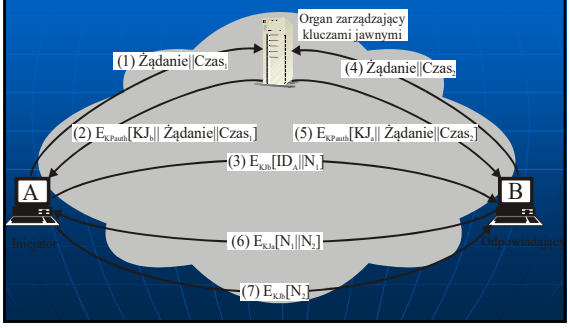
Ogólnie dostępny katalog

- Organ zarządzający utrzymuje katalog, z pozycjami {*nazwa, klucz jawny*}
- Każdy uczestnik rejestruje klucz jawny u osobiście lub w formie uwierzytelnionego przekazu
- Uczestnik może w każdej chwili zmienić klucz na nowy
- Okresowo zarządzający publikuje (lub uaktualnia) cały katalog
- Dostęp do katalogu także drogą elektroniczną za pomocą bezpiecznej, uwierzytelnionej komunikacji

Ogólnie dostępny katalog - wady

- Awaria katalogu
- Katalog może się okazać 'wąskim gardłem' (*bottleneck*)
- Kompromitacja całego katalogu w przypadku wykradzenia klucza prywatnego zarządcy katalogu

Organ zarządzający kluczami jawnymi



Organ zarządzający kluczami jawnymi - wady

- Awaria
- 'Wąskie gardło'
- Kompromitacja w przypadku wykradzenia K_{Pauth}

Certyfikat klucza jawnego

Certyfikat to dokument elektroniczny zawierający:

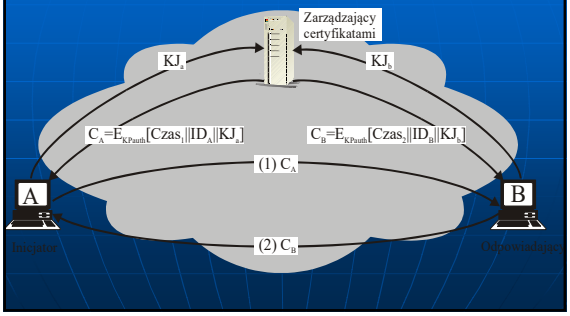
- Nazwę właściciela klucza
- Klucz jawny
- Termin ważności klucza

Podpisany przez wystawcę certyfikatu

Certification Authority

- Organy wydające certyfikaty (CA) są instytucjami zaufania publicznego
- Certyfikat można uzyskać po potwierdzeniu swojej tożsamości
- Istnieją certyfikaty różnego rodzaju, m.in. certyfikat klucza publicznego, certyfikat SSL

Komunikacja z certyfikatem



Hierarchia certyfikatów

Co zrobić, jeżeli nie znamy CA, który wydał certyfikat?

Należy pobrać certyfikat CA i za jego pomocą potwierdzić tożsamość CA. Certyfikat CA jest wydawany przez CA wyższego poziomu

Co zrobić, jeżeli nie znamy CA wyższego poziomu, który wydał certyfikat dla CA?

…

Algorytm hybrydowy (pełny)

- Dane są szyfrowane algorytmem symetrycznym z kluczem sesji
- Zapewniona integralność (funkcja hashująca, podpis cyfrowy)
- Klucze sesji są przesyłane w postaci zaszyfrowanej (alg. asymetryczny) lub uzgadniane metodą D-H

Odcisk palca (*fingerprint*)

- Skrót (najczęściej SHA) klucza, zapisany szesnastkowo
- Po wygenerowaniu odcisku można się skontaktować z właścicielem klucza celem weryfikacji
- Odcisk palca można np. umieścić na wizytówce lub opublikować
- Wyliczany automatycznie przez aplikacje kryptograficzne i przeglądarki

Fingerprint - przykłady

Klucz z certyfikatu NCCert:

Skrót danych służących do walidacji danych powiązanych z certyfikatem Narodowego Centrum Certyfikacji wystawionym w 2016 r. (NCCert2016):

29b3 c8c4 dfa3 87f8 6605 1258 fd46 2ab8 980d 7987

Klucz z certyfikatu e.pwr.edu.pl:

Odciski

Odcisk SHA-256	03:79:A5:98:39:6F:94:2B:38:FC:55:FA:6F:46:C2:56:87:DD:14:93:AA:EA:D9:85:77:F4:8D:9D:AE:ED:E0:C4
Odcisk SHA1	EB:43:9F:55:6F:91:0B:F5:5F:1B:08:A6:BD:18:67:63:57:E4:65:C7

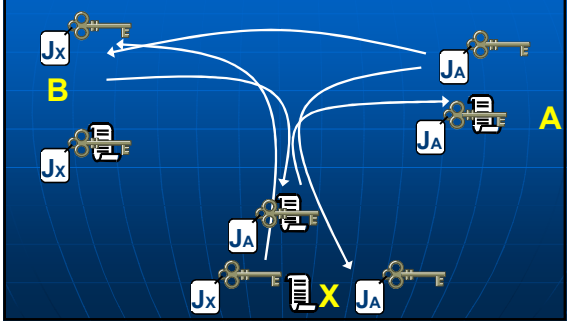
Klucz serwera SSH (w putty):

The server's rsa2 key fingerprint is:
ssh-rsa 1024 1e:d6:0d:f2:c6:eb:cf:ff:e4:cd:e3:e1:b3:fd:46:ec

Infrastruktura klucza publicznego

Public Key Infrastructure (PKI)

Podrabianie klucza publicznego



PKI

Zbiór standardów, norm i procedur zapewniających autentyczność kluczy komunikujących się stron

System urzędów certyfikacji (Zaufana strona trzecia – agenda rządowa, instytucja, akredytowana firma, komórka organizacyjna)

PKI

- Standardy: ITU X.509, RSA PKCS, IETF PKIX
- Urzędy certyfikacji (CA), urzędy rejestracji (RA)
- Certyfikaty cyfrowe, szablony certyfikatów cyfrowych
- Listy odwołania certyfikatów (CRL)

Standard ITU X.509 v3

- Formaty danych
- Procedury dystrybucji
- Weryfikacja ścieżek certyfikacji
- Normy dot. CRL

Infrastruktura klucza publicznego

- Nadrzędny urząd certyfikacji
- Podrzędny urząd certyfikacji (możliwe poziomy)
- Urząd rejestracji

Nadrzędny CA

- Najważniejszy z urzędów w PKI organizacji
- Pracuje w trybie *off-line*
- Wystawia certyfikat dla siebie oraz dla podrzędnych CA

Podrzędny CA

- Podlega nadrzędnemu CA
- Wydaje certyfikaty odbiorcom końcowym lub podrzędnym CA niższego poziomu

Urząd rejestracji (RA)

- Działa na podstawie upoważnienia podrzędnego CA
- Odpowiada za weryfikację podmiotu ubiegającego się o certyfikat
- Wnioskuje do CA o wystawienie certyfikatu

Rodzaje certyfikatów

- Certyfikat kwalifikowany – spełnia warunki określone w ustawie o podpisie elektronicznym, wystawiony przez podmiot wpisany do rejestru
- Certyfikat niekwalifikowany

CRL

- Lista certyfikatów unieważnionych przed datą wygaśnięcia
- Przypadki
  - Utrata klucza prywatnego
  - Ujawnienie klucza prywatnego
  - Zastąpienie certyfikatu nowym

Budowa certyfikatu X.509

- Wersja (0-2)
- Nr seryjny – unikalny w ramach CA
- Algorytm sygnatury
- Data ważności
- Dane wystawcy
- Dane użytkownika
- Klucz publiczny

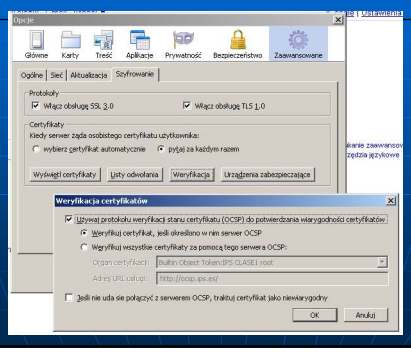
Budowa certyfikatu X.509 - rozszerzenia

- Krytyczne i niekrytyczne
- Czy klucz CA czy użytkownika
- Do czego może być wykorzystywany klucz
- Zasady wykorzystania klucza
- Dostępność CRL

PKI - protokoły

- Online Certificate Status Protocol (OCSP)
- Wezwanie - odpowiedź
- Jako protokół transportowy może być użyty HTTP (metoda GET)
- Do sprawdzania statusu certyfikatu (ważny, unieważniony, nieznany)
- Formaty wniosków: PKCS#10 lub CRMF

OCSP w praktyce



PKI - protokoły

- Certificate Management Protocol (CMP)
- Wydawanie certyfikatów (wnioski i odpowiedzi)
- Unieważnianie certyfikatu
- Dostarczanie CRL
- Certyfikacja krzyżowa pomiędzy CA

PKI a prawo w Polsce

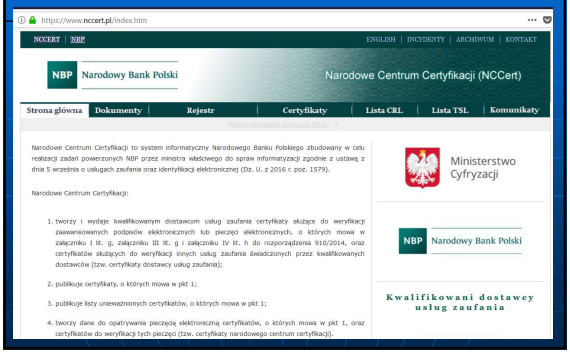
Ustawa z dnia 18.IX.2001 o podpisie elektronicznym:

- Warunki stosowania podpisu elektronicznego
- Skutki prawne
- Zasady świadczenia usług certyfikacji
- Zasady nadzoru nad CA

Rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne

https://www.nccert.pl

www.nccert.pl



NCCert

- Podstawowe informacje ze strony NCCert obowiązują na kolokwium:
  - Ile certyfikatów wykorzystuje NCCert ? W których latach zostały wystawione ?
  - Ilu kwalifikowanych dostawców jest autoryzowanych przez NCCert ?
  - Od kiedy w certyfikatach nie stosuje się SHA-1 ?
  - Co to jest lista TSL ?

Uwierzytelnienie

Identyfikacja

Metody weryfikacji tożsamości

- **Coś, co znasz** (*something you know*)
  Hasła, identyfikatory, numery PIN, ...
- **Coś, co posiadasz** (*something you own*)
  karta magnetyczna, karta chipowa, klucz do drzwi, ...
- **Coś, czym się charakteryzujesz** (*something you are*)
  linie papilarne, geometria twarzy, tęczówka oka, charakterystyka głosu, ręczny podpis, kod DNA, zapach, cechy behawioralne, ...

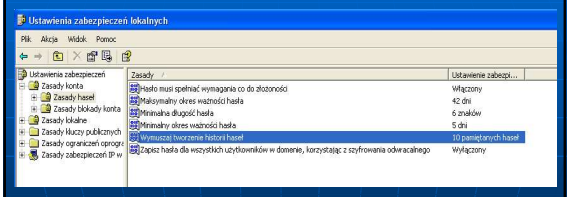
Ochrona haseł

- Hasła przechowywane są w postaci zaszyfrowanej lub hashowanej
- Ataki na hasła: brutalny, kradzież, konie trojańskie, podsłuchiwanie.
- Wymuszanie skomplikowanych haseł poprawia poziom bezpieczeństwa (i utrudnia użytkownikom korzystanie z systemu ;-).

Bezpieczeństwo haseł

- Dołączanie do hasła tzw. „domieszek".
- Wymuszanie na użytkownikach odpowiedniej długości haseł.
- Wymuszanie na użytkownikach czasowej zmiany haseł.
- Generatory haseł, tokeny.
- Aktywne sprawdzanie haseł.
- Hasła jednorazowe.
- Frazy

Przykład – Windows Server



Biometria

- Zautomatyzowane techniki identyfikacji lub uwierzytelniania osób z wykorzystaniem ich charakterystyki fizjologicznej lub behawioralnej
- Identyfikacja: jeden do wielu
- Uwierzytelnianie/weryfikacja: jeden do jednego

Biometryka

Nauka o mierzalnych cechach fizycznych lub behawioralnych organizmów żywych, znajdująca zastosowanie w systemach kontroli dostępu

„bios" -> żywy, „metron" -> mierzyć

Biometryka

Które cechy fizyczne można wykorzystać do identyfikacji ?

- Uniwersalność
- Unikatowość
- Trwałość
- Mierzalność

Biometria

- siatkówka
- tęczówka
- linie papilarne
- geometria twarzy
- układ żył w dłoni lub palcu
- geometria dłoni
- głos
- dynamika podpisu
- dynamika chodu
- …

Linie papilarne

- Cechy mierzalne
  - ogólny wzór linii papilarnych
  - nieregularny kształt krawędzi
  - kształt i rozmieszczenie porów
  - minucje (linie, oczka, rozwidlenia, kropki)
- Wymagana jest określona minimalna liczba cech wspólnych

Geometria twarzy

- Do pobrania próbki wystarczy kamera
- Na bazie punktów charakterystycznych budowany jest trójwymiarowy model

Geometria dłoni

- Zdjęcie dłoni - wykonywane na specjalnym panelu
- Wyznaczenie około 40 geometrycznych cech dłoni
- Problemy w przypadku ran i blizn

Geometria dłoni

Siatkówka

- Skanowanie warstwy naczyń krwionośnych oplatających dno oka
- Niezmienność wzoru siatkówki
- Wymaga zdjęcia okularów
- Brak metod spreparowania fałszywej siatkówki

Tęczówka

- Analiza cech kolorowej tkanki otaczającej źrenicę
- Bardzo duża liczba punktów charakterystycznych (ok. 260) – unikatowość cechy w całej populacji
- Odporność na 'sztuczne oko'
- Niezmienność w czasie
- Ważne cechy zanikają 5 sekund po śmierci
- Odporność na wpływy zewnętrzne
- Czas identyfikacji: ok. 2 sekund

Tęczówka

Ograniczenia metody:

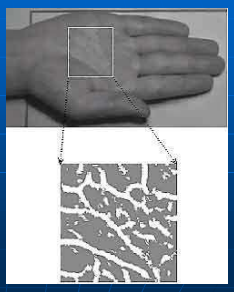
- Akceptowalność / obawa przed badaniem
- Duża porcja danych opisujących tęczówkę
- Problemy w przypadku wad wzroku (np. katarakta)

Układ żył

- Rozmieszczenie naczyń krwionośnych jest unikalne dla każdego człowieka
- Żyły są umieszczone pod powierzchnią skóry - nie ulegają zniszczeniu
- Metoda łatwo akceptowalna
- Czas badania poniżej 2 sekund

Pomiar układu żył

- Absorpcja promieni podczerwonych przez krew



Zalety i wady biometrii

- Wysoka niezawodność
- Nie trzeba nic pamiętać/posiadać
- Liczne zastosowania w kontroli dostępu (drzwi, bramki, komputery, sejfy, …)
- Co w przypadku kradzieży tożsamości biometrycznej ?
- Problem akceptowalności
- Obawa przed nieuprawnioną identyfikacją (np. z kamer miejskiego monitoringu)

Protokoły uwierzytelniania

Mechanizm pojedynczego logowania

Single Sign-On (SSO):

- Skrypty automatycznego logowania
- Enterprise Access Management (EAM) – np. Cookies
- Serwer uwierzytelniania (Kerberos)

Kerberos

- Protokół uwierzytelniający
- Wykorzystuje kryptografię symetryczną
- Infrastruktura:
  - Centrum dystrybucji kluczy (KDC)
  - Usługa przyznawania biletów (TGS)
  - Usługa uwierzytelniania (AS)

Kerberos – idea działania

1. Serwer Kerberos współdzieli tajne klucze z użytkownikami i serwerami usług
2. Klient uwierzytelnia się przed serwerem Kerberos (raz – na określony czas)
3. Klient prosi o połączenie z serwerem usług
4. Kerberos zestawia bezpieczną sesję pomiędzy użytkownikiem a serwerem usług
5. Koniec pracy lub skok do punktu 3.

Uwierzytelnianie w Kerberos (1)

1. Klient loguje się na stacji roboczej, hash hasła klienta jest kluczem do szyfrowania transmisji klient<->AS (K_{K-AS})
2. Klient wysyła zgłoszenie do AS (nie szyfrowane)
3. AS odnajduje w bazie klucz współdzielony z klientem (lub wykonuje hashowanie hasła klienta)

Uwierzytelnianie w Kerberos (2)

4. AS wysyła do klienta:
   - K_{K-AS} (K_{K-TGS})
   - K_{TGS} (ID_K, $Addr_K$, $Czas_T$, K_{K-TGS}) – *Ticket Granting Tickets*
5. Klient deszyfruje pierwszą wiadomość i uzyskuje bezpieczny kanał z TGS. Klucz K_{K-TGS} jest ważny w czasie ważności $Czas_T$

Żądanie dostępu do serwera usług

1. Klient wysyła do TGS:
   - TGT, ID_S
   - K_{K-TGS} (ID_K, Czas) - autentykator
2. TGS wysyła do Klienta:
   - K_{S-TGS} (ID_K, $Addr_K$, $Czas_T$, K_{K-S}) – *client-to-server-ticket*
   - K_{K-TGS} (K_{K-S})

Dostęp do serwera usług

1. Klient wysyła do Serwera:
   - K_{S-TGS} (ID_K, $Addr_K$, $Czas_T$, K_{K-S})
   - K_{K-S} (ID_K, Czas) - autentykator
2. Serwer akceptuje żądanie:
   - K_{K-S} (Czas + 1)
3. Bezpieczna sesja szyfrowana kluczem sesji K_{K-S}

Wady Kerberos

- Pojedynczy punkt awarii (AS, TGS)
- Wszystkie hasła przechowywane są na AS i TGS
- Konieczność synchronizacji zegarów
- Możliwość nielegalnego wykorzystania przechwyconego biletu w określonym czasie
- Hasło klienta jest tymczasowo przechowywane na stacji roboczej
- Brak jednego standardu Kerberos

Kontrola dostępu zdalnego

- Oddzwanianie
- Password Authentication Protocol
- Challenge Handshake Authentication Protocol
- Extensible Authentication Protocol
- RADIUS
- TACACS, TACACS+ (Cisco)

Password Authentication Protocol

- Działanie PAP:
  1. Użytkownik przesyła identyfikator i hasło - w postaci jawnej
  2. Dane są porównywane z informacją w bazie
- Podatność na przechwycenie
- Używany na łączach dostępowych
- Nie wymaga protokołu L3

CHAP

Challenge Handshake Authentication Protocol:

1. Użytkownik nawiązuje połączenie i przesyła identyfikator
2. Serwer przesyła wyzwanie (*challenge*)
3. Użytkownik przesyła odpowiedź, serwer porównuje ją z samodzielnie wyliczoną
4. Etapy 2 i 3 są cyklicznie powtarzane podczas sesji

Wyzwanie CHAP

- Obliczenia z wykorzystaniem funkcji hashującej, np.:
  1. utwórz liczbę L z drugiego i czwartego znaku hasła,
  2. oblicz: M = L * 273654 mod 3745,
  3. oblicz skrót: MD5(M)
- Wyzwania powinny być unikalne i nieprzewidywalne
- Wyliczenie hasła na podstawie znanych wyzwań i odpowiedzi musi być niemożliwe

EAP

- Architektura:
  - Suplikant (klient)
  - Autentykator (urządzenie dostępowe)
  - Serwer uwierzytelniający
- Około 40 metod uwierzytelniania:
  - MD5 Challange (jak CHAP)
  - One Time Password
  - Generic Token Card
  - Kryptografia asymetryczna

RADIUS

- *Remote Authentication Dial In User Service*
- Połączenia telefoniczne, VPN, WiFi
- Protokół 3A
  - Authentication (uwierzytelnianie)
  - Authorization (autoryzacja)
  - Accounting (kontrola dostępu do usług)

RADIUS

- Architektura:
  - Serwer dostępu sieciowego
  - Klient
  - Serwer Radius (może współpracować z Kerberos, LDAP, ActiveDirectory)
  - Protokoły: PAP, CHAP lub EAP
- Serwer dostępu nie musi znać ani rozumieć metod uwierzytelniania