Krzysztof Szczypiorski, Piotr Kijewski
Instytut Telekomunikacji
Politechnika Warszawska, Warszawa
E-mail: {K.Szczypiorski,P.Kijewski}@tele.pw.edu.pl

Podstawy ochrony informacji - handel elektroniczny

Elektroniczne płatności poprzez WWW

Streszczenie

W artykule przedstawiono zagadnienia związane z handlem elektronicznym realizowanym w Internecie poprzez WWW. Przedstawiono problemy ochrony informacji występujące w sieciach telekomunikacyjnych, a także podstawowe metody zabezpieczeń (w tym usługi i mechanizmy ochrony informacji). Zdefiniowano obszary zabezpieczeń w WWW. Omówiono sposób realizacji płatności za pomocą kart płatniczych, ilustrując niektóre cechy systemu kart – sposób sprawdzania poprawności numeru kart. Przedstawiono ideę Internet bankingu. Zaprezentowano ewolucję zabezpieczeń w protokołach TCP/IP, która kreuje bezpieczne środowisko dla handlu elektronicznego. Szczególną uwagę poświęcono najpopularniejszemu protokołowi SSL/TLS.

1 Wprowadzenie

Handel elektroniczny (ang. *electronic commerce*) jest pojęciem równie modnym, jak i trudnym do jednoznacznego określenia. Na potrzeby tego opracowania przyjmujemy, że handel elektroniczny jest wymianą w sieci telekomunikacyjnej informacji, służących zrealizowaniu finansowego zobowiązania - płatności.

W artykule **ograniczymy się do handlu elektronicznego realizowanego** w Internecie **poprzez WWW**. Przedstawimy techniczne aspekty realizacji elementów bezpiecznego środowiska dla elektronicznych płatności. Większość istniejących internetowych systemów płatności wykorzystuje karty płatnicze jako podstawowy środek umożliwiający regulacje długu klienta względem usługodawcy. To niewątpliwie wygodne rozwiązanie, zarówno dla klientów, jak i banków, nosi w sobie piętno systemu kart płatniczych - zatrważającą możliwość dokonania płatności jedynie przy użyciu numeru i daty ważności karty[1].

Innym coraz powszechniejszym zastosowaniem WWW w kontekście handlu elektronicznego jest prowadzenie przez banki oddziałów elektronicznych (ang. *home banking, office banking, direct banking* - ogólnie *Internet banking*), w których klient ma możliwość przeglądania historii swojego konta, a także dokonywania transakcji (przelewy, zakładanie rachunków terminowych).

2 Podstawy ochrony informacji w sieciach telekomunikacyjnych

Typowe zagrożenia występujące w sieciach telekomunikacyjnych, a w szczególności w Internecie to:

- odmowa usługi (Z1),
- nielegalny dostęp (Z2),
- zmiana, przekłamanie strumienia danych (Z3),

[1] dot. klasycznych kart (tzw. wypukłych) – część kart np. Visa Electron, Maestro jest obsługiwanych wyłącznie przez elektroniczne terminale

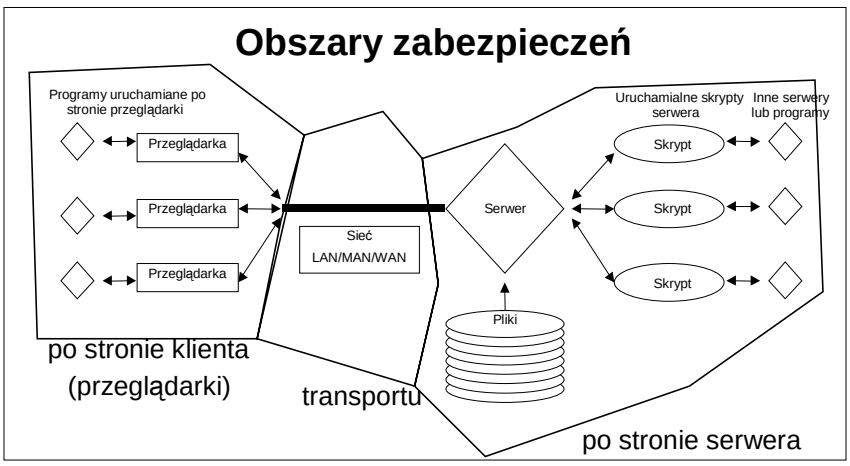
- podszycie się pod innego uprawnionego użytkownika lub spreparowanie danych (Z4),
- wyparcie się faktu zajścia sesji komunikacyjnej, połączenia sieciowego (Z5),
- podsłuch transmitowanych danych (Z6).

Przed wspomnianymi zagrożeniami chronią podstawowe usługi ochrony informacji:
- **kontrola dostępu** - ochrona przed nieuprawnionym dostępem do zasobów sieciowych [chroni przed Z1, Z2],
- **integralność danych** - gwarancja spójności danych; ochrona przed modyfikacją, wtrąceniem, wymazaniem danych [Z3],
- **uwierzytelnienie** - kontrola tożsamości stron lub pochodzenia danych wymienianych pomiędzy nimi podczas sesji komunikacyjnej [Z4],
- **niezaprzeczalność** - metoda rozstrzygnięcia ewentualnego sporu pomiędzy nadawcą a odbiorcą dotyczącego zarówno faktu nadania i odbioru informacji jak i jej treści [Z5],
- **poufności danych** - ochrona danych przed nieuprawnionym uzyskaniem ich przez strony nieupoważnione [Z6].

Kontrola dostępu jest usługą pierwotną względem pozostałych. Niezaprzeczalność, zawsze wiąże się z uwierzytelnieniem, której elementem jest z kolei integralność. Poufność danych jest usługą niezależną.

Usługi ochrony informacji są realizowane poprzez użycie odpowiednich mechanizmów kryptograficznych, z których najważniejsze to:
- **szyfrowanie** – przekształcenie strumienia danych przy użyciu klucza kryptograficznego; algorytmy, w których ten sam klucz służy do szyfrowania i odszyfrowania określa się mianem symetrycznych; algorytmy, w których inny klucz służy do szyfrowania a inny do odszyfrowania – algorytmami asymetrycznymi (klucza publicznego),
- **podpis cyfrowy** – wiążą się z nim dwie operacje – generacja i weryfikacja; podczas pierwszej z nich jest wykorzystywana pewna tajna informacja (np. klucz prywatny), podczas drugiej – powszechnie dostępna (np. klucz publiczny)
- **wymiana uwierzytelniająca** – proces wymiany informacji umożliwiających stwierdzenie tożsamości drugiej strony,
- **mechanizmy integralności** – przekształcenia (np. funkcje skrótu) umożliwiające z dużym prawdopodobieństwem określić ewentualne zmiany w wiadomości.

3 Obszary zabezpieczeń w WWW



Rysunek 1 Obszary zabezpieczeń i architektura usługowa WWW

W przypadku WWW mamy do czynienia z trzema obszarami zabezpieczeń, wynikającymi wprost z architektury usługowej (por. Rysunek 1):

- obszarem po stronie klienta (przeglądarki),
- obszarem transportu,
- obszarem po stronie serwera WWW.

W dalszej części artykułu skupimy się na obszarze transportu, który jest oparty na stosie protokołów TCP/IP rozszerzonym o protokół HTTP (ang. *HyperText Transfer Protocol*). Problemy związane z pozostałymi obszarami w głównej mierze sprowadzają się do poprawnej implementacji aplikacji oraz prawidłowej konfiguracji serwera i przeglądarki.

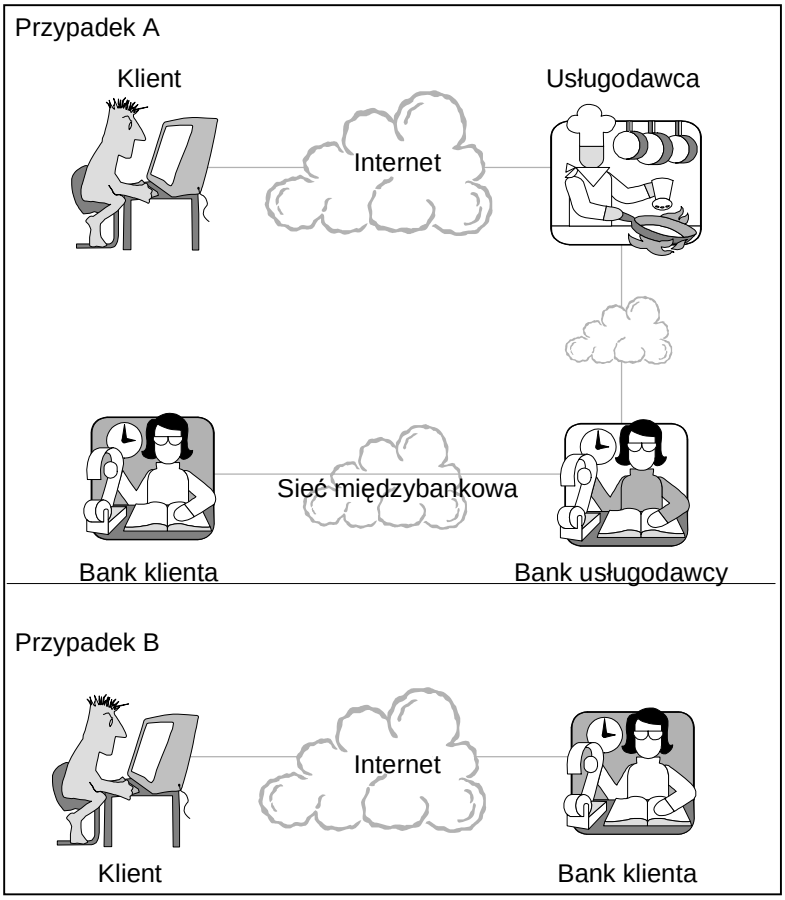
W standardowym stosie protokołów TCP/IP nie zrealizowano żadnych usług ochrony informacji. Stąd też informacje przekazywane w sieci Internet są podatne na większość przedstawionych w rozdz. 2 zagrożeń, w tym na:

- zmianę, przekłamanie strumienia danych (Z3),
- podszycie się pod innego uprawnionego użytkownika lub spreparowanie danych (Z4),
- podsłuch transmitowanych danych (Z6).

Ewolucja protokołów w sieciach TCP/IP przebiega w kierunku wykreowania bezpiecznego środowiska dla różnorodnych aplikacji, w tym związanych z elektronicznym handlem (patrz rozdz. 6).

4 Płatności w Internecie realizowane za pomocą kart płatniczych

4.1 Przebieg płatności



Rysunek 2 Przykłady handlu elektronicznego w Internecie

W przypadku płatności realizowanych za pomocą kart płatniczych (Rysunek 2 - przypadek A) mamy do czynienia z czterema podmiotami:

- klientem,
- usługodawcą,
- bankiem usługodawcy,
- bankiem klienta - będącym jednocześnie wystawcą karty płatniczej.

Proces realizacji płatności przebiega następująco:

1. Klient "podaje" kartę usługodawcy.
2. Usługodawca inicjuje wystawienia rachunku, a następnie kontaktuje się ze swoim bankiem prosząc o autoryzację transakcji.
3. Poprzez sieć międzybankową bank usługodawcy przesyła prośbę o autoryzację do banku klienta.
4. Bank klienta wysyła do banku usługodawcy poprzez sieć międzybankową informację dot. autoryzacji.
5. Bank usługodawcy przekazuje usługodawcy informacje o statusie autoryzacji.
6. W przypadku braku autoryzacji transakcja nie może zostać zrealizowana. W przeciwnym przypadku usługodawca może zakończyć wystawianie rachunku, wysyłając jednocześnie do swojego banku potwierdzenie zakończenia transakcji.
7. Po pewnym czasie bank usługodawcy rozlicza się z bankiem klienta. Także banki rozliczają się ze swoimi klientami.

"Podanie" karty usługodawcy, czyli przekazanie poprzez sieć telekomunikacyjną numeru karty i daty ważności, może nastąpić na trzy sposoby:

- poprzez zwykły kanał internetowy (poczta elektroniczna, metoda POST w HTTP),
- poprzez zaszyfrowany kanał (najczęściej realizowane na bazie opisanego w rozdz. 6.2 SSL/TLS[2]) – zrealizowana zatem jest usługa poufności,
- poprzez telefon.

Pierwszy sposób należy uznać za niebezpieczny, ze względu na rozpowszechnienie oprogramowania do podsłuchu pakietów (ang. sniffer). Dwa pozostałe wydają się równie bezpieczne, przy założeniu, że serwer jest niedostępny dla nieautoryzowanych osób oraz połączenie telefoniczne nie jest podsłuchiwane (np. na poziomie PABX lub sieci dostępowej w budynku).

Istotną rzeczą jest zaufanie klienta, że powierza swoje dane działającemu w dobrej wierze usługodawcy, który posiada prawa do realizacji transakcji (problem uwierzytelnienia usługodawcy).

Warto podkreślić, że w rozważanym przypadku nie należy zapominać o bezpieczeństwie sieci międzybankowej.

4.2 Cechy karty płatniczej wykorzystywane przy transakcjach w Internecie

Przy dokonywaniu transakcji w Internecie istotne są trzy cechy karty płatniczej:

- nazwa organizacji wydającej kartę (np. Visa),
- numer karty (zasadniczo 13-16 cyfr),
- data ważności (zasadniczo w formacie MM/YY).

W niektórych (dość rzadkich) sytuacjach wymagane jest podanie czwartej cechy:

- imienia i nazwiska (albo nazwy w przypadku firmy) wypisanego (wypisanej) na karcie.

[2] protokół SET (Secure Electronic Transaction) opracowany przez organizacje Visa i MasterCard nie jest w praktyce wykorzystywany

Numer karty jednoznacznie określa organizację, która ją wydała. Data ważności nie jest w żaden sposób powiązana z numerem. Pierwsze cztery cyfry są charakterystyczne dla banku wystawiającego daną kartę.

Aby zweryfikować poprawność posiadanego numeru karty płatniczej należy rozpatrzyć dwie cechy:
- **cechę wspólną** dla współczesnego systemu kart płatniczych, ,
- **cechę indywidualną** dla organizacji wydającej określoną kartę.

Cechę wspólną – algorytm sprawdzania numerów kart płatniczych – określa norma [ISO 2894]. Dla łatwiejszego zrozumienia przedstawimy algorytm na przykładzie (dydaktycznego!) numeru 4251 1000 1000 0830.

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 karty 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

W tabeli 1 zgrupowano **cechy indywidualne** dla przykładowych organizacji wydających karty.

Tabela 1 Cechy indywidualne karty płatniczej

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	-
JCB	16	-	-	3088, 3096, 3112, 3158, 3337,3528

Obecnie większość internetowych usługodawców stosuje powyższy schemat sprawdzania poprawności numeru kart klienta, przed połączeniem się ze swoim bankiem w celu autoryzacji. W przeszłości część sklepów internetowych pracujących off-line, a także serwisów WWW sprawdzających poprzez podanie numeru i daty ważności karty pełnoletność klienta, akceptowało poprawny numer bez autoryzacji.

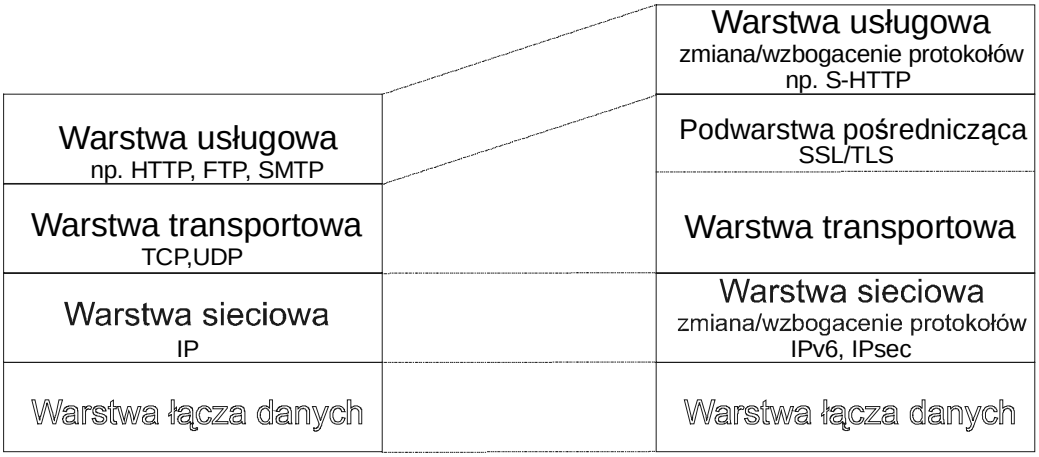
5 Internet banking

Internet banking stanowi nową ofertę banków dającą możliwość dostępu do usług bankowych z poziomu przeglądarki WWW albo innej aplikacji internetowej z dowolnego miejsca na świecie, przez 24 godziny na dobę. Oprócz wymaganej dla transakcji za pomocą kart płatniczych poufności i uwierzytelnienia serwera bankowego, niezbędne jest uwierzytelnienie klienta banku, dokonywane najczęściej przy użyciu dostarczanego przez bank oprogramowania kryptograficznego, często wykorzystującego karty inteligentne. Jako protokół wspomagający, chroniący transport danych, często używany jest SSL/TLS.

6 Rozwiązania zwiększające bezpieczeństwo transakcji

Ewolucja zabezpieczeń w protokołach sieci TCP/IP jest konieczna z punktu zastosowania ich w elektronicznym handlu. Dla poszczególnych protokołów i aplikacji są zauważalne dwa podstawowe kierunki:

- **rozbudowanie (wzbogacenie)** tego co jest – potraktowania bezpieczeństwa jako opcji,
- **zmiana** tego co jest – potraktowania zabezpieczeń jako niezbędnej składowej.



Rysunek 3 Ewolucja poszczególnych warstw sieci TCP/IP

Za pierwszym trendem przemawia przede wszystkim elastyczność, brak konfliktów natury prawnej (ograniczenia w używaniu kryptografii w niektórych państwach), cena (nie trzeba zmieniać od razu całego oprogramowania i sprzętu). Za drugim – pełna i bezwarunkowa realizacja usług ochrony informacji. Warto dodać, że zabezpieczenia w poszczególnych warstwach powinny być realizowane niezależnie.

W dziedzinie używanych algorytmów kryptograficznych zauważalny jest wzrost zainteresowania systemem uzgodnienia klucza Diffie-Hellman (DH – [Diffie77]) rozszerzonym o uwierzytelnienie za pomocą podpisów cyfrowych DSS (ang. *Digital Signature Standard* – [FIPS186]), kosztem spadku popularności systemu RSA (*Rivest Shamir Adleman* – [Rivest78]). Wynika to z problemów

związanych z patentami[3]. Coraz większą rolę zaczynają odgrywać systemy kryptograficzne oparte na krzywych eliptycznych [Menezes96].

W kolejnych trzech podrozdziałach przedstawiono ewolucję poszczególnych warstw sieci (Rysunek 3), z wyłączeniem warstwy łącza danych, która wychodzi poza zakres tego artykułu.

6.1 Warstwa sieciowa

Protokół IP wersja 4 – serce komunikacyjne sieci TCP/IP – nie zawiera w sobie żadnych usług ochrony informacji. Ataki typu odmowa usługi, podsłuch informacji, nieautoryzowana modyfikacja informacji, podszycie się są dość rozpowszechnione.

Następna wersja protokołu IPv6 (IP wersja szósta [RFC2401]) zawiera wsparcie dla usług ochrony informacji. Proponowane dwa mechanizmy bezpieczeństwa to: IP Authentication Header (AH) - nagłówek uwierzytelniający - zapewniający integralność i uwierzytelnienie [RFC2402], IP Encapsulating Security Payload (ESP) - bezpieczna koperta - zapewniająca zawsze poufność i zależnie od użytego algorytmu i trybu także integralność i uwierzytelnienie [RFC2406]. Wspomniane mechanizmy zostały także zaadaptowane dla IPv4 – tak rozszerzony protokół nosi nazwę IPsec.

Dystrybucja klucza połączona z uwierzytelnieniem jest realizowana za pomocą protokołu IKE – Internet Key Exchange [RFC2409].

6.2 Warstwa transportowa

W warstwie transportowej zwiększa się bezpieczeństwo poprzez dodanie podwarstwy – TLS (ang. *Transport Layer Security*) [RFC2246] - pośredniczącej w wymianie danych z aplikacjami (Rysunek 4). Zapewnia to bezpieczną warstwę gniazd transportowych (co koresponduje z poprzednią nazwą systemu: SSL – ang. *Secure Socket Layer*). TLS składa się z dwóch warstw: warstwy zarządzania bezpieczeństwem połączenia (TLS Handshake Protocol[4]) oraz warstwy tworzącej jednostki protokołu TLS (TLS Record Protocol) zgodnie z wynegocjowanym kontekstem (algorytmy szyfrujące[5], kompresja danych). Przy nawiązywaniu połączenia za pomocą TLS uzgadniany jest przy użyciu algorytmów klucza publicznego klucz sesyjny K (SSL/TLS MasterSecret). Typowy przebieg procesu dystrybucji klucza z uwierzytelnieniem serwera składa się z następujących kroków:

1. Klient żąda, pobiera i weryfikuje certyfikat serwera.
2. Klient tworzy losowo 160-bitową wartość K.
3. Klient szyfruje K kluczem publicznym serwera.
4. Klient 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 klienta.
8. Klient dokonuje skrótu K i porównuje z wartością (7) otrzymaną.

Po zakończeniu tego procesu - serwer jest uwierzytelniony przed klientem, gdyż:

- klient zna jego uwierzytelniony poprzez certyfikat klucz publiczny,

[3] na DH patent już wygasł

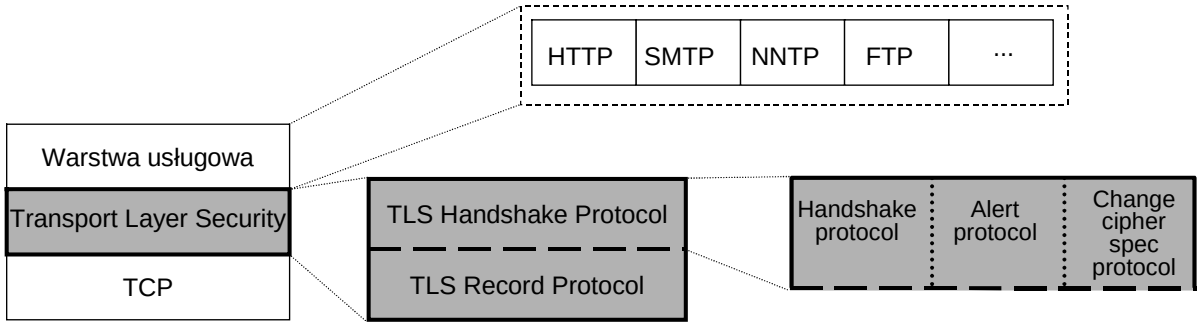
[4] w podwarstwie występują trzy protokoły: Handshake protocol (uzgodnienie), Alert protocol (obsługa błedów), Change cipher spec protocol (zmiana kryptosystemów)

[5] algorytmy klucza publicznego: RSA, Fortezza i Diffie-Hellman (z certyfikatami opartymi o RSA, DSS albo bez nich); algorytmy symetryczne RC4, RC2, IDEA, DES (40-bitowy), DES, TripleDES i in.

- serwer wykazał się posiadaniem klucza prywatnego (zdolność do odszyfrowania K)

Dane szyfrowane kluczem K chronią informacje przed podsłuchem. Dodatkowo istnieje możliwość uwierzytelnienia klienta, a także rezygnacja z uwierzytelnienia serwera. TLS w obecnej formie (wersja 1.0) posiada kilka ograniczeń: wymaga niezawodnego protokołu transportowego (TCP), nie ma wsparcia dla proxy, wymaga zastosowania kosztownych obliczeniowo algorytmów klucza publicznego. Trwają pracę nad zintegrowaniem TLS z innymi (”starymi”) systemami kryptograficznymi takimi jak np. Kerberos.

Należy się spodziewać, że coraz więcej usług w sieciach TCP/IP będzie miało wsparcie dla TLS (obecnie są to m.in.: HTTP, SMTP, NNTP, FTP, TELNET, IMAP4, IRC, POP3). Wprowadzenie TLS (a przedtem SSL) położyło kres nieudanym pod względem elastyczności próbom bezpośredniej ingerencji w protokoły warstwy transportowej – TCP i UDP (zapomniane już koncepcje typu Secure TCP).



Rysunek 4 Protokół TLS: schemat, umiejscowienie w modelu sieci TCP/IP

6.3 Warstwa usługowa

Zabezpieczenie warstwy usługowej jest równie bogate jak ilość występujących w niej aplikacji. Najsilniej dają się zaobserwować wspomniane wcześniej dwa równoległe trendy:

- wzbogacenie starego protokołu,
- zaproponowanie nowego protokołu z zabezpieczeniami.

Także coraz częściej wykorzystuje się wsparcie na poziomie warstwy transportowej (TLS/SSL), które niweluje niekiedy sens stosowania bezpiecznych protokołów aplikacyjnych (np. zapominana powoli koncepcja S-HTTP).

Elementem wspólnym dla bezpieczeństwa większości usług jest ich powiązanie z systemem nazywania domen DNS (ang. *Domain Name System*). System ten definiuje relacje pomiędzy adresami warstwy IP (w IPv4 32-bitowe) a hierarchicznymi nazwami sieci, podsieci i maszyn. DNS jest podatny na atak podszycia się - stąd też zaproponowane rozszerzenie [RFC2535] – nazywane czasem DNSSEC - uzupełnia system o usługę uwierzytelnienia poprzez zastosowanie dodatkowego pola z podpisem cyfrowym potwierdzającym wiadomość. Dodatkowo na poziomie DNS może być realizowana dystrybucja klucza – także na potrzeby innych usług.

W odróżnieniu do innych warstw bezpieczeństwo warstwy usługowej jest niejednolite. Przypuszczamy, że określenie wspólnej platformy zarządzania zabezpieczeniami (w tym systemu certyfikacji kluczy publicznych) pozwoli na uporządkowanie protokołów rozszerzających bezpieczeństwo aplikacji.

7 Podsumowanie

Większość istniejących internetowych sklepów oferuje możliwość dokonania zapłaty za towary i usługi poprzez użycie kart płatniczych. Najsłabszym punktem tego typu rozwiązania jest sam system kart, który umożliwia na dokonanie transakcji jedynie przy użyciu numeru i daty ważności karty. Najpopularniejsza metoda ochrony transmitowanych danych, a także uwierzytelnienia usługodawcy to opisany w artykule SSL/TLS. Mimo przedstawionych w artykule ograniczeń SSL/TLS stanowi potencjalną platformę do rozwoju bezpiecznych aplikacji związanych z bezpiecznym handlem (np. Internet banking).

W najbliższej przyszłości należy spodziewać się ewolucji systemu kart płatniczych – użycia kart inteligentnych, na których będzie można zaimplementować także elektroniczną gotówkę. Użycie wyrafinowanych rozwiązań opartych na kartach inteligentnych wiążę się z uzupełnieniem wyposażenia internetowego komputera o czytnik kart, czego do tej pory starano się uniknąć.

Literatura

[Diffie77] W. Diffie, M. E. Hellman - *New Directions in Cryptography* - IEEE Transactions on Information Theory, V. IT-22, n. 6, June 1977

[FIPS186] NIST FIPS PUB 186 - *Digital Signature Standard* - National Institute of Standards and Technology, U.S. Department of Commerce, May 18, 1994.

[Menezes96] A.Menezes, P. van Oorschot, S.Vanstone - *Handbook of Applied Cryptography* - CRC Press, October 1996

[ISO 2894] ISO/IEC 2894 - *Embossed credit cards - Specifications, numbering system and registration procedure*, 1980

[RFC2246] T. Dierks, C. Allen - *The TLS - Protocol Version 1.0* - RFC 2246, January 1999

[RFC2401] S. Kent, R. Atkinson - *Security Architecture for the Internet Protocol*, RFC 2401, November 1998

[RFC2402] S. Kent, R. Atkinson - *IP Authentication Header*, RFC 2402, November 1998

[RFC2406] S. Kent, R. Atkinson - *IP Encapsulating Security Payload*, RFC 2406, November 1998

[RFC2409] D. Harkins, D. Carrel - *The Internet Key Exchange (IKE)*, RFC 2409, November 1998

[RFC2535] D. Eastlake - *Domain Name System Security Extensions* - RFC 2535, March 1999

[Rivest78] R. Rivest, A. Shamir, L. M. Adleman - *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* - Communications of the ACM, v. 21, n. 2, February 1978