Technologie zapewniające bezpieczeństwo w systemach operacyjnych

Systemy Operacyjne 2002/2003

Bezpieczeństwo :-)

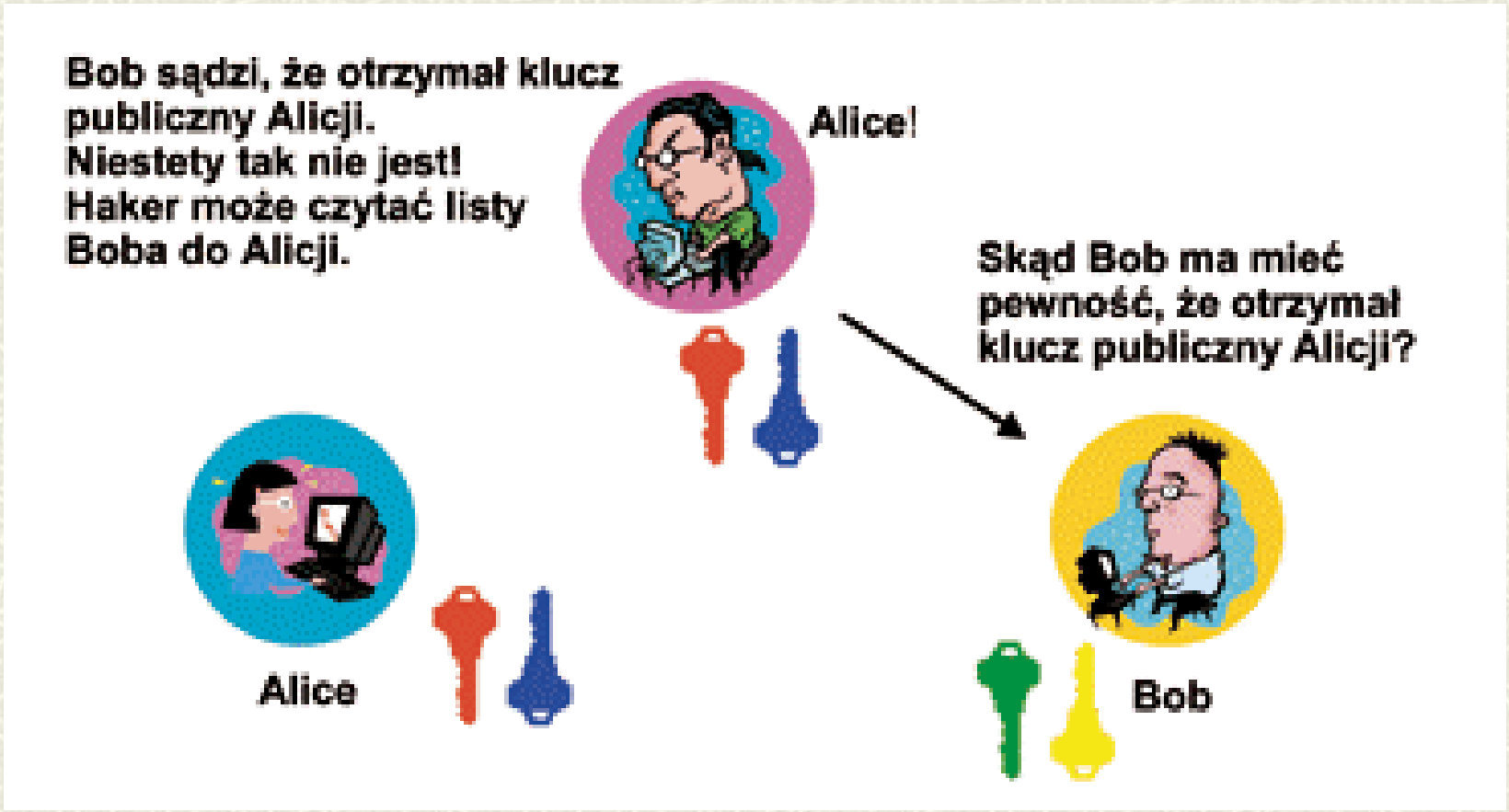
O czym będzie mowa...

- Klucze symetryczne i PKI
- Smart Cards
- SSL
- SSH

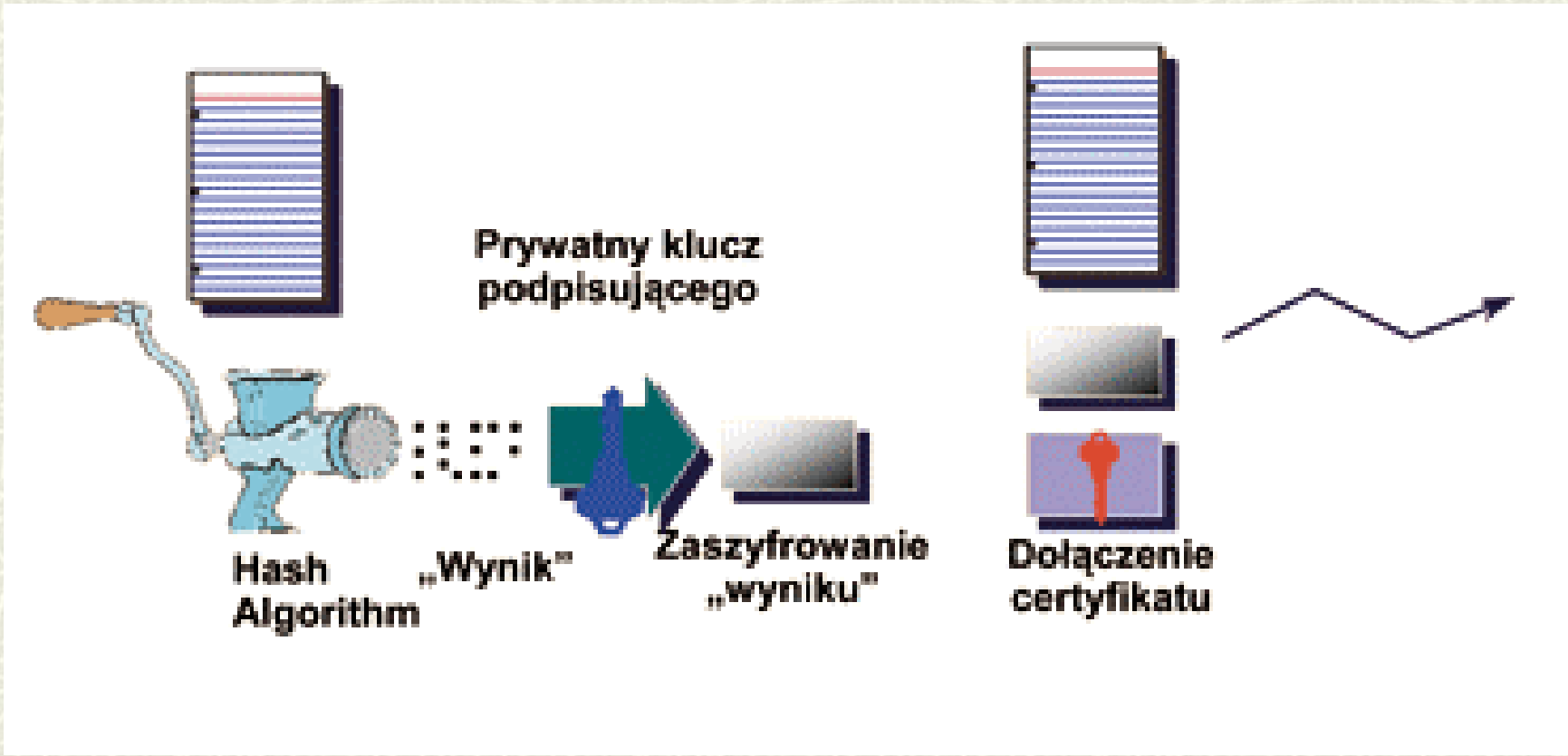
Architektura klucza symetrycznego

Architektura klucza asymetrycznego

Atak „man in the middle”



Podpis elektroniczny



Infrastruktura...

- Posiadanie przez Użytkownika pary kluczy
- Przyjęcie standardu
- Urzędy Certyfikacji
- Procedury

Usługi PKI

- Uwierzytelnianie podmiotów
- Uwierzytelnianie danych
- Integralność danych
- Niezaprzeczalność
- Poufność
- Prywatność

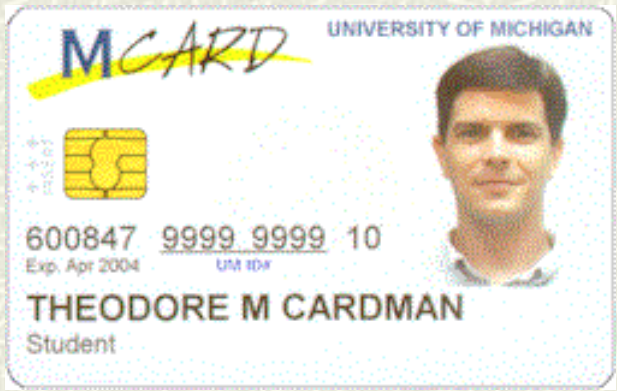
Funkcje PKI

- Rejestracja
- Certyfikacja
- Generacja kluczy
- Odnawianie kluczy
- Certyfikacja wzajemna
- Odwołanie certyfikatu
- Odzyskiwanie klucza

Smart Cards wprowadzenie

- Karta podobna do karty kredytowej z mikroprocesorem i pamięcią
- Wygląda jakoś tak

- Albo tak...



Smart Cards zalety

- Bezpieczne miejsce na dane
- Ograniczony kontakt ze światem zewnętrznym
- Mobilność

Smart Cards zastosowanie

- Portfel elektroniczny
- Klucz do drzwi
- Karta biblioteczna
- Identyfikator
- Inne

Smart Cards

- Drzewiasta struktura katalogów
- Nazwy plików to słowa dwubajtowe

Systemy operacyjne dla S.C.

- Java Card Operating System
- MultiOS
- Microsoft Windows for Smart Cards

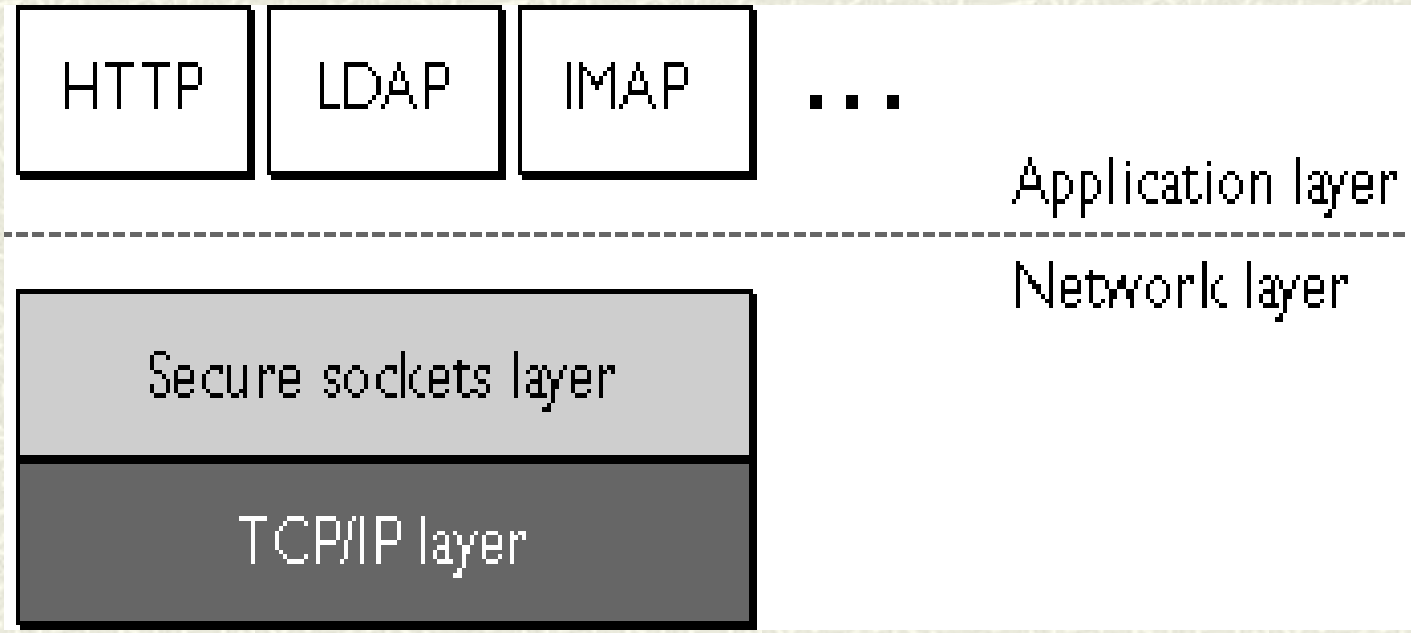
Aplikacje wykorzystujące S.C. dla Linuxa

- scas
- smartcard
- ssh-smart
- smarttools-rsa
- smartsign

SSL wprowadzenie

- SSL - Secure Socket Layer
- Zaprojektowany przez Netscape
- Protokół bezpiecznej komunikacji pomiędzy klientem a serwerem
- Podkładka pomiędzy istniejące protokoły a TCP/IP

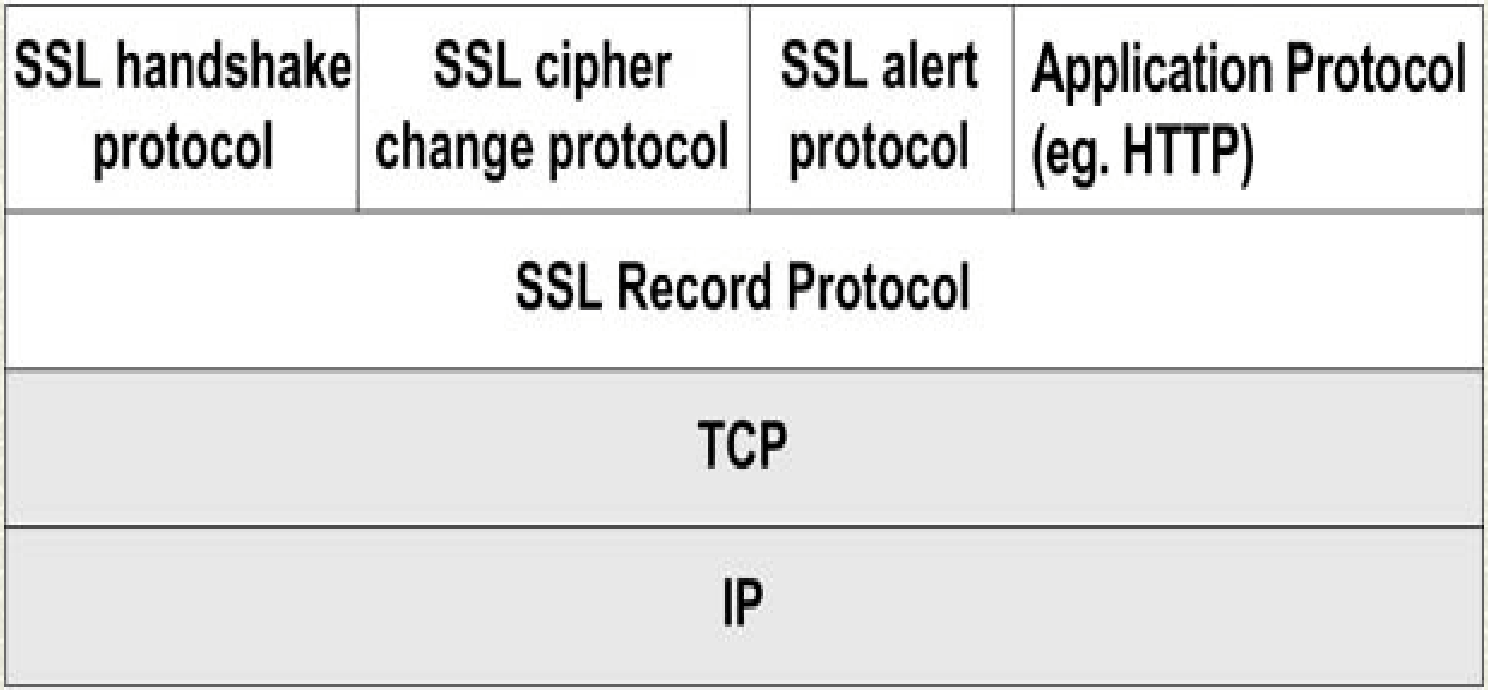
SSL wprowadzenie c.d.



SSL główne założenia

- Prywatność – połączenie jest szyfrowane
- Autoryzacja – klient i serwer określają swoją tożsamość
- Integralność przesyłanych danych (poprzez wykorzystanie sum kontrolnych)

SSL od środka



SSH wprowadzenie

- Początki SSH (Secure Shell) 1995
- Wprowadzony gdy poprzednicy przestają spełniać bezpiecznie swoje zadania
- SSH1 i SSH2

SSH - idea

- Klient łączy się z serwerem - otrzymuje Pb_Ser
- Porównuje z bazą
- Wysyła losowa liczbę zakodowaną Pb_Ser i Pr_Kl
- Serwer odkodowuje - session key
- Autoryzacja użytkownika

Autoryzacja klienta

- /etc/hosts.equiv lub /etc/shosts.equiv
- .rhosts lub .shosts
- Autoryzacja poprzez klucz publiczny
- Autoryzacja przez „agenta”
- Autoryzacja przez hasło
- Kerberos

SSH podstawowe cechy

- Sesje kodowane przy użyciu symetrycznego klucza
- Kryptografia klucza publicznego do ochrony klucza symetrycznego
- Kilka sposobów autoryzacji
- Wiele różnych algorytmów szyfrujących
- Autoryzacja obu maszyn

Algorytmy wykorzystywane przy kodowaniu kluczem symetrycznym

- 128 bit AES
- Blowfish
- 3DES
- CAST128
- Arcfour
- 192 bit AES
- 256 bit AES