Електронна поща

Общи положения

Електронната поща (**e-mail** или **email)** е метод за обмен на електронни съобщения.

Едно съобщение се състои най-малко от съдържанието си, адрес на автора и адресите на един или повече получатели.

Корените на днешната email са в Arpanet – стандарт за кодиране на съобщения - RFC 733.

Преходът от Arpanet към Internet в началото на 1980-те добави постепенно новостите към основната услуга:

- транспортния протокол Simple Mail Transfer Protocol (SMTP), RFC 821 през 1982 г.

- ревизия на RFC 733 - RFC 822

- прикрепяния на мултимедия – от 1996 г. - от RFC 2045 до RFC 2049, известни като Multipurpose Internet Mail Extensions (MIME).

Общи положения

Email се базират на модела с пълно буфериране (store-and-forward).

Сървърът за електронна поща приема, препраща, доставя или съхранява съобщения за сметка на потребителите.

Тяхна задача е само да се свържат към email инфраструктурата с помощта на компютрите си.

Терминология

Mail-box – файл или директория/и от файлове, където се съхраняват входящите съобщения.

mail user agent (MUA) е приложна програма, стартирана от потребителя. Използва се за оформяне и изпращане на съобщения, както и за показване, сортиране като файлове и принтиране на получени в кутията съобщения. Такива са elm, mailx, mh, zmail, Mozilla Thunderbird, MS Outlook и др.

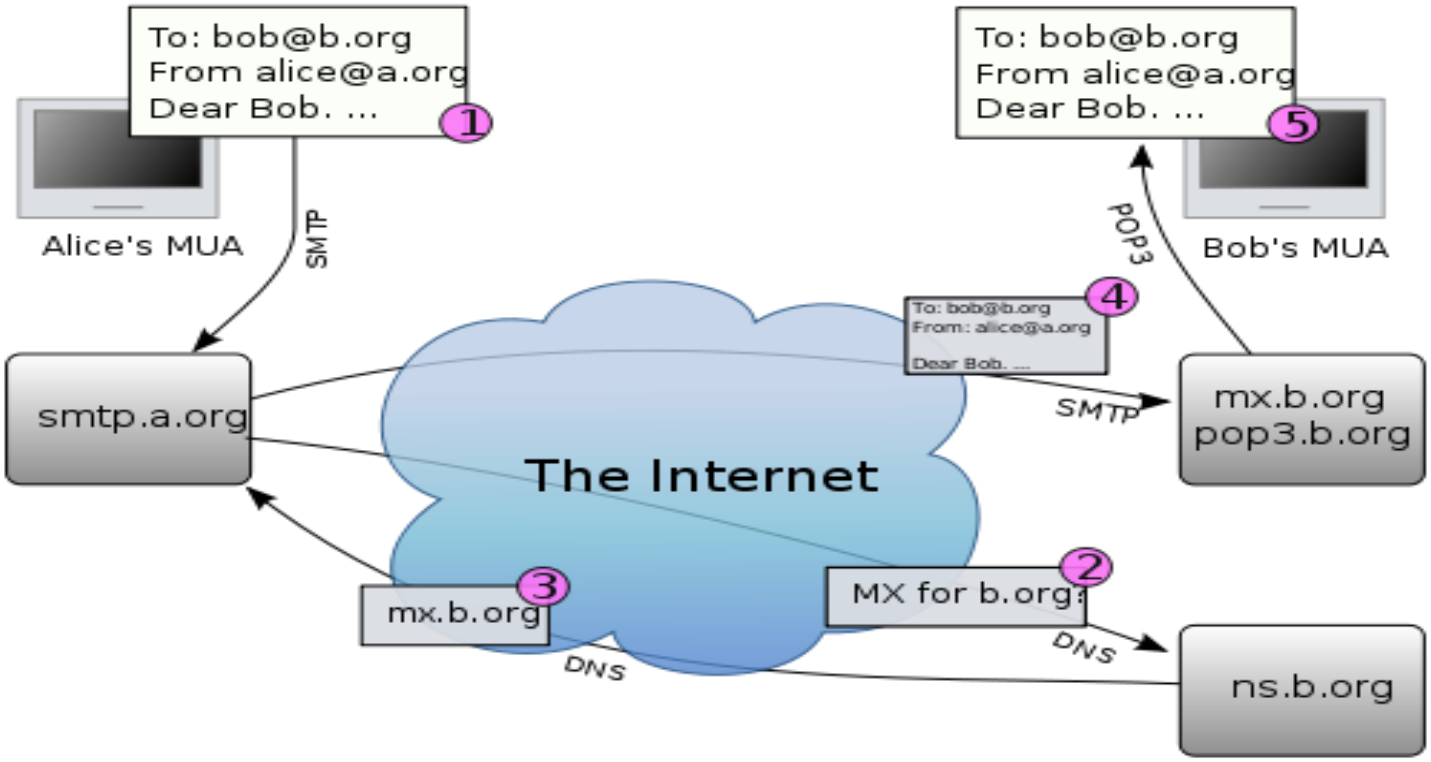
Терминология

Mail transfer agent (MTA) осъществява маршрутизацията на съобщенията, подадени от MUA, до получателя.

Най-популярният MTA е **sendmail**.

Delivery agent поставя съобщението в пощенската кутия на потребителя. Най-популярният DA е mail.local.

Alice си пише с Bob



Какво става

1. mail user agent (MUA) на Алис форматира съобщението в e-mail формат и с помощта на SMTP го изпраща към местния mail transfer agent (MTA) - smtp.a.org.
2. MTA гледа за крайния адрес, според SMTP протокола (а не в главата на съобщението) - bob@b.org. В e-mail адреса частта пред @ е локалната част, най-често потребителското име на получателя. Частта след @ е име на домейна. MTA по името на домейна определя пълното домейн име на пощенския сървър в DNS.
3. DNS сървърът за домейн b.org - ns.b.org, отговаря с MX записи, изброяващи пощенските сървъри в този домейн, в случая mx.b.org.
4. smtp.a.org изпраща съобщението до mx.b.org по SMTP, който го доставя до пощенската кутия (mailbox) на bob.
5. Bob натиска бутон "get mail" на своя MUA, с което изтегля съобщението с помощта на Post Office Protocol (POP3).

Алтернативи на последователността

- Alice може да няма MUA на компютъра си, а да се свърже към webmail услуга.
- На компютъра на Alice може да е “качен” MTA, т.е. да прескочи стъпка 1.
- Bob има много начини да изтегли пощата си, например, по протокол Internet Message Access Protocol, като се логне на mx.b.org и си я чете директно от там, или и той с webmail.
- В един домейн има няколко пощенски сървъра, така че те могат да продължат да приемат поща, даже когато главният е отпаднал.
- За повишаване на сигурността и конфиденциалността е добре пощата да се криптира (OpenPGP, X.500 сертификати). Но това е друга тема.

open mail relay

MTAs, които приемат съобщения от произволни податели и полагат максимални усилия да ги препратят по посока към получателите.

Такива MTAs се наричат open mail relay.

В зората на Internet, когато мрежите не бяха надеждни, това усилие беше похвално. Да може съобщението все пак да достигне целта си през един или повече relay.

Но от този механизъм се възползваха недобросъвестни “изпращачи” на спам и друга нерегламентирана поща.

Затова днешните MTAs не са open mail relays и не приемат поща от open mail relays, която си е чист спам.

Това важи и за сървърите СУ. Използваме и отворен софтуер SpamAssassin.

open relay denied (пример)

```
[stefan@shuttle ~]$ telnet email.uni-sofia.bg 25
Trying 62.44.101.22...
Connected to email.uni-sofia.bg (62.44.101.22).
Escape character is '^]'.
220 email.uni-sofia.bg ESMTP Postfix
HELO email.uni-sofia.bg
250 email.uni-sofia.bg
MAIL FROM:alabala@gmail.com
250 2.1.0 Ok
RCPT TO:abracadabra@yahoo.com
554 5.7.1 <abracadabra@yahoo.com>: Relay access denied
QUIT
221 2.0.0 Bye
```

Формати

Форматът на e-mail съобщенията е дефиниран в RFC 5322 и серия от RFC-та, RFC 2045 до RFC 2049, "Multipurpose Internet Mail Extensions" или MIME.

e-mail съобщенията се състоят от два основни дяла, отделени с празен ред:

Header (глава) Структурирано е от полета, обобщение (summary), подател (sender), получател (receiver) и др.

Body (тяло) Самото съобщение като неструктуриран текст. Понякога завършва и с “подпис”, signature block.

Полета в заглавието

Заглавието включва най-малко следните полета:

From: e-mail address и евентуално името на изпращача. При подателя се попълва автоматично.

To: Адрес(ите) и евентуално име(ната) на получател(ите).

CC: До кой да се изпрати видимо за получателя To: копие.

Bcc: Blind Carbon Copy До кой да се изпрати невидимо за получателя To: копие.

Subject: Или Относно: Предмета на съобщението.

Date: Дата и час на изпращане в локалното време. Поставя се автоматично.

Спекулации с "From"

С полето "From" може лесно да се заблуждава, затова се препоръчва да се ползва цифрово подписване (OpenPGP или X.500 сертификат).

Други важни полета

In-Reply-To: Message-ID на съобщението, на което настоящото е отговор.

Received: Проследява пътя, по който е минало съобщението, през кои пощенски сървъри. Показва кой е истинския подател по IP адрес.

References: Message-ID на това съобщение и на това, на което е отговор.

Reply-To: Адресът за отговор на подателя.

Пример. Заглавие на phishing съобщение

Subject: Уважаеми Uni-sofia.bg потребителски акаунт

From: Софийски университет <web-master@Uni-sofia.bg>

Date: Sun, March 21, 2010 13:22

To: undisclosed-recipients:;

Priority: Normal

Mailer: SquirrelMail/1.4.13

Пълно заглавие

Return-Path: <web-master@Uni-sofia.bg>

Received: from mailbox.uni-sofia.bg ([unix socket])

by mailbox.uni-sofia.bg (Cyrus v2.3.7-Invoca-RPM-2.3.7-7.el5_4.3) with LMTPA; Sun, 21 Mar 2010 13:22:36 +0200

X-Sieve: CMU Sieve 2.3

Received: from olc-11.verat.net (olc-11.verat.net [62.108.127.37])

by mailbox.uni-sofia.bg (8.13.8/8.13.8) with ESMTP id o2LBMYL9015117

for <stefan@ucc.uni-sofia.bg>; Sun, 21 Mar 2010 13:22:35 +0200

Пълно заглавие

Received: from webmail.verat.net (webmail.verat.net [85.222.160.153]) by olc-11.verat.net (Postfix) with ESMTP id D595BFC999; Sun, 21 Mar 2010 12:18:43 +0100 (CET)

Received: from 41.138.189.77(SquirrelMail authenticated user djmaxa) by webmail.verat.net with HTTP; Sun, 21 Mar 2010 12:22:33 +0100 (CET)

Message-ID: <3754.41.138.189.77.1269170553.squirrel@webmail.verat.net>

Date: Sun, 21 Mar 2010 12:22:33 +0100 (CET)

Пълно заглавие

Subject:

=?windows-1251?Q?=D3=E2=E0=E6=E0=E5=EC=E8_Uni-sofia.bg_

From: =?windows-1251?Q?=D1=EE=F4 ... =?windows-1251?Q?=E5=F2?= <web-master@Uni-sofia.bg>

Reply-To: w0642406@gmail.com

User-Agent: SquirrelMail/1.4.13

MIME-Version: 1.0

Content-Type: text/plain;charset=windows-1251

Content-Transfer-Encoding: 8bit

X-Priority: 3 (Normal)

Importance: Normal

Пълно заглавие

To: undisclosed-recipients:;

X-Spam-Status: No, score=-2.6 required=5.0 tests=BAYES_00 autolearn=ham

version=3.2.5

X-Spam-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on mailbox.uni-sofia.bg

Кодиране. UTF-8.

Първоначално E-mail е била 7-bit ASCII.

Стандартът MIME въведе предаване и на не-ASCII данни.

UTF-8 (8-bit UCS[1]/Unicode Transformation Format) е кодиране на знаците с променлива дължина за Unicode[2].

Представя всеки знак в Unicode стандарта, но същевременно е обратно съвместим с ASCII.

Затова става все по-предпочитан за e-mail, web и др.

UTF-8 кодира всеки знак (code point) с 1 до 4 байта, като с един байт се кодират 128 US-ASCII знаците.

Internet Mail Consortium (IMC) препоръчва всички email програми да са в състояние да изобразяват и създават поща с помощта UTF-8.

[1]Universal Character Set (UCS) **ISO/IEC 10646** стандарт, разработен съвместно с Unicode Consortium.

[2]Unicode осигурява уникален номер за всеки знак, независимо от платформата, независимо от програмата, независимо от езика.

UTF-8

Първите 128 знака (US-ASCII) им трябва 1 байт.

Следващите 1920 – 2 байта. Това са латински букви с диакрити, гръцки, кирилица, арменски, арабски, иврит и др.

3 байта са необходими за за останалите лингвистични знаци.

4 байта – за знаци в други равнини на Unicode, рядко използвани в практиката.

SMTP

Протоколът за изпращане на поща е **SMTP** (Simple Mail Transfer Protocol).

Базира се на транспортен протокол TCP.

От клиента, от порт с номер по-голям от 1024, се прави заявка за съединение към IP адреса на пощенския сървър на порт 25, т.е. порт 25 стои отворен в пощенския сървър и чака заявка за съединение.

Ако сървърът е в състояние да получи заявката, отговаря с 220, което означава готов.

След това клиентът изпраща съобщение HELLO, а при успех сървърът отговаря с 250.

SMTP

След това клиентът изпраща MAIL FROM (от кого е пощата), RCPT TO (кой е получателя) и накрая се прехвърля самото съобщение, след което връзката се разпада.

Описаното си е едно TCP/IP съединение. В неговите рамки се обменят ASCII съобщения, които са с определена структура.

Пример на SMTP сесия

По-долу имате един типичен пример на изпращане на съобщение по SMTP до две пощенски кутии (*alice* и *theboss*) в един и същ домейн (*example.com*).

“Репликите” на сървъра са означени със (*S:*), а на клиента - с (*C:*).

След като изпращачът на съобщението (SMTP client) установи надежден канал с получателя (SMTP server), сесията се отваря с поздравление от страна на сървъра.

Клиентът започва диалог, отговаряйки с команда HELO, в която се идентифицира.

Пример на SMTP сесия

S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>

Пример (прод.)

C: From: "Bob Example" <bob@example.org>
C: To: Alice Example <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 Jan 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: Bob
C: .

Пример (прод.)

S: 250 Ok: queued as 12345

C: QUIT

S: 221 Bye

{Сървърът затваря сесията}

sendmail и IPv6

Пакетът sendmail, който реализира SMTP, е компилиран с поддръжка на IPv6.

За IPv6 интеграция в SMTP се въвеждат следните опции:

DAEMON_OPTIONS(`Port=smtp,Addr=62.44.109.37, Name=MTA')dnl

DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl

DAEMON_OPTIONS(`Port=smtp,Addr=2001:67c:20d0:10::37, Name=MTA6, Family=inet6')dnl

DAEMON_OPTIONS(`Port=smtp,Addr=::1, Name=MTA6, Family=inet6')dnl

POP3

Крайният получател на писмото не е SMTP-сървъра. В него се събират изпратените писма до съответния домейн.

Сървърът трупа тези писма на диск при себе си.

С помощта на друг протокол крайният получател изтегля получените писма от пощенския сървър.

Например, **POP3** (Post Office Protocol). При него сървърът слуша на порт 110.

За разлика от SMTP, POP3 поддържа автентикация на клиента (username + password), т.е. притежателят на пощенската кутия е регистриран като POP3 потребител.

Когато клиентът се свърже към POP3 сървъра, той първо се идентифицира, след което може да извърши други команди за прочитане на получените от него mail-ове.

IMAP

Internet Message Access Protocol (IMAP или IMAP4) “слуша” на порт 143 и е другата възможност крайният клиент да получи достъп до пощата си, стояща на отдалечен сървър.

Сегашната версия, IMAP version 4 revision 1 (IMAP4rev1) е дефинирана в RFC 3501.

IMAP поддържа и online, и offline режими.

E-mail клиенти с IMAP оставят съобщенията на сървъра, докато потребителят не реши да ги изтрие.

IMAP позволява повече от един клиент да има достъп до една и съща пощенска кутия. Т.е. можете да имате достъп до пощата си едновременно от няколко места.

IMAP

За разлика от POP3, IMAP4 клиентите са свързани за сървъра, докато потребителският интерфейс е активен.

Потребителите изтеглят съобщения на диска си само по желание.

IMAP4 клиентите могат да създават, преименуват и/или изтриват пощенски кутии (потребителят ги вижда като папки) на сървъра и да местят съобщения между кутиите.

POP3 и IMAP услуги предлагат Cyrus IMAP server (http://cyrusimap.web.cmu.edu/) и Dovecot (www.dovecot.org).

IMAP4 команди

IMAP4 Commands

Command	Syntax	Description
AUTHENTICATE	a100 AUTHENTICATE method + challenge response + challenge response	Authenticates on the IMAP4 server via a secure authentication method.
LOGIN	a100 LOGIN username password	Authenitcates on the IMAP4 server via plaintext.
LIST	a102 LIST "" *	Lists contents of an account.
SELECT	a102 SELECT INBOX	Selects a mailbox.
EXAMINE	a102 EXAMINE INBOX	Returns statistics on a mailbox, without selecting it.
CREATE	a104 CREATE mailbox a104 CREATE directory\	Creates a new mailbox or directory hierarchy on the server. Note: "\" should match the hierarchy separator returned by the LIST command.
DELETE	a102 DELETE mailbox	Deletes a mailbox or a directory hierarchy.
RENAME	a102 RENAME mailbox name	Renames a mailbox or a directory hierarchy.

Документация на mail решение

Системата включва:

Sendmail за MTA

Cyrus за MDA

RedHat Directory Server за LDAP база за потребителски акаунти и конфигурация на sendmail

phpLDAPadmin - за външно управление на LDAP директорията

Saslauthd за посредник между cyrus и LDAP базата

Документация (прод.)

Spamassassin за антиспам защита.
(*Използва шаблони, по които анализира съдържанието на пощата и го класифицира като спам или не. Подлежи на самообучение.*)

Clamav за антивирусна защита

http://www.mimedefang.org/ за връзка на sendmail с антивирусната защита и за допълнителни филтри

SquirrelMail и HastyMail за уеб достъп до пощенските кутии.

Алгоритъм на MX йерархия в DNS.

...

$ORIGIN domain.uni-sofia.bg.

MX 10 mail.*faculty*.uni-sofia.bg

MX 20 ns.uni-sofia.bg.

MX 20 ady.uni-sofia.bg.

MX йерархия

Съгласно горната MX йерархия при иницииране на сесия за предаване на писмо към получател с пощенска кутия в домейна *faculty*.uni-sofia.bg:

- опит да се установи SMTP сесия към mail.*faculty*.uni-sofia.bg. Ако този опит пропадне:

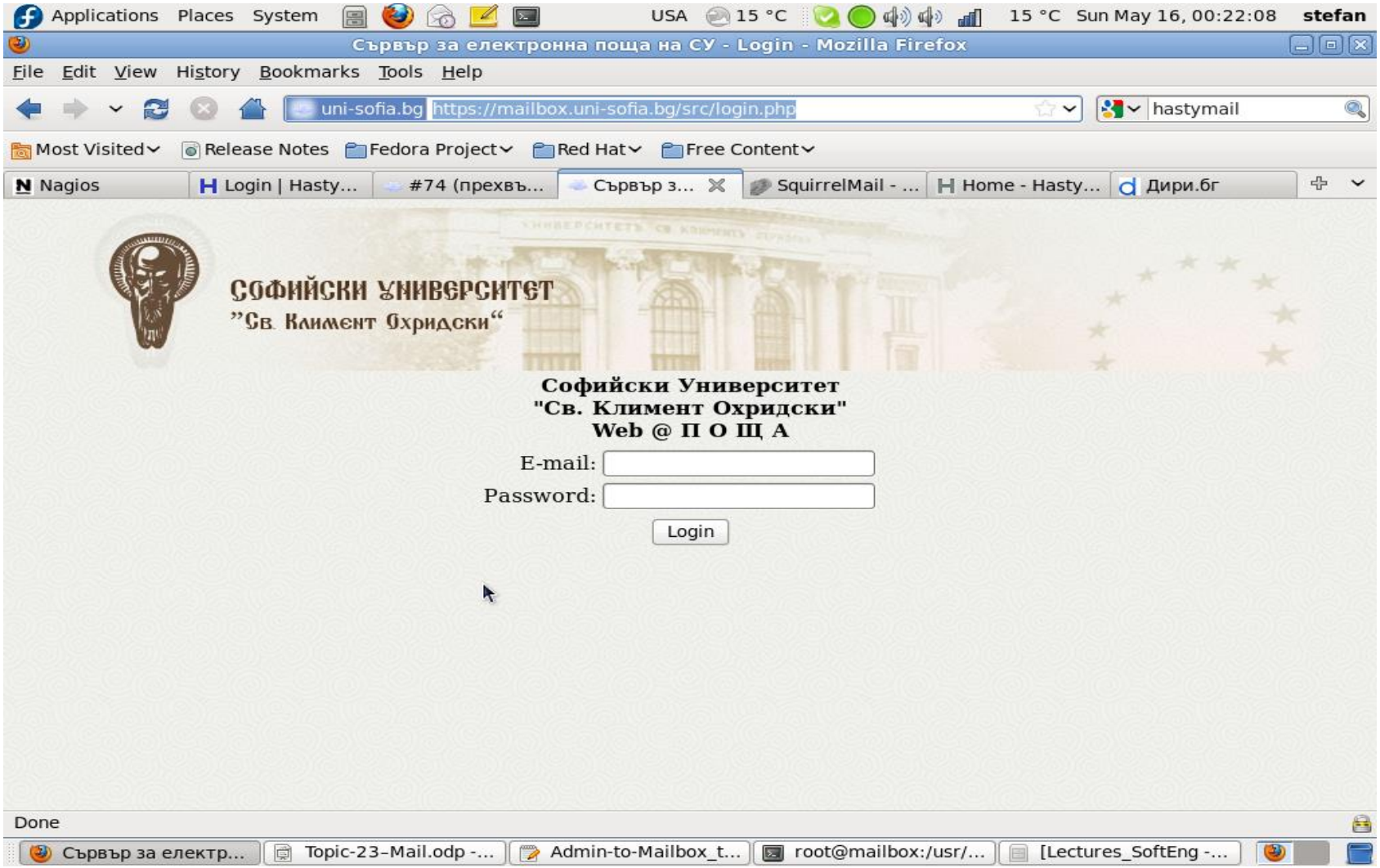
- установяване на SMTP сесия към един от двата SMTP сървъра, с MX приоритет 20 (ns.uni-sofia.bg или ady.uni-sofia.bg).

SquirrelMail и Hastymail

squirrelmail.org е с вградена PHP поддръжка за IMAP и SMTP, страниците са чист HTML 4.0 (не е необходим JavaScript) за съвместимост с всички браузъри.
mailbox.uni-sofia.bg

hastymail.org - IMAP/SMTP клиент, писан на PHP. Съвместим с PDAs, мобилни апарати, текстови и други браузъри.
mailbox.uni-sofia.bg/mobile

https://mailbox.uni-sofia.bg/src/login.php



config.php

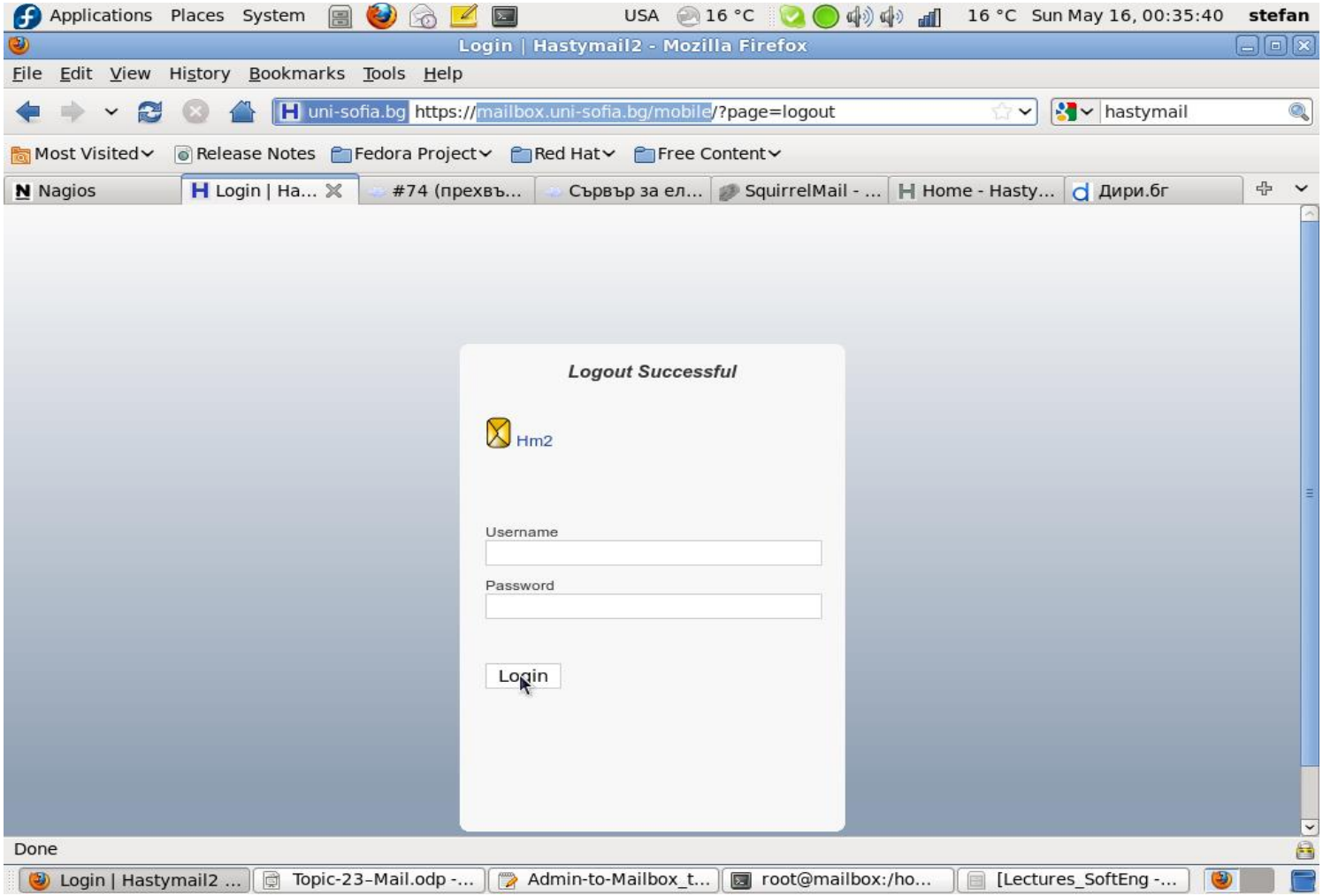
```
<?php

/**
 * SquirrelMail Configuration File
 * Created using the configure script, conf.pl
 */

global $version;
$config_version = '1.4.0';
$config_use_color = 1;

$org_name      = "Софийски Университет<br/>\"Св. Климент Охридски\"<br/>Web
@ П О Щ А";
$org_logo      = SM_PATH . 'images/logo_su.jpg';
$org_logo_width  = '940';
$org_logo_height = '145';
```

https://mailbox.uni-sofia.bg/mobile/



index.php

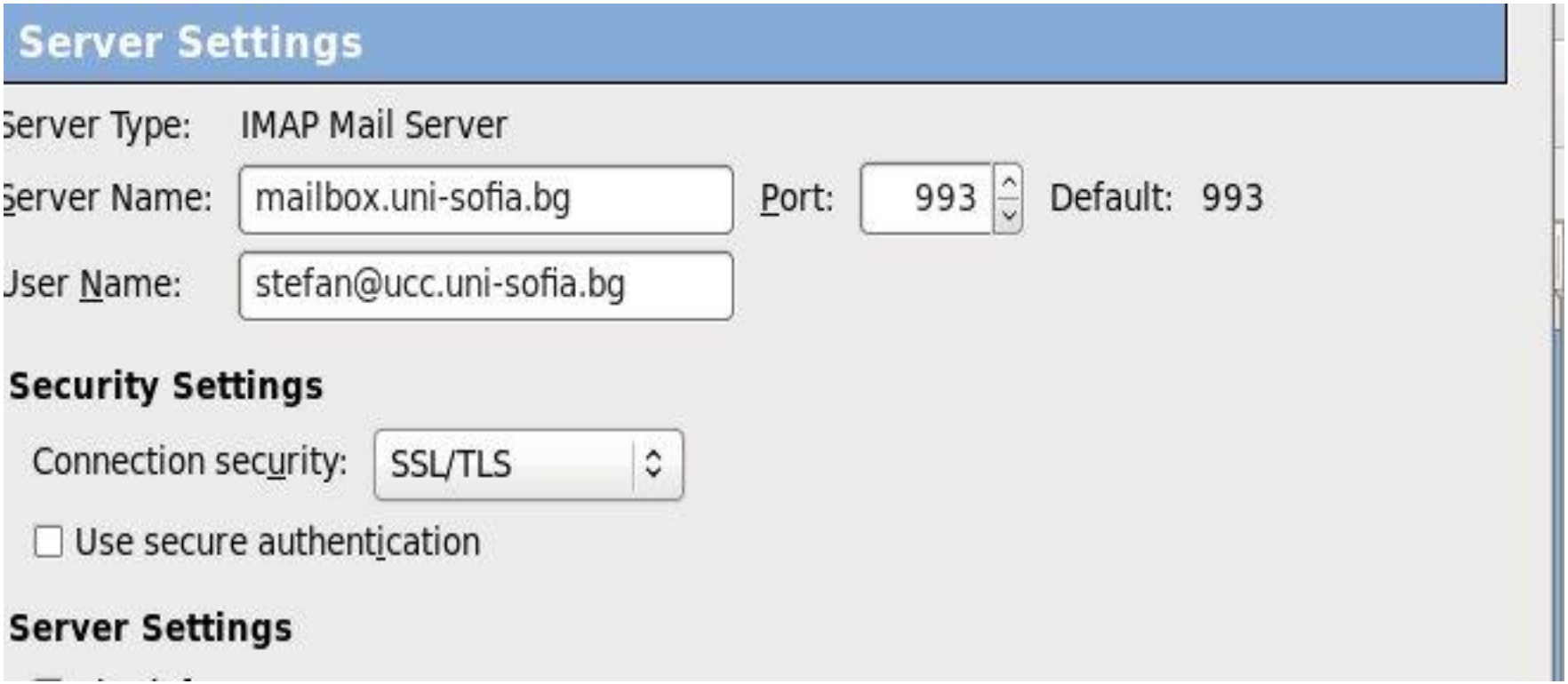
```
/* configuration file */
$hm2_config = '/etc/hastymail2/hastymail2.rc';

/* capture any accidental output */
ob_start();

/* timer debug prep */
$page_start = microtime();

/* required includes */
require_once('lib/misc_functions.php');    /* various helpers */
require_once('lib/utility_classes.php');   /* base classes */
require_once('lib/url_action_class.php');  /* GET processing */
require_once('lib/imap_class.php');              /* IMAP routines */
require_once('lib/site_page_class.php');   /* print functions */
```

Защитена поща. IMAPS.



Защитена поща. SMTPS.

Защитена поща*

Secure SMTP (SSMTP) - port 465

IMAP4 over SSL (IMAPS) - port 993

Паролата и потребителското име са криптирани при преноса им до сървъра.

Служебната информация, отнасяща се до съдържанието на писмата и процедурите на протокола (SMTP / IMAP), се пренася в Интернет в криптиран вид!

**Ако провайдерът ви го осигури.*

CAPTCHA

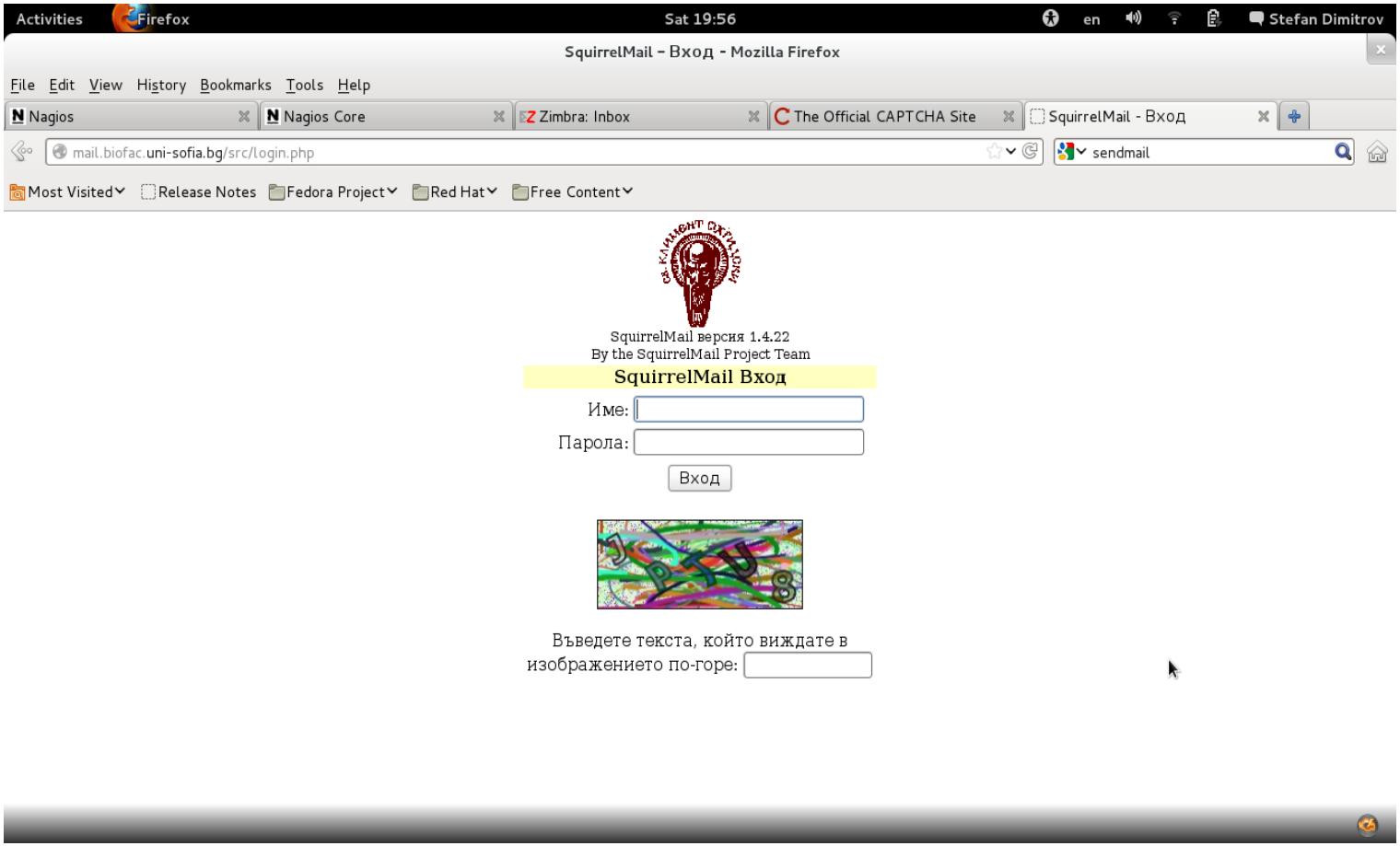
CAPTCHA

CAPTCHA (**C**ompletely **A**utomated **P**ublic **T**uring Test To Tell **C**omputers and **H**umans **A**part) е създадена през 2000 г. от Luis von Ahn, Manuel Blum, Nicholas Hopper и John Langford (Carnegie Mellon University).

Програма за защита на web сайтове (вкл. Webmail), генерираща тестове, които могат да се изпълняват от хора, но не и от компютърни програми.

Напр., разкривен текст.

Squirrelmail: captcha + lockout



Squirrelmail: captcha + lockout

cd /usr/share/squirrelmail/plugins/lockout/

cd data

vi config.php

...

логин опити на ip - max 10 за 15 min, при Превишаване – 30 min lockdown

$max_login_attempts_per_IP = '10:15:30';

...

Squirrelmail: captcha + lockout

да се активира captcha - след 5 неуспешни опита в рамките на 10мин;

captcha ще е активна за 30мин;

1=при успешно логване captcha се деактивира

$activate_CAPTCHA_after_failed_attempts = '5:10:30:1';

Squirrelmail: captcha + lockout

cd /usr/share/squirrelmail/plugins/captcha/

vi config.php

има подробен списък с видовете captcha и изисванията, настройките за тях

...

* @package plugins

* @subpackage captcha

DNSBL (срещу спама)

Domain Name System Blacklists (**DNSBL**) са списъци с IP адреси и мрежи, излъчватели на **спам**.

Позволяват на администраторите да блокират съобщения от тях.

Възможен е субективизъм при изготвянето им.

Spamassassin напр. ползва DNSBL.

DNSBL

Базата с IP адреси или мрежи на източници се съхранява в DNS зона на домейн (напр. dnsbl.uni-sofia.bg).

За всеки IP адрес или мрежа от IP адреси се изгражда **A** ресурсен запис към IP адрес от 127.0.0.0/8.

Ресурсният A запис следва синтаксиса на in-addr.arpa представянето.

dnsbl.uni-sofia.bg

```
$ORIGIN .
$TTL 86400      ; 1 day
dnsbl.uni-sofia.bg      IN SOA  ns.uni-sofia.bg.
   root.ns.uni-sofia.bg. (
                                2006288400 ; serial
$ORIGIN dnsbl.uni-sofia.bg.
...
$TTL 60 ; 1 minute
80.124.108.111          A       127.0.0.2
```

#IP: 111.108.124.80 >> 80.124.108.111.dnsbl.uni-sofia.bg.