

# Elektronický poštový systém

Mária Matušisková

Slovenská technická univerzita v Bratislave  
Fakulta informatiky a informačných technológií  
Vedúci: Ing. Fedor Lehocki

18.október 2021

## Abstrakt

E-mail môžeme považovať za predchodcu internetu a hral významnú rolu pri jeho vzniku. Dnes je používanie e-mailov bežná súčasť nášho života, tak ako je dôležité mať telefónne číslo, rovnako je podstatné mať aj e-mailovú adresu.

V tomto dokumente sa zaoberáme vznikom prvej elektronickej pošty. Ako fungovala na jej počiatkoch a dnes. Povieme si o štruktúre mailového systému a jeho protokoloch ako SMTP, IMAP či POP. Zásadným bodom projektu je objasnenie algoritmu odosielania elektronickej pošty, čo všetko sa odohráva za jediným kliknutím „odoslať“. Následne si priblížime bezpečnosť a filtrovanie spamov, ako mailové servery chránia používateľov pred malvermi a vírusmi.

*Kľúčové slová: e-mail; e-mailový server; IMAP; SMTP; POP; algoritmus e-mailu*

## 1 Úvod

E-mail je elektrické odosielanie a prijímanie správ medzi dvoma alebo viacerými adresátmi. Vznik e-mailu sa datuje koncom 20.storočia. Presnejšie v roku 1971, kde prvý uznávaný e-mail poslal Raymond Tomplinson z jedného počítača na druhý pomocou organizácie ARPANET. A odvtedy sa odštartovala nová etapa dorozumievania sa medzi ľuďmi.

Táto komunikácia by však nemohla fungovať bez protokolov ako IMAP, POP, SMTP. Ich úlohou je odoslať správu na druhý server, teda prijímateľovi správy. Adresát si tak vie správu otvoriť, prečítať a uložiť.

Štruktúra e-mailu je však omnoho komplikovanejšia, než si myslíme. Začína už len formatovaním pri zadávaní správy. Ako prvú informáciu zadávame komu chceme odkaz odoslať, ktorej e-mailovej adrese. Následne napíšeme predmet obsahu správy, o čom daná informácie bude. A nakoniec vypíšeme takzvané telo (body) správy, kde už je samotný obsah, môže sa tam nachádzať text alebo príloha. Tento formát sa nazýva MIME (viacúčelové rozšírenie internetovej pošty).

S rozvojom e-mailov sa vyvinulo aj ich zabezpečenie. V niektorých prichádzajúcich mailoch sa vyskytujú vírusy, ktoré sa môžu rozšíriť aj do zariadenia adresáta. Osoba, ktorá tieto správy odosiela sa označuje ako spammer a nevyžiadaná pošta sa označuje ako SPAM. Na vyvarovanie sa pred týmito správami vznikol systém, ktorý filtruje a šifruje informácie na zvýšenie bezpečnosti pre používateľov.

Záleží aj od e-mailovej domény, ktorú adresát používa. V tomto článku si povieme aj o najpoužívanejších z nich.

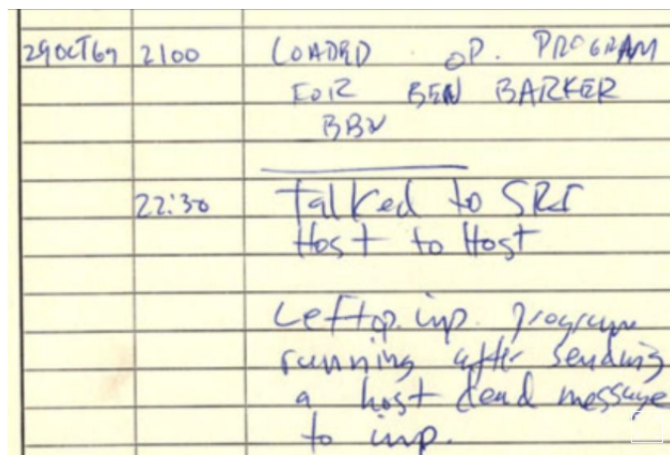
Dôležité súvislosti sú uvedené v kapitolách 3 a 4.

Záverečné poznámky prináša časť 7.

## 2 Vznik e-mailu

So vznikom e-mailu sa najviac spája meno Ray Tomlinson alebo spoločnosť ARPANET. Táto organizácia bola sieť, ktorá spájala rad počítačov po celom oddelení a bola vytvorená agentúrou DARPA (Defense Advanced Research Agency), ktorá patrila pod ministerstvo obrany USA. Účelom zriadenia výskumnej organizácie ARPANET bolo udržanie technologického pokroku oproti súperiacemu Rusku, hlavne po úspešnej misii Sputnik.

Historicky prvý e-mail sa poslal 29. októbra 1969 o pol jedenástej večer a to práve sieťou ARPANET. Správa bola odoslaná študentom programovania menom Charlye Kline z počítača, ktorý patril Leonardovy Kleinrockému do počítača Stanfordského výskumného ústavu.



Obr. 1: Prvá odoslaná elektronická správa [4]

Reálnu podobu systému odosielanie e-mailov akú poznáme dnes však vynášiel **Ray Tomlinson** v roku 1971. Dostal nápad skombinovať správu so systémom CPYNET (program určený na odosielanie súborov do druhého PC) cez sieť ARPANET:

„V CPYNET proces používania prechádza cez Initial Connection Protocol (ICP) do servera socketu 7, čím sa vytvorí plne duplexné pripojenie s veľkosťou 8 bitov. Riadiace informácie vrátane používateľského mena, hesla, príkazu (čítanie, zápis alebo pridanie), názvu súboru a veľkosti bajtu pre dátové pripojenie sa prenášajú z procesu používania do procesu poskytovania. Pôvodné plne duplexné pripojenie sa potom uzavrie a vytvorí sa nové plne duplexné pripojenie s použitím pôvodných čísel socketu, ale s možnou inou veľkosťou bajtu. Súbor sa teraz prenáša na toto novo vytvorené spojenie. Koniec súboru je indikovaný zatvorením spojenia. [3]“

Vymyslel tiež systém pre identifikáciu adresy druhého počítača, kde sa meno používateľa oddeľuje od počítačového serveru za pomoci symbolu @ (at): „používateľskémeno@menopočítača“.

Bol to taký úspech, že do roku 1976 sa v organizácii ARPANET využíval tento systém na 75% prevádzky. Postupom času sa začala riešiť nová problematika e-mailu. Spoločnosť chcela, aby sa elektronická pošta dala odoslať aj mimo internej siete a práve táto požiadavka motivovala myšlienku vzniku internetu.

Na verejnej konferencii ICC (International Computer Communication Conference) v roku 1972 ARPANET prvýkrát verejne predviedol túto myšlienku spolu s novinkou e-mailu. Už v roku 1973 sa internet stal medzinárodným spojením a to medzi USA a Spojením Kráľovstvom. Úplnej verejnosti sa odprezentoval v roku 1983. ARPANET môžeme teda považovať ako predchodcu Internetu.

Elektrická pošta sa rozšírila internacionálne v počiatkoch Internetu 80. rokov. Poskytovatelia internetových služieb začali vytvárať e-mailové hostingové stránky pre spájanie ľudí na celom svete.

V roku 1993 bola vynájdená bezdrôtová sieť (Wi-fi) čo túto službu ešte viac rozšírilo a do popredia sa dostali e-mailové servery ako AmericaOnline (AOL), EchoMail, Hotmail a Yahoo. [4, 6, 8]

### 3 E-mailový systém

Na fungovanie e-mailu potrebujeme aplikačné softvéry na prijímanie, ukladanie a odosielanie správ. Takzvanú elektronickú schránku – mailbox. Poznáme súkromné (lokálne) a webové servery.

- súkromné servery
  - Aplikácia je nainštalovaná v počítači a e-maily sú uložené priamo v zariadení. Nevýhodou je, že prístup k správam je obmedzený, nedá sa pripojiť k serveru z iného zariadenia, ktoré nie je prihlásené na túto aplikáciu. Tento server je však bezpečnejší oproti webovému, pretože je súkromnejší. Dáta sa ukladajú do PC a nie na web. Využíva sa hlavne vo firmách a v podnikoch. Príkladom môžu byť aplikácie Microsoft Outlook, Thunderbird a ProtonMail.
- webové servery
  - Používateľ má prístup k mailovej schránke z rôzneho zariadenia, pretože server je na webovej adrese. Dáta sa ukladajú na web, je však menej bezpečnejší ako súkromný server. Príkladom sú služby ako Gmail, Yahoo a Webmail.

E-mailový systém funguje na vzájomnom prepojení protokolov a služieb. [5]

#### 3.1 Služby

**UA (User Agent) /používateľská služba** – Adresát 1 vytvorí správu a odošle ju Adresátovi 2. Úlohou UA je vytvorenie a uloženie správy do mailovej schránky používateľa. U Adresáta 1 sa správa uloží ako odoslaná respektíve vytvorená a u Adresáta 2 sa správa uloží ako doručená. [5]

**MTA (The Message Transfer Agent)/služba prenosu súborov** – Nie vždy platí pravidlo, že druhý Adresát má rovnaký mailový server. Úlohou MTA je spracovávanie spojenia medzi dvoma Adresátmi. Kontroluje adresu mailového serveru Adresáta, ktorý správu odoslal a následne adresu servera komu je správa odoslaná. Napríklad: *menopouzivatela@gmail.com* → *menopouzivatela@yahoo.com*

**Systém názov domén DNS (The Domain Name System)** – Odošle sa názov domény patriaci Adresátovi 2, potom sa názov domény preloží na IP a používa sa na mapovanie správy zo servera Adresáta 1 na server Adresáta 2. [5, 9]

**MAA (Message Access Agent)/služba prístupu k správam** – Adresáti nie sú vždy prítomní na serveroch súčasne. Táto služba zabezpečuje načítanie e-mailu adresátom v danom čase, keď sa nachádzajú na servery alebo keď sú pripojení na sieť. [5]

#### 3.2 Protokoly

Na doručovanie e-mailov používame protokoly a každý protokol má náležitú funkciu. Najpoužívanejšie sú SMTP, POP, IMAP, ktoré patria pod TCP/IP (Transmission Control Protocol/Internet Protocol). [5]

##### 3.2.1 SMTP (Simple Mail Transfer Protocol)

Je jednoduchý protokol na prenos elektronickej pošty cez internet. Pre lepšie pochopenie ho môžeme vnímať ako jazyk e-mailových serverov. Jeho hlavnou funkciou je zabezpečenie správy. Aby sa odkaz **doručil** určenému používateľovi a aby mal adresát istotu, že daný odkaz prijal od tej istej osoby. Overuje adresy domén používateľov a snaží sa tak zabrániť zneužitiu e-mailov. Ďalšou funkciou je šifrovanie správy, aby sa správa neodoslala len ako bežný čitateľný text.

Funguje ako priebeh odosielateľa/prijemcu, kde odosielateľ odošle príkazy (správu) a server ich vykoná, vráti kód odpovede (stavu) v prípade potreby. Ak prijímateľ akceptuje prichádzajúcu správu stáva sa odosielateľom SMTP. [5, 7, 9]

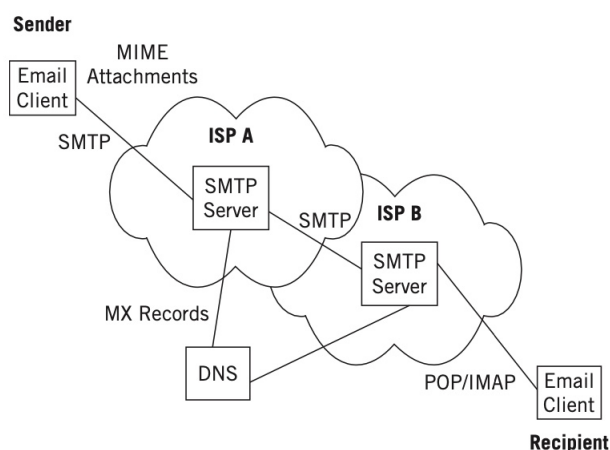
### 3.2.2 POP (Post Office Protocol)

Momentálne najaktuálnejším protokolom je POP3, je určený hlavne pre občasných používateľov e-mailu. POP3 neposiela e-mail, to ma za úlohu SMTP. Jeho hlavnou funkciou je overenie správnosti správy a následne vymazanie (ak nespĺňa protokol) alebo zobrazenie správy prijímateľovi.

Prijímateľ musí e-mail stiahnuť zo servera do zariadenia, nedá sa skontrolovať predtým, najprv sa stiahne až potom otvorí. Dôsledkom môže byť zachytenie vírusu či malvéru. Odoslané alebo vymazané správy sa stiahnuť nedajú a nie je možná organizácia súborov na servery. Nevýhodou tiež je, že automaticky po stiahnutí sa e-mail vymaže zo servera a už k nemu používateľ viac nemá prístup na opätovné stiahnutie. Výhodou ale je, že adresát má prístup ku e-mailom aj offline a šetrí internetový priestor. Je jednoduchší než IMAP. [2, 5]

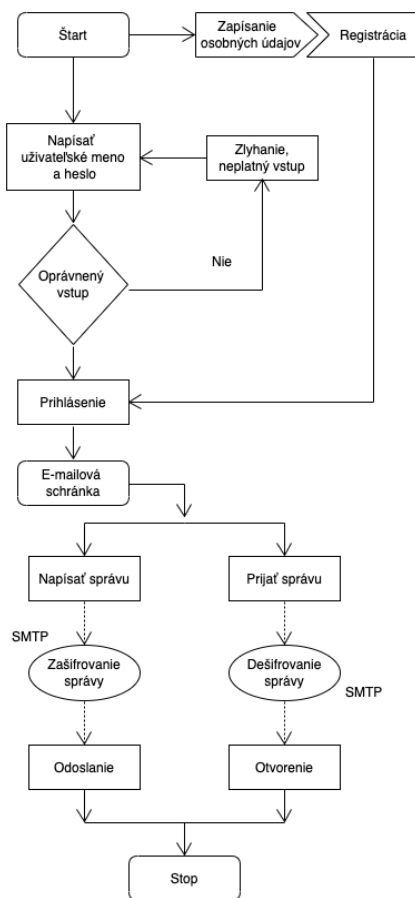
### 3.2.3 IMAP (Internet Message Access Protocol)

Používateľ má prístup k elektronickej pošte cez internet vo forme webového prehliadača. E-mail môže otvoriť na viacerých zariadeniach súčasne bez toho, aby ich musel sťahovať. Možnosť triedenia a organizácie mailov do priečinkov. Spotrebuje viac CPU a pamäti než POP3, pretože ukladá dáta do vyrovnávacej pamäte. Najviac zaberá miesta pri synchronizácii. Najaktuálnejší protokol je IMAP4 a je zložitejší a drahší ako POP3. [2]



Obr. 2: Zobrazenie prepojenia protokolov [5]

## 4 Algoritmus e-mailu



Obr. 3: Vývojový diagram  
(vlastná tvorba, inšpirácia - citácia) [1]

Do e-mailovej schránky sa dostaneme štandardným vstupom a to overením ID pošty používateľa.

Ak používateľ nemá založený účet na e-mailovom serveri, mal by si založiť účet. Základom je zapísanie osobných údajov používateľa a následná registrácia. Vďaka tomu softvér môže overiť ID používateľa a tak zvýšiť bezpečnosť dôveryhodnosti.

Ak je používateľ už zaregistrovaný, môže sa opakovane prihlasovať do jeho osobnej e-mailovej schránky. Pri každom prihlasovaní systém kontroluje ID používateľa cez vstup. Ak je zadané heslo nesprávne, program si vypýta zadanie údajov znova. Po prihlásení je užívateľ prenesený do prideleného e-mailového prostredia.

Hlavnou myšlienkou elektronickej pošty je výmena správ medzi dvoma adresátmi. Používateľ ma teda možnosť odoslať správu ďalším používateľom alebo prijať správu od ostatných používateľov.

Pri napísaní a posielaní správy, systém najprv správu zašifruje, aby sa tak zvýšila bezpečnosť pred tretími stranami. O túto problematiku sa stará protokol SMTP. Zašifrovaná správa sa odošle určeným adresátom a keď sa im doručí automaticky sa im dešifruje. [1]

## **5 Zabezpečenie a filtrácia spamov**

## **6 Súčasná podoba e-mailu**

### **6.1 Najpoužívanéjšie e-mailové servery**

## **7 Záver**

## Literatúra

- [1] S. Acharya, A. Gomes, D. Suvarna, and T. Paulson. Smart mailing system for secure transmissions, 2014.
- [2] S. Ali. Email protocols. In *Performance Evaluation of IMAP and POP3 Protocols Using Optimized Network Engineering Tool (OPNET)*, 2020.
- [3] A. Bhushan. Another look at data and file transfer protocols. Technical report, Network Working Group, MIT-MAC, Apr. 1972.
- [4] Daniel Uria. First internet connection made over military arpanet 50 years ago. <https://tinyurl.com/san4jsvk>, Oct. 2019.
- [5] W. Goralski. Chapter 25 - smtp and email. In W. Goralski, editor, *The Illustrated Network (Second Edition)*, pages 637–659. Morgan Kaufmann, Boston, second edition edition, 2017.
- [6] L. Kleinrock. History of the internet and its flexible future. *History of the Internet and its flexible future*, 15(1):8–18, Feb. 2008.
- [7] N. V. Pakulin, A. N. Tugaenko, and V. Z. Shnitman. Model-based testing of internet e-mail protocols. *Programming and Computer Software volume*, 38(5):268–275, Sept. 2012.
- [8] Phrasee Brand Language Optimization. A brief history of email: Dedicated to ray tomlinson. <https://www.phrasee.co/blog/a-brief-history-of-email/>, Sept. 2021.
- [9] R. Sureswaran, H. A. Bazar, O. Abouabdalla, A. M. Manasrah, and H. El-Taj. Active e-mail system SMTP protocol monitoring algorithm. In *Active e-mail system SMTP protocol monitoring algorithm*. IEEE, Oct. 2009.