Politechnika Warszawska
Instytut Telekomunikacji

Podstawy ochrony informacji - handel elektroniczny

Elektroniczne płatności poprzez WWW

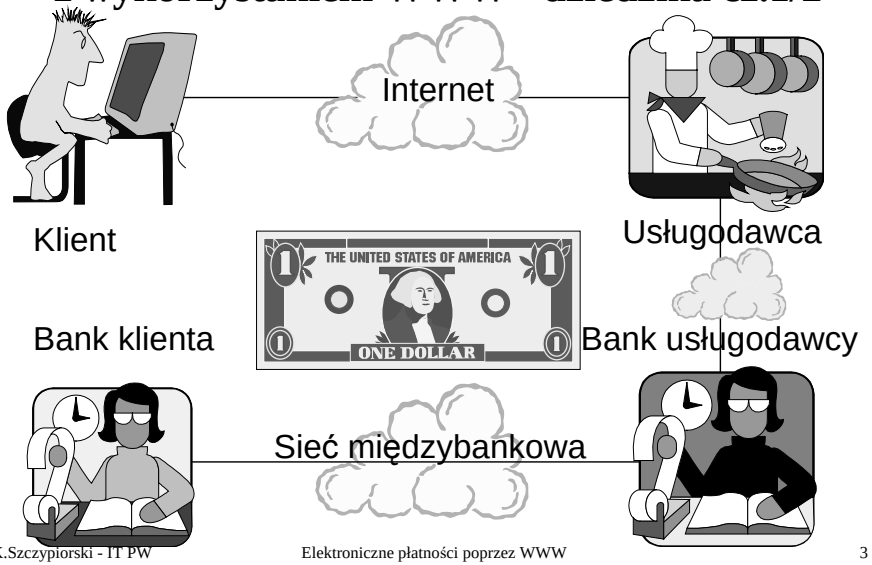
Krzysztof Szczypiorski, Piotr Kijewski
e-mail:{K.Szczypiorski,P.Kijewski}@tele.pw.edu.pl

INTERNET'99 - Wrocław, 9-10 grudnia 1999

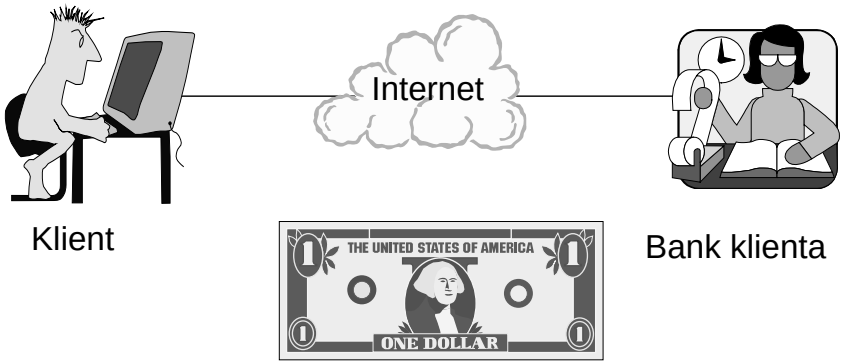
Plan prezentacji

- Odmiany handlu elektronicznego poprzez WWW
- Podstawowe problemy ochrony informacji w Internecie
- Obszary zabezpieczeń w WWW
- Płatności za pomocą kart
- Ewolucja zabezpieczeń w protokołach TCP/IP

Elektroniczny handel z wykorzystaniem WWW - dziedzina cz.1/2



Elektroniczny handel z wykorzystaniem WWW - dziedzina cz.2/2



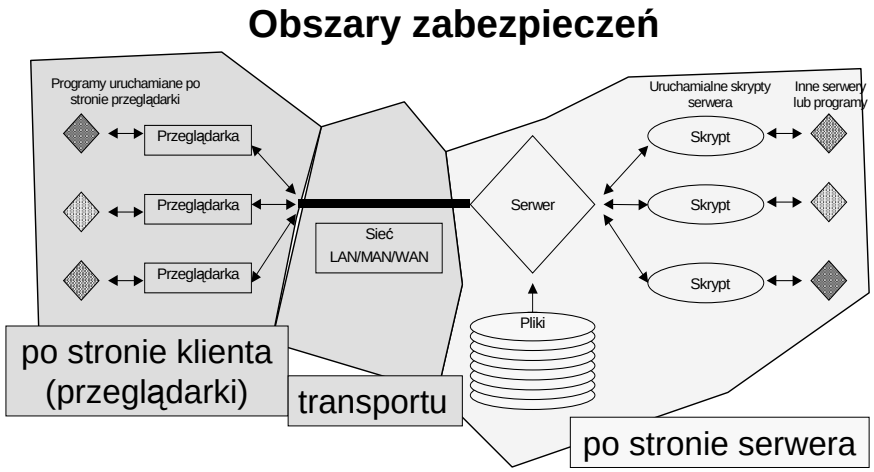
Home-, office-, direct-, Internet-banking

Podstawy ochrony informacji

Zagrożenia
- odmowa usługi (Z1)
- nielegalny dostęp (Z2)
- zmiana, przekłamanie strumienia danych (Z3)
- podszycie się pod innego uprawnionego użytkownika lub spreparowanie danych (Z4)
- wyparcie się faktu zajścia sesji komunikacyjnej, połączenia sieciowego (Z5)
- podsłuch transmitowanych danych (Z6)

Usługi ochrony informacji
- kontrola dostępu [chroni przed Z1, Z2]
- integralność danych [Z3]
- uwierzytelnienie [Z4]
- niezaprzeczalność [Z5]
- poufności danych [Z6]

Obszary zabezpieczeń w WWW



Płatności za pomocą kart

- przebieg procesu płatności w Internecie
- przy dokonywaniu transakcji w Internecie istotne są następujące cechy karty płatniczej:
  - nazwa organizacji wydającej kartę (np. Visa),
  - numer karty (na ogół 13-16 cyfr),
  - data ważności (na ogół w formacie MM/YY),
  - oraz (rzadko) imię i nazwisko (albo nazwa w przypadku firmy) wypisane (wypisana) na karcie.
- numer karty jednoznacznie określa organizację, która ją wydała
- data ważności nie jest w żaden sposób powiązana z numerem

Cecha wspólna [ISO 2894]

Prawdziwe dla kart płatniczych, których długość numeru jest mniejsza od 20.

4 2 5 1 1 0 0 0 1 0 0 0 0 8 3 0

1. Wszystkim cyfrom przyporządkujemy na przemian liczbę 1 albo 2 zgodnie z zasadą głoszącą, że ostatnia cyfra otrzymuje 1.

```
4 2 5 1 1 0 0 0 1 0 0 0 0 8 3 0
2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1
```

2. Traktując każdą cyfrę numeru kart płatniczej jako liczbę mnożymy ją przez przyporządkowaną liczbę.

```
4 2 5 1 1 0 0 0 1 0 0 0 0 8 3 0
2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1
-----------------------------------------------
8 2 10 1 2 0 0 0 2 0 0 0 0 8 6 0
```

3. Jeśli otrzymany iloczyn wynosi 10 albo jest większy – wyznaczamy resztę z dzielenia przez 10 i dodajemy 1.

```
4 2 5 1 1 0 0 0 1 0 0 0 0 8 3 0
2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1
-----------------------------------------------
8 2 10 1 2 0 0 0 2 0 0 0 0 8 6 1
8 2 1 1 2 0 0 0 2 0 0 0 0 8 6 0
```

4. Tak otrzymane wyniki dodajemy i sprawdzamy czy są podzielne przez 10 – jeśli tak – numer jest prawidłowy.

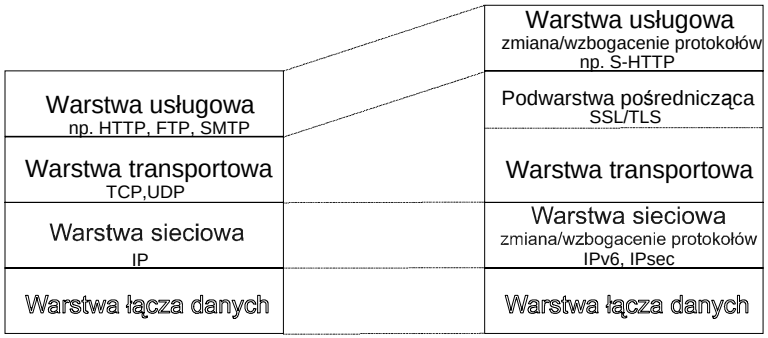
(8 + 2 + 1 + 1 + 2 + 0 + 0 + 0 + 2 + 0 + 0 + 0 + 0 + 8 + 6 + 0) mod 10 = 30 mod 10 = 0
numer jest prawidłowy

Cecha indywidualna

Organizacja	Długość numeru	1. cyfra	2. cyfra	4 pierwsze cyfry
Visa	16, 13	4	-	-
MasterCard	16	5	1,2,3,4,5	-
American Express	15	3	4,7	-
Diners Club Carte Blanche	14	3	0,6,8	-
Discover	16	-	-	6011
enRoute	15	-	-	2014, 2149
JCB	16	-	-	3088, 3096, 3112, 3158, 3337,3528

Ewolucja protokołów zabezpieczeń

Ewolucja poszczególnych warstw modelu sieci TCP/IP



Ewolucja w wybranych warstwach

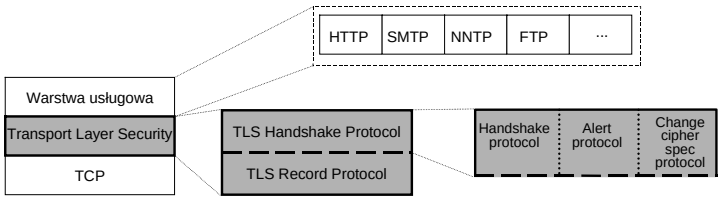
2

- **IPv6/IPsec** - Authentication Header, Encapsulating Security Payload, Internet Key Exchange

---

3

- np. **Secure-TCP???**
- **TLS/SSL**



- SSL/TLS: poufność, integralność, uwierzytelnienie klienta lub serwera
- w zasadzie wyeliminował rozwiązania w warstwie aplikacji

SSL/TLS - idea pracy cz.1/2

- Użytkownik dokonuje zakupów w internetowym sklepie (czyli na serwerze) sprzedawcy
- Faza 1 - Handshake - ustalenie wspólnego klucza K
  1. Użytkownik żąda, pobiera i weryfikuje certyfikat serwera.
  2. Użytkownik tworzy losowo 160-bitową wartość K.
  3. Użytkownik szyfruje K kluczem publicznym serwera.
  4. Użytkownik wysyła szyfrogram (3) do serwera.
  5. Serwer deszyfruje szyfrogram swoim kluczem prywatnym - odzyskuje K.
  6. Serwer dokonuje skrótu K.
  7. Serwer wysyła skrót (6) do użytkownika.
  8. Użytkownik dokonuje skrótu K i porównuje z wartością (7) otrzymaną.

SSL/TLS - idea pracy cz.2/2

- Po zakończeniu fazy 1 - serwer jest uwierzytelniony przed użytkownikiem, gdyż:
  - zna jego uwierzytelniony poprzez certyfikat klucz publiczny
  - serwer wykazał się posiadaniem klucza prywatnego (zdolność do odszyfrowania K)
- K jest wspólny kluczem (SSL/TLS MasterSecret)
- Faza 2 - Bezpieczna wymiana danych przy pomocy wspólnego klucza K
  - dane transmitowane w postaci pakietów zaszyfrowanych K (poufność) i chronionych MAC (integralność)

Podsumowanie

- podstawowe ograniczenia wynikają z cech samego systemu kart płatniczych
- SSL/TLS stanowi podstawę do zrealizowania bezpiecznego środowiska
- przyszłość: karty inteligentne + czytniki przy każdym komputerze
- rozwój protokołów elektronicznego pieniądza na kartach inteligentnych

KONIEC

Czy mają Państwo pytania?