Polityka bezpieczeństwa

Marcin Szeliga
marcin@wss.pl

Agenda

- **Dlaczego polityka bezpieczeństwa jest nieskuteczna?**
  - Bezpieczeństwo jako proces
- **Socjotechnika**
- **Uwierzytelnianie**
- **Autoryzacja**

Dlaczego polityka bezpieczeństwa jest nieskuteczna?

- Zabezpieczenia przeszkadzają użytkownikom

Dlaczego polityka bezpieczeństwa jest nieskuteczna?

- **Zabezpieczenia w najlepszym wypadku odbierane są przez użytkowników jak niepotrzebny bagaż, w najgorszym – jako przeszkoda w wykonywaniu codziennej pracy**
  - Nic nie wnoszą
  - Utrudniają wymianę informacji
- **Użytkownicy nie chcą czekać na program**
  - W którymś momencie nasza cierpliwość się kończy
- **Użytkownicy nie chcą powtarzać nudnych, podatnych na błędy operacji**
  - Ile razy w ciągu godziny można wpisywać hasło?

Dlaczego polityka bezpieczeństwa jest nieskuteczna?

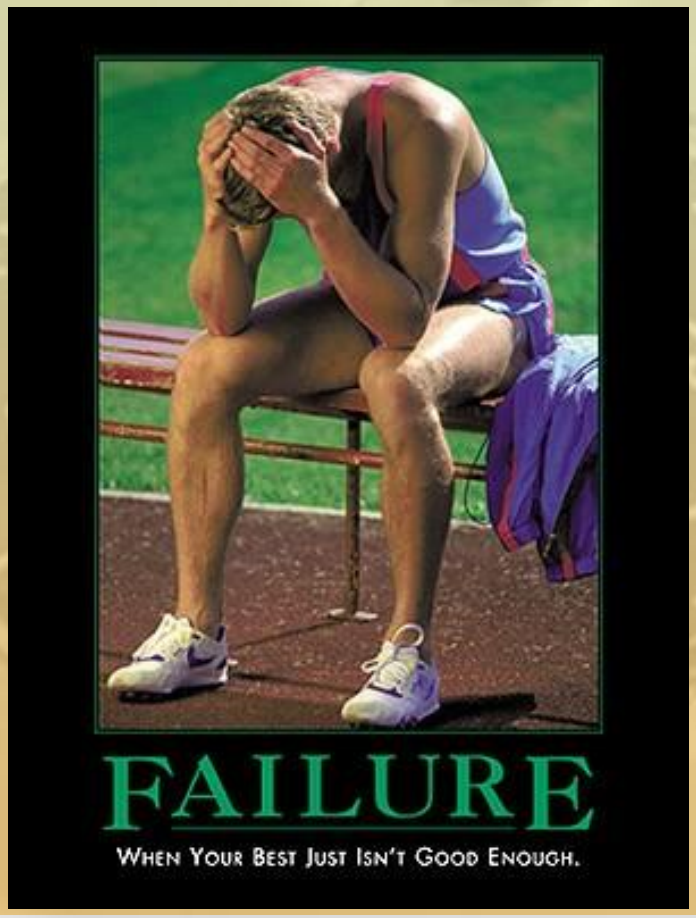
- Zasady bezpieczeństwa w świecie IT nie są wrodzone

Dlaczego polityka bezpieczeństwa jest nieskuteczna?

- **Użytkownicy muszą opanować zasady używania systemów komputerowych, nie zasady ich działania**
  - Jak mają się nauczyć unikać nieznanych zagrożeń?
  - Jak mogą ocenić ryzyko?
  - „Te reguły są bez sensu”
- **To samo dotyczy kierowników i dyrektorów**

Dlaczego polityka bezpieczeństwa jest nieskuteczna?

- Startujemy z trudnej pozycji …



Dlaczego polityka bezpieczeństwa jest nieskuteczna?

- **Musimy obronić się przed inteligentnym atakującym:**
  - Któremu wystarczy znaleźć jeden słaby punkt
  - I który może zautomatyzować atak, tak że będą go mogli przeprowadzić mniej inteligentni atakujący
- **Codziennie należy spodziewać się niespodziewanego:**
  - Jeżeli nic się nie dzieje, to znaczy, że czegoś nie zauważyliśmy
- **Administrator musi być na bieżąco:**
  - Szkolenia, listy mailingowe, subskrypcje …

Dlaczego polityka bezpieczeństwa jest nieskuteczna?

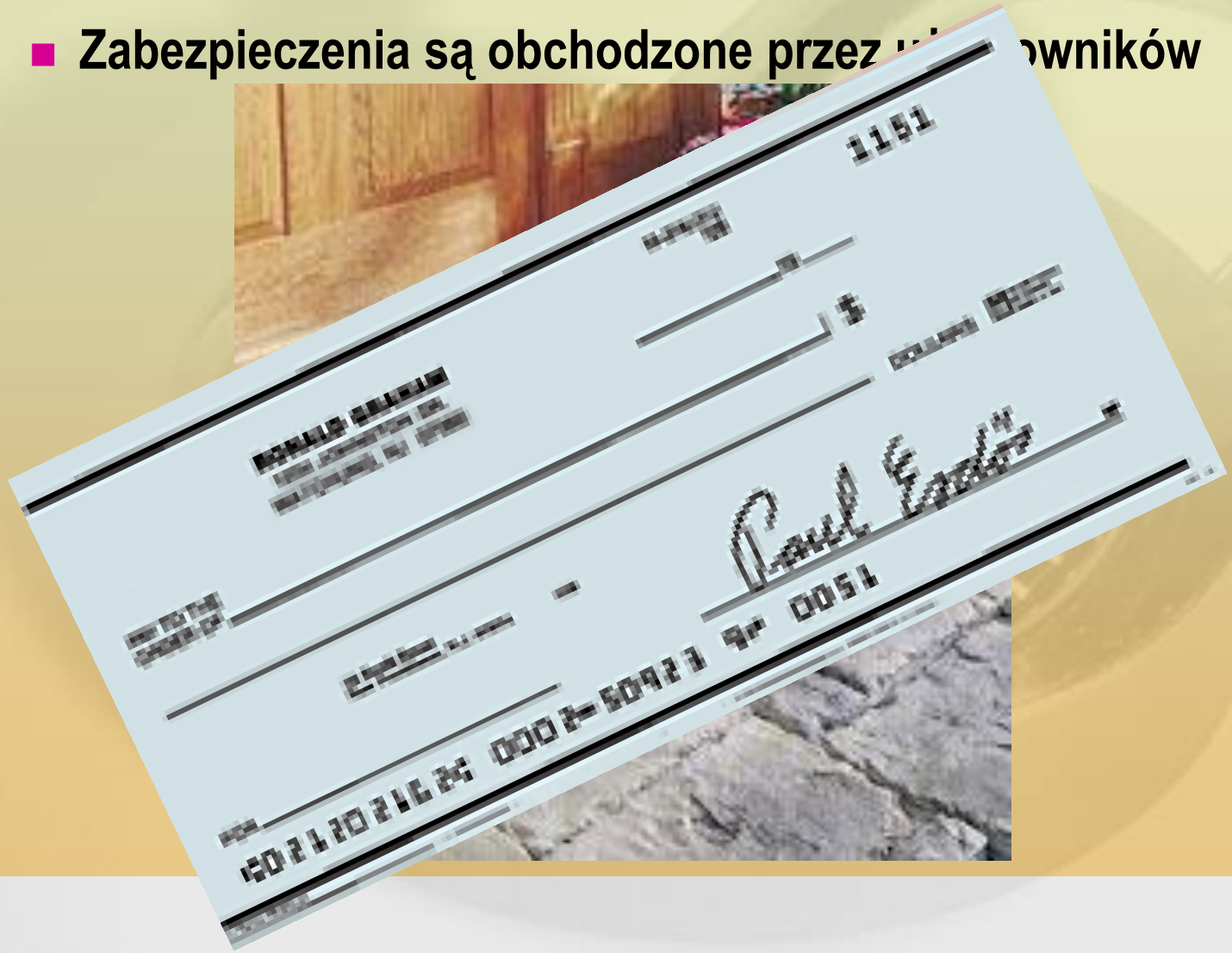
- Nie ma zabezpieczeń absolutnych

Dlaczego polityka bezpieczeństwa jest nieskuteczna?

- **Nawet wyłączony komputer nie jest w 100% bezpieczny**
- **Bezpieczeństwo wymaga ciągłej pracy**
  - Zmieniają się technologie
  - Pojawiają się nowe zagrożenia
- **Polityka bezpieczeństwa musi być na bieżąco aktualizowana**

Dlaczego polityka bezpieczeństwa jest nieskuteczna?

- Zabezpieczenia są obchodzone przez u[illegible]owników



Dlaczego polityka bezpieczeństwa jest nieskuteczna?

- **Niepraktyczna, rygorystyczna polityka bezpieczeństwa przynosi odwrotny skutek od zamierzonego**
  - Uwzględnienie informacje od użytkowników
  - Użytkownicy powinni wiedzieć, czemu służy polityka bezpieczeństwa
  - I wiedzieć, czym może grozić jej nieprzestrzeganie
- **Przestrzeganie polityki musi być ciągle monitorowane**
- **Polityka bezpieczeństwa często jest podstawą do wniesienia oskarżenia**

Dlaczego polityka bezpieczeństwa jest nieskuteczna?

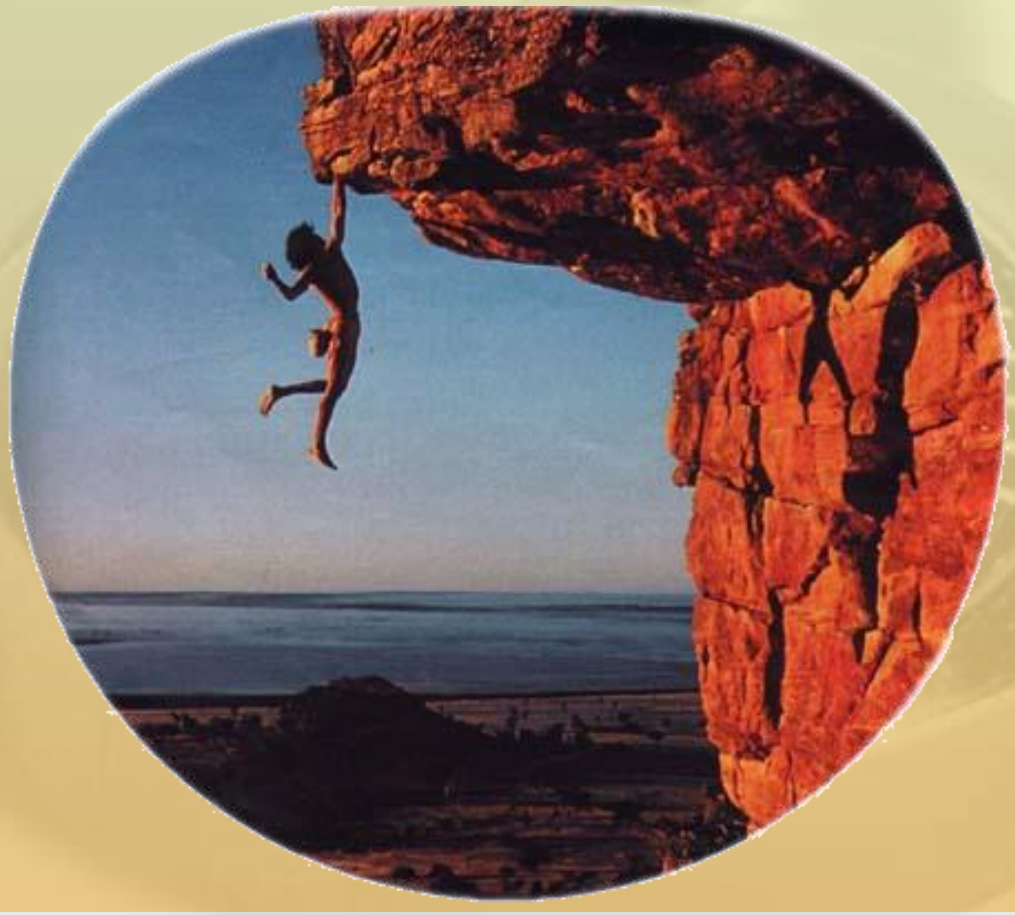
- Zachęca do jej nieprzestrzegania

Socjotechnika

- **Przekonanie osoby, żeby zrobiła dla nas to, co chcemy**
  - Ale co nie odbiega zbytnio od jej codziennych obowiązków
- **Atak wymierzony w ludzi**
  - Omija wszystkie zabezpieczenia
- **Ludzie są podatni na manipulację!**

Socjotechnika

- Nie potrafimy właściwie ocenić ryzyka



Socjotechnika

- **Przeceniamy ryzyko związane z:**
  - Zjawiskami i rzeczami których nie rozumiemy lub które są poza naszą kontrolą
  - Które są rozpowszechniane w mediach
- **Nie doceniamy ryzyka związanego z:**
  - Rzeczami codziennymi i przyziemnymi
  - Regularnie wykonywanymi operacjami
  - Zdarzeniami przytrafiającymi się naw w dobrze znanym otoczeniu

Socjotechnika

- **Jesteśmy pewni, że nic nam nie grozi**

Socjotechnika

- **Działamy rutynowo**
- **Przyzwyczailiśmy się do tego, że komputery są niezawodne:**
  - Za to ludzie często się mylą
- **Zareagowanie na alarm wymaga wiedzy, czasu i zaangażowania – najprościej jest go wyłączyć**
- **Polityka bezpieczeństwa często nie zawiera informacji, jak się zachować w nietypowych sytuacjach**

Socjotechnika

- **Ufamy komputerom**

Socjotechnika

- **To programy, a nie ludzie podpisują cyfrowo lub szyfrują dokumenty**
- **Przeniesienie zaufania z komputera na użytkownika i odwrotnie jest nadużyciem**
  - Jeden z najtrudniejszych problemów specjalistów od bezpieczeństwa systemów komputerowych
  - Komputer (i zapisane w nim hasła lub certyfikaty) może wpaść w niepowołane ręce
  - Na komputerze może działać (bez wiedzy użytkownika) wrogie oprogramowanie

Socjotechnika

Rozmycie odpowiedzialności

“Kowalski powiedział, że bierze wszystko na siebie…

Chęć zysku

“Możesz na tym nieźle wyjść!”

Nadużycie zaufania

“To swój człowiek, czemu nie miałbym mu pomóc?”

Presja moralna

“Musisz mi pomóc!”

Socjotechnika

Poczucie winy

“Nawet tego nie możesz dla mnie zrobić…”

Poczucie wspólnoty

“Tylko Ty mnie rozumiesz…”

Gotowość do pomocy

“Proszę, pomóż mi”

Gotowość do współpracy

“Zróbmy to razem!”

Socjotechnika

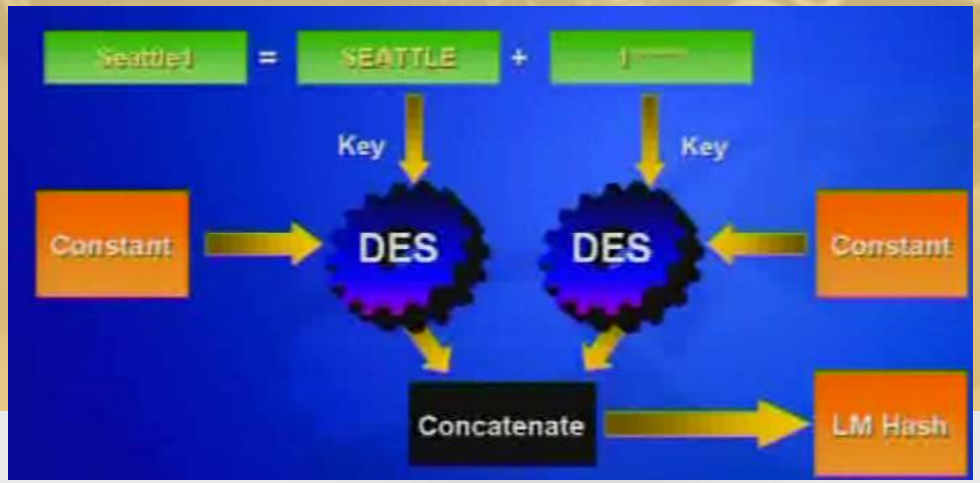
Area of risk	*Attacker tactic*	*Combat strategy*
Help desk	Impersonation and persuasion	Train employees to never give out passwords or other confidential info by phone
Building entrance	Unauthorized physical access	Tight badge security, employee training, and security officers present
Office	Shoulder surfing	Don't type in passwords with anyone else present (or if you must, do it quickly!)
Help desk	Impersonation on help desk calls	All employees should be assigned a PIN specific to help desk support
Office	Wandering through halls looking for open offices	Require all guests to be escorted
Mail room	Insertion of forged memos	Lock and monitor mail room
Machine room/Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment
Phone and PBX	Stealing phone toll access	Control overseas and long-distance calls, trace calls, refuse transfers
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas, shred important data, erase magnetic media
Intranet/ internet	Creation and insertion of mock software on intranet or internet to snarf passwords	Continual awareness of system and network changes, training on password use
Office	Stealing sensitive documents	Mark documents as confidential and require them to be locked
General—psychological	Impersonation and persuasion	Keep employees on their toes through continued awareness and training programs

Uwierzytelnianie

- **Uwierzytelnianie = potwierdzanie tożsamości**
  - Użytkownika (np. za pomocą sprawdzenia loginu i hasła)
  - Programu (np. za pomocą kluczy)
  - Informacji (np. za pomocą sprawdzenia dołączonej do niej sygnatury)

Uwierzytelnianie

- **Protokoły uwierzytelniania: LM**
  - Używany tylko systemach MS-DOS
  - Hasła LM dzielone są na dwie części, po siedem znaków każda. Następnie wszystkie litery obu części hasła konwertowane są na duże litery i tak zmodyfikowane hasło zostaje zaszyfrowane algorytmem DES



Uwierzytelnianie

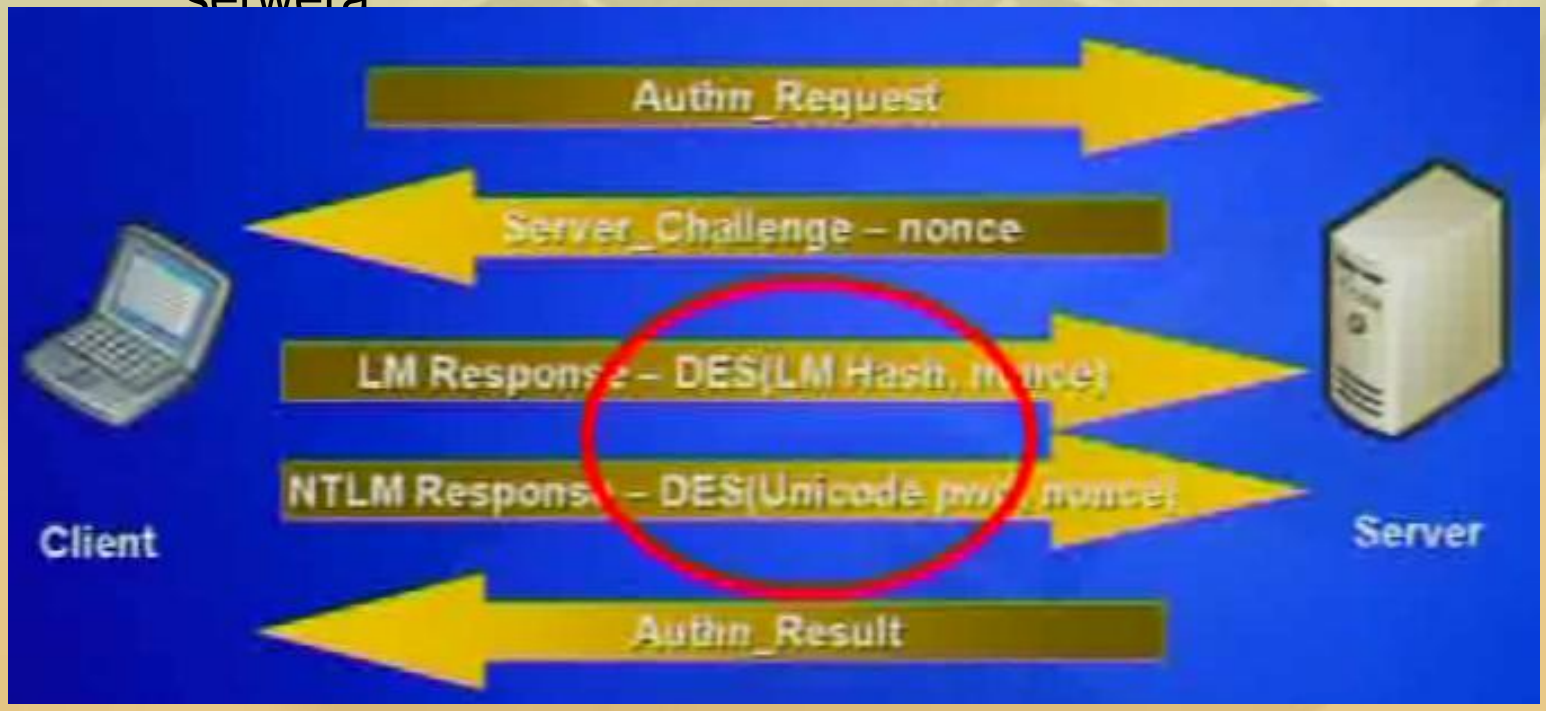
- **Protokoły uwierzytelniania: NTLM**
  - W ogóle nie powinien być używany
  - Hasła NTLM zostają zaszyfrowane algorytmem MD4 i zapisane w chronionym obszarze rejestru lokalnego systemu (maks. dł. 14 znaków)

Uwierzytelnianie

- **Protokoły uwierzytelniania: NTLMv2**
  - Używany tylko w systemach Windows 9x i NT
  - Hasła NTv2 zostają zaszyfrowane algorytmem MD5 przy użyciu klucza o długości 128 bitów i zapisane w chronionym obszarze rejestru lokalnego systemu

Uwierzytelnianie

- **Wymiana komunikatów wyzwania i odpowiedzi:**
  - Użytkownik próbuje uzyskać dostęp do zasobów serwera



Uwierzytelnianie

- **Przesyłanie hasła LM, czyli jak tego robić nie należy**
  - Klient wysyła do serwera losowy, 8 bajtowy komunikat wyzwania *0001020304050607*.
  - Serwer odczytuje hasło LM użytkownika i uzupełnia je pięcioma zerami *4EFC971E2C6A11F0AAD3B435B51404EE0000000000*
  - Otrzymany ciąg jest dzielony na trzy grupy po 7 bajtów: *4EFC971E2C6A11*, *F0AAD3B435B514* i *04EE0000000000*

Uwierzytelnianie

- **Przesyłanie hasła LM, czyli jak tego robić nie należy c.d.**
  - Otrzymane w ten sposób klucze wykorzystane są, po dodaniu bajtu parzystości, do zaszyfrowania algorytmem DES otrzymanego komunikatu wyzwania:
    - Tekst — *0001020304050607*, klucz — *4EFC971E2C6A11*, szyfrogram *AAAAAAAAAAAAAAAA*,
    - tekst — *0001020304050607*, klucz — *F0AAD3B435B514*, szyfrogram *BBBBBBBBBBBBBBBB*,
    - tekst — *304050607*, klucz — *04EE0000000000*, szyfrogram *CCCCCCCCCCCCCCCC*.
  - Otrzymane szyfrogramy są łączone (*AAAAAAAABBBBBBBBCCCCCCCC*) i wysyłane jako komunikat odpowiedzi do komputera klienckiego

Uwierzytelnianie

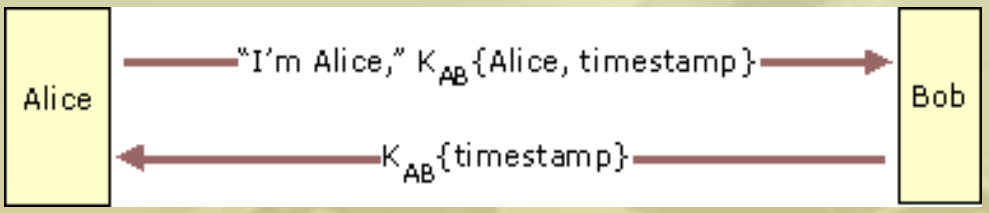
- **Przesyłanie hasła LM, czyli jak tego robić nie należy c.d.**
  - Komputer kliencki w taki sam sposób wylicza wartość komunikatu odpowiedzi i porównuje ją z odpowiedzią otrzymaną z serwera

Uwierzytelnianie

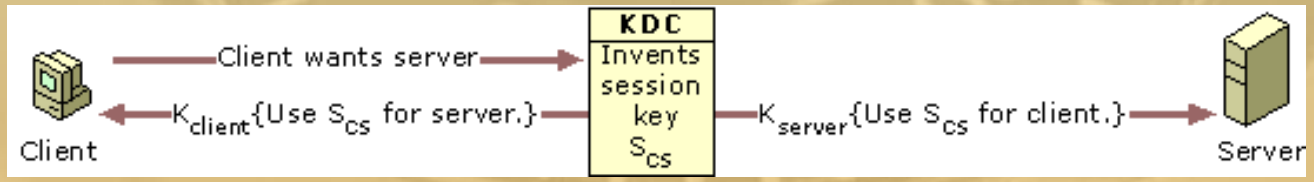
- **Kerberos został zdefiniowany w RFC 1510 i RFC 1964**
- **Do uwierzytelniania używane są:**
  - Wyprowadzone z hasła klucze długoterminowe lub certyfikaty
- **Tożsamość potwierdza bilet**
  - Bilet może być używany wielokrotnie, aż utraci ważność
- **Centrum dystrybucji kluczy (KDC):**
  - Przechowuje klucze długoterminowe i certyfikaty
  - Wydaje bilety TGT i bilety usług

Uwierzytelnianie

- **Wstępne uwierzytelnienie**

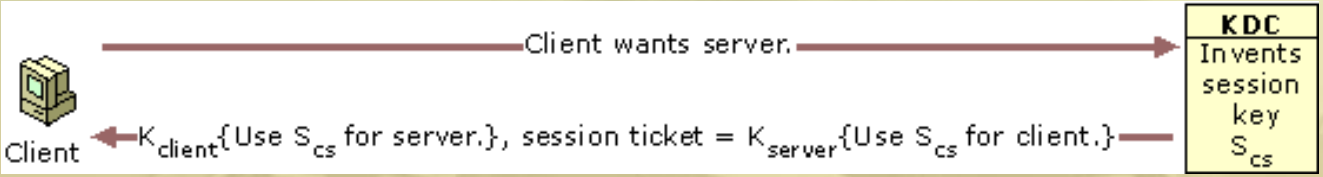


- **Problem: przechowywanie, wybór i wymiana klucza**
- **Rozwiązanie: zaufany serwer KDC przechowujący długoterminowe, wyprowadzone np. z hasła klucze**

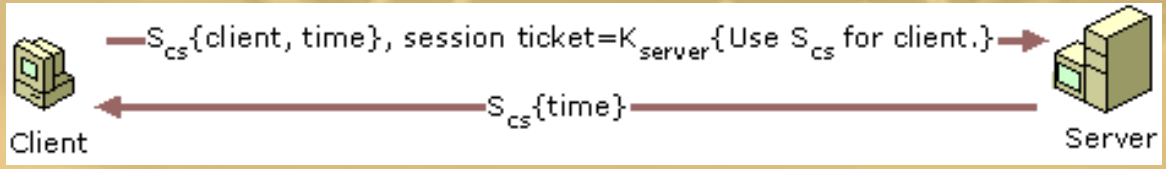


Uwierzytelnianie

- Proces uwierzytelniania Kerberos:
- Klient żąda „przepustki” (biletu usługi) do serwera



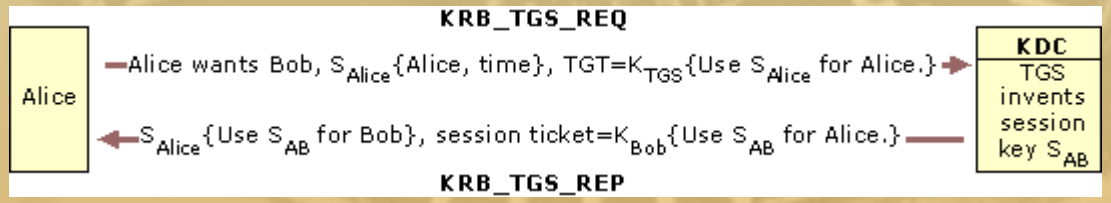
- Otrzymany bilet jest zapisywany buforze
- Jeśli klient żąda dostępu do serwera, wysyła mu bilet sesji i poświadczenie tożsamości



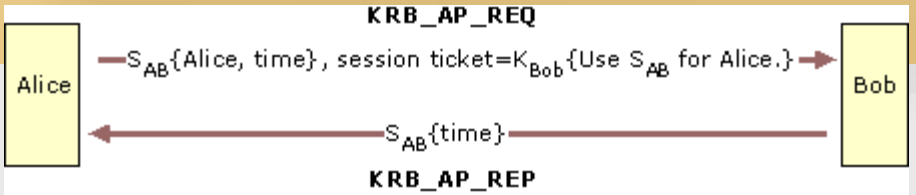
Uwierzytelnianie

- **Protokoły wymiany kluczy:**
  - Logowanie - Authentication Service (AS) Exchange

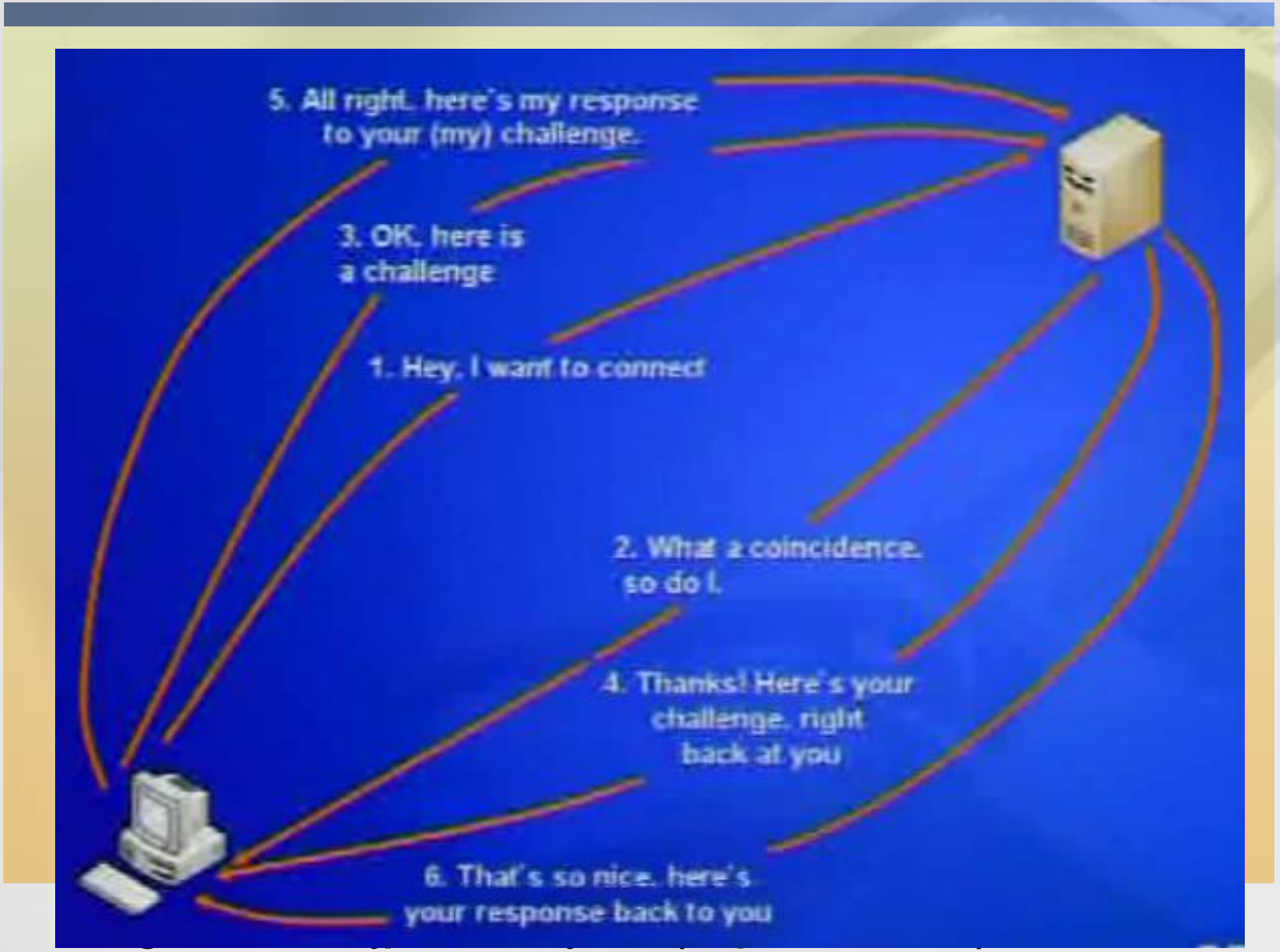
  - Dystrybucja *tickets* - Ticket-Granting Service (TGS) Exchange



  - Dostęp do usługi - Client/Server (CS) Exchange



Uwierzytelnianie



Autoryzacja

- **Autoryzacja = sprawdzanie, czy uwierzytelnione principium ma uprawnienia do wykonania operacji**
- **Główne rodzaje kontroli dostępu:**
  - Obowiązkowa (MAC) – obiekty są sklasyfikowane w hierarchii zabezpieczeń (tajne, poufne, publiczne) a użytkownicy otrzymują pewien poziom uprawnień
  - Uznaniowa (DAC) – uprawniania do obiektu nadaje jego właściciel
  - Przez role (RBAC) – uprawnienia są przyznawana rolą

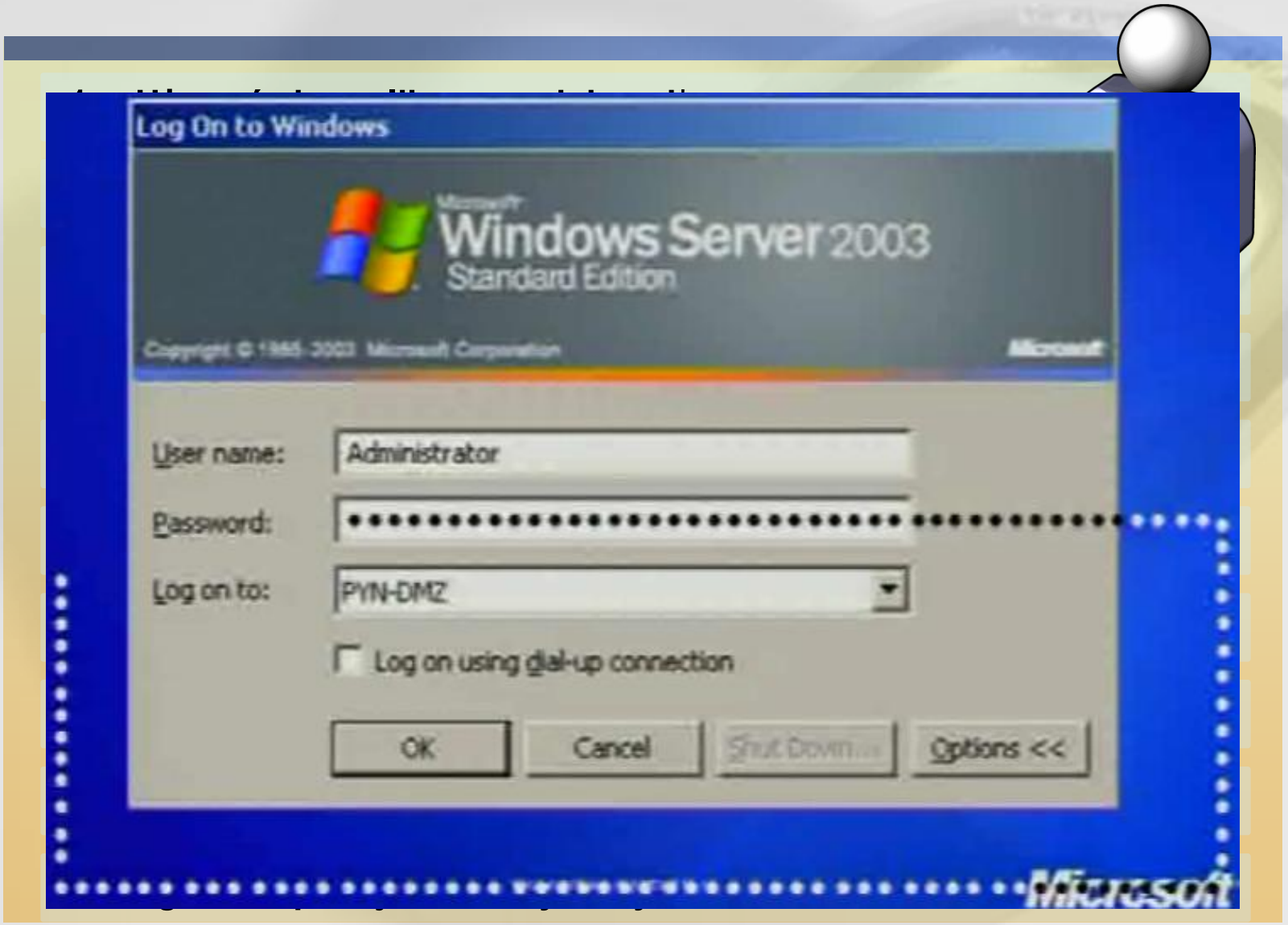
Autoryzacja

- **Zasady przepływu informacji w modelu Bella-LaPaduli:**
  - Podmiot może odczytywać informacje z obiektu, jeżeli jego poziom uprawnień zdominuje (będzie co najmniej taki sam) poziom uprawnień obiektu.
  - Podmiot może zapisać dane w obiekcie, jeżeli poziom uprawnień tego podmiotu jest zdominowany przez poziom zabezpieczeń obiektu

Autoryzacja

- **Obowiązkowa kontrola integralności Windows Vista**
  - Każdy proces (program lub usługa systemowa) działa na określonym poziomie zaufania, a każdy obiekt (na przykład plik) jest sklasyfikowany na pewnym poziomie zaufania. Ponieważ obowiązuje zasada zezwalająca jedynie na modyfikowanie zdominowanych obiektów, proces działający na niższym poziomie zaufania, nawet jeżeli został uruchomiony przez administratora, nie zmodyfikuje zaufanych (czyli systemowych) obiektów
  - Utworzony przez proces obiekt dziedziczy jego poziom zaufania

Podsumowanie



*Te wskazówki można częściowo wdrożyć za pośrednictwem scentralizowanych zasad