



Metody matematyczno-ekonomiczne oraz informatyka w biznesie
Studia podyplomowe

Blok I6
Poczta elektroniczna, szyfrowanie i podpis
elektroniczny

Semestr letni 2006/07

Jacek Sroka
sroka@mimuw.edu.pl

Poczta elektroniczna

Co to jest poczta elektroniczna

e-mail (*ang. electronic mail*)

- usługa internetowa działająca podobnie jak zwykła poczta (*ang. snail mail*)
- przesyłki to tekst z załącznikami (*ang. attachment*)
- nie jest usługą telekomunikacyjną
- historia
 - Compatible Time-Sharing System (CTSS) w 1961 roku na MIT
 - 1969 pierwsze próby wysyłania wiadomości przez sieć
 - 1971 znak @ rozdziela nazwę użytkownika od nazwy maszyny (ARPANET)

Zalety poczty elektronicznej

- duża szybkość działania – przesyłki **zazwyczaj** dochodzą w kilka minut/sekund
- mały koszt – jeżeli posiada się trwały dostęp do łącza internetowego
- proste adresy
- do przesyłek można dołączać nietekstowe załączniki
- wygoda użytkowania – nie trzeba wychodzić z domu

Wady poczty elektronicznej

Brak mechanizmu potwierdzenia dostarczenia

- poczta (zwykła i elektroniczna), a prawo
 - Wyrok SN z 11 grudnia 1996 roku (sygn. akt I PKN 36/96, OSNAPiUS z 1997 r., z. 14, poz. 251): Złożenie oświadczenia woli o rozwiązaniu umowy bez wypowiedzenia (a zatem także o wypowiedzeniu umowy) jest skuteczne także wówczas, gdy pracownik, mając realną **możliwość zapoznania** się z jego treścią, z własnej woli nie podejmuje przesyłki pocztowej zawierającej to oświadczenie. Orzeczenie to należy stosować także do wypowiedzenia umowy o pracę.
 - Uznaje się, że możliwość zapoznania się z wiadomością elektroniczną jest już w chwili jej wypłynięcia na serwer

Wady poczty elektronicznej

Umożliwia rozprzestrzenianie się wirusów

- skanery antywirusowe
- o otwarciu załącznika powinien decydować użytkownik
- niektóre rodzaje załączników są z zasady niebezpieczne (nawet jeżeli wysyłający nie miał złych intencji)
- użytkownicy są naiwni
 - łańcuszki
 - „drogi użytkowniku sam zepsuj swój system”

Wady poczty elektronicznej

Jest źródłem niechcianych wiadomości – **spam**

- czy to dobrze, że poczta jest za darmo
- historia terminu spam
 - w 1937 konserwa „Hormel SpicedHam” została przemianowana na „SPiced hAM” czyli SPAM
 - niektóre inne popularne wyjaśnienia skrótu SPAM, to:
 - „Spare-Parts-Already-Minced”
 - „Something Posing As Meat”
 - „Specially Processed Artificial Meat”
 - w latach 1980 spamowanie używano w znaczeniu „flooding” lub „trashing”
 - pierwszy spamowany w ten sposób dialog pojawił się w skeczu Monty Pythona
 - 5 marca 1994 małżeństwo prawników Laurence Canter i Martha Siegel wysłało pierwszy spam **komercyjny** – “Green Card spam”



Wady poczty elektronicznej

- Łatwo paść ofiarą wyłudzenia, bądź oszustwa – phishing
- Łatwo się pod kogoś podszyć
- Łatwo podejrzeć zawartość przesyłek
- ...

Na szczęście wady nie przyćmiewają zalet

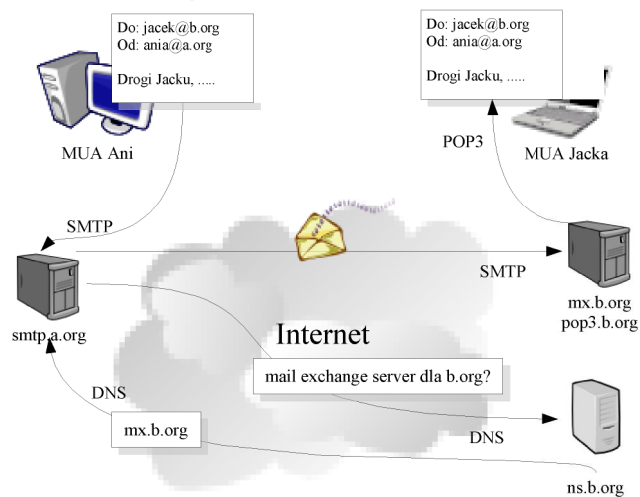
Adresy i aliasy

- Adres składa się z dwóch części rozdzielonych znakiem „@”, np.
jacek@mimuw.edu.pl
- Aliasy to alternatywne nazwy konta, np.
jacek.placek@mimuw.edu.pl lub j.placek@mimuw.edu.pl
- Adresy i aliasy nie mogą zawierać spacji (znaki, litery i „.”)
- Nie można używać znaków narodowych
- Małe i duże litery nie są rozróżniane

Mechanizm funkcjonowania poczty elektronicznej

- medium transportowym jest Transmission Control Protocol/Internet Protocol (TCP/IP)
- pocztę wysyła Mail Transport Agent (MTA) przy pomocy Simple Mail Transport Protocol (SMTP)
- pocztę odbiera Mail User Agent (MUA) przy pomocy POP3 lub IMAP4
 - Mozilla Thenderbird (Windows, Linux)
 - Microsoft Outlook Express (Windows)
 - Microsoft Outlook (Windows)
 - The Bat! (Windows)
 - Eudora (Windows)
 - Evolution (Linux)
 - KMail (Linux)
 - Aplikacje działające przez WWW

Mechanizm funkcjonowania poczty elektronicznej



Komunikat SMTP

```
S: 220 www.example.com ESMTP Postfix
C: HELO mydomain.com
S: 250 Hello mydomain.com
C: MAIL FROM:<sender@mydomain.com>
S: 250 Ok
C: RCPT TO:<friend@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: test message
C: From: sender@mydomain.com
C: To: friend@example.com
C:
C: Hello,
C: This is a test.
C: Goodbye.
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
```

POP3

Post Office Protocol v3 (POP3)

- kolejkuje wiadomości dla osób, które nie mogą być bez przerwy w sieci i odbierać poczty przy pomocy SMTP
- zazwyczaj wiadomości są pobierane, kasowane z serwera i przetwarzane na komputerze klienta (resztę symulują programy pocztowe)
- każdy list musi być pobierany razem z załącznikami i jego części nie można w łatwy sposób pomijać
- nie ma możliwości przeszukiwania kolejki
- jest propozycja POP4 z m.in. podstawowymi folderami i flagowaniem wiadomości
- alternatywą jest IMAP

```
S: <wait for connection on TCP port 110>
C: <open connection>
S: +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
C: USER mrose
S: +OK User accepted
C: PASS mrosepass
S: +OK Pass accepted
C: STAT
S: +OK 2 320
C: LIST
S: +OK 2 messages (320 octets)
S: 1 120
S: 2 200
S: .
C: RETR 1
S: +OK 120 octets
S: <the POP3 server sends message 1>
S: .
C: DELE 1
S: +OK message 1 deleted
C: RETR 2
S: +OK 200 octets
S: <the POP3 server sends message 2>
S: .
C: DELE 2
S: +OK message 2 deleted
C: QUIT
S: +OK dewey POP3 server signing off (maildrop empty)
C: <close connection>
S: <wait for next connection>
```

MIME

- SMTP umożliwia jedynie przysyłanie 7-bitowych znaków ASCII
- Multipurpose Internet Mail Extension (MIME) to mechanizm
 - umieszczania w poczcie innych znaków narodowych
 - umieszczania w poczcie nietekstowych załączników
 - łączenia w jedne przesyłce kilku rodzajów zawartości (ang. Multipart Message)
- MIME dodaje nowe nagłówki do wiadomości, np. Content-type
 - standardowe nagłówki: „To:”, „Subject:”, „From:” i „Date:”
- Można używać znaki narodowe w nagłówkach
 - „=?charset?encoding?encoded text?=”
- Kodowanie i dekodowanie wykonują programy pocztowe
- Wiadomości MIME mogą być przesyłane przez stare serwer

Przykład wiadomości wieloczęściowej

```
Content-type: multipart/mixed; boundary="frontier"
MIME-version: 1.0
```

```
To jest wieloczesciowa wiadomosc w formacie MIME.
--frontier
Content-type: text/plain
```

```
To jest zawartosc wiadomosci
--frontier
Content-type: application/octet-stream
Content-transfer-encoding: base64
```

```
PGh0bWw+CiAgPGh1YWQ+CiAgPC9oZWFKPgogIDxib2R5gogICAgPHA+VGhpcyBp
cyBpcyB0aGUgYm9keSBvZiB0aGUgbWVzc2FnZS48L3A+CiAgPC9ib2R5Pgo8L2h
0bWw+Cg==
```

Serwer poczty

- Dzięki serwerom poczta dochodzi nawet jak użytkownicy nie są cały czas podłączeni do sieci
- Co więcej zwykli użytkownicy nie muszą konfigurować serwera i rozwiązywać problemów z nim związanych
- Kiedyś MTA działały jako „open mail relays”

Szyfrowanie i podpisywanie

Szyfrowanie symetryczne

- Jest tylko jeden klucz
- Używa się go zarówno do szyfrowania i deszyfrowania
- Nadawca i odbiorca muszą się nim bezpiecznie wymienić
- Stosowane algorytmy szyfrowania symetrycznego są bardzo szybkie

Szyfrowanie niesymetryczne

- Są dwa klucze: publiczny i prywatny
- Klucz publiczny można wszystkim oznajmić
- Klucz prywatny należy chronić
- Wiadomość zaszyfrowana kluczem publicznym może być odszyfrowana jedynie odpowiadającym mu kluczem prywatnym
 - wysyłanie wiadomości jedynie do czyjejs wiadomości
- Wiadomość zaszyfrowana kluczem prywatnym może być odszyfrowana jedynie odpowiadającym mu kluczem publicznym
 - pewność kto wysłał wiadomość

Szyfrowania poczty elektronicznej

- Potrzebne jest specjalne oprogramowanie
- Obie strony wymieniają się swoimi kluczami publicznymi (np. umieszczając je na stronie WWW)
- Nadawca szyfruje wiadomość kluczem publicznym odbiorcy

Podpis elektroniczny

- Potrzebne jest specjalne oprogramowanie
- Obie strony wymieniają się swoimi kluczami publicznymi
- Do wiadomości dołączana jest jej suma kontrolna zaszyfrowana kluczem prywatnym nadawcy
- Odbiorca weryfikuje podpis przy pomocy klucza publicznego nadawcy
- Wiadomo kto wysłał wiadomość i że to był dokładnie ta wiadomość
- To jeszcze nie jest podpis elektroniczny zgodnie z ustawą
 - patrz <http://www.certum.pl/>

Weryfikowanie klucza publicznego

- Ja jestem Jan Kowalski, a to jest mój klucz publiczny
 - uwierzyć, czy nie?
 - SSL, TLS
 - szyfrowany jest kanał komunikacji między serwerem, a użytkownikiem
 - chronimy hasło i login
 - pomiędzy serwerami (MTA) wiadomości przesyłane są normalnie
 - HTTPS
- Klucze publiczne też można podpisywać
 - podpisywanie wykonują organizacje Certificate Authority (CA)
 - klucze publiczne najważniejszych CA są ogólnie znane
- Zweryfikowany klucz publiczny może posłużyć do ustalenia klucza symetrycznego

Unieważnienie klucza publicznego

- Klucz publiczny można umieścić na publicznie dostępnym serwerze
- Unieważnienie (ang. revocation)
 - np. chcemy zacząć używać innej pary kluczy
 - wymaga klucza prywatnego i hasła
- Co jeżeli klucz prywatny lub hasło przepadły?
 - Czy może istnieć możliwość unieważnienia bez ich znajomości?
- Na podstawie klucza prywatnego i hasła można wygenerować certyfikat (ang. Key Revocation Certificate)