Elektronická pošta

Elektronická pošta

Je to způsob odesílání, doručování a přijímání zpráv přes elektronické komunikační systémy, je založený na protokolu SMTP (Simple Mail Transfer Protocol). Lze ho využít kromě Internetu také tak i pro intranetové systémy.

Historie

- Elektronická pošta vznikla v roce 1965 jako způsob komunikace více uživatelů mainframového počítače.
- Systémy AUTODIN první, které umožňovaly přenos elektronických textových zpráv mezi různými počítači (1966).
- Ray Tomlinson začal v rámci ARPANETUv roce 1972 používat znak @ na oddělení jména uživatele od názvu stroje. Velká obliba elektronické pošty v rámci ARPANETu.
- Dříve nebyly všechny počítače nebo sítě navzájem síťově propojené, e-mailové adresy musely obsahovat „cestu“ pro zprávu, t.j. trasu mezi počítačem odesílatele a příjemce. Tímto způsobem bylo možné posílat e-maily mezi více sítěmi. Cestu specifikovala tzv. „bang path“ adresa, která již specifikovala skoky (hops) mezi lokacemi, které byly považované za dostupné adresátovi. Používalo se vytáčených spojení pracující v nočních hodinách způsobovala týden dlouhé přenosy. Bang cesty se volily často podle času přenosu a spolehlivosti, takže se zprávy často ztrácely.

Technické principy

Komunikační protokoly

Mezi počítači na internetu se vyměňují zprávy pomocí Simple Mail Transfer Protocol a SW M TA.

Uživatelé mívají na svém počítači nainstalován program, který se nazývá e-mailový klient. Ten stahuje zprávy z poštovního serveru použitím protokolů POP nebo IMAP, existují komerční protokoly jako např. Lotus Notes neebo Microsoft Exchange Server.

E-maily lze ukládat buď na straně serveru, nebo na straně klienta. Jelikož jsou to data, tak jsou uložena v souborech. Existují dva základní formáty (způsob organizace emailů v soborech) pro mailové schránky Maildir a mbox. Několik e-mailových klientů používá vlastní formát a na konverzaci mezi těmito formáty je potřebný speciální program.

MBOX

- souborový formát pro skladování elektronické pošty.
- Všem e-mailům, které jsou v poštovním klientu uloženy v jedné složky, odpovídá jeden MBOX soubor. E-maily jsou v tomto souboru uloženy v textové podobě za sebou.
- Používají jej poštovní klienti založené na Mozille (např. Mozilla Thunderbird) či Eudora.

Maildir

- je široce používaný formát pro uložení e-mailových zpráv.
- Každá zpráva je uložena jako samostatný soubor s unikátním názvem.
- Všechny změny se provádějí pomocí atomických(dílčích) souborových operací.
- Současný vícenásobným přístup.
- Maildir je adresář (často nazvaný Maildir) se třemi podadresáři nazvanými tmp, new a cur.

Jak funguje e-mail

Někteří uživatelé nepoužívají e-mailového klienta, ale přistupují ke zprávám umístěným na poštovním serveru přes webové rozhraní. Tento postup se často používá zejména u freemailových (bezplatných) služeb.

Při posílání pošty přes internet má být zaručen spolehlivý přenos zprávy i v případě dočasného výpadku cílového serveru. Zpráva se obvykle píše v prostředí programu typu e-mailového klienta nebo v obdobném formuláři webového rozhraní. Klient pomocí Simple Mail Transfer Protocol (SMTP) pošle zprávu programu Mail Transfer Agent (MTA).

Program MTA zjistí z uvedených cílových adres název domény (část adresy za zavináčem) a tyto domény vyhledá v Domain Name System (DNS). DNS server domény odpoví a uvede mail exchange server pro danou doménu.

MTA server odešle zprávu na mail exchange server pomocí protokolu SMTP. Domény obvykle mají záložní mail exchange server, takže můžou pokračovat v přijímaní pošty, i když je právě nedostupný hlavní mail exchange server. Když není možné zprávu doručit, MTA příjemce o tom musí odeslat zpět odesílateli zprávu (en:bounce message), ve které ukazuje na problém.

Mail exchange server zprávu doručí do schránky adresáta.

Ze schránky adresáta si zprávu stáhne pomocí protokolu POP (POP3) nebo IMAP nebo ji adresátovi umožní prohlédnout poštovní klient příjemce nebo webová služba.

POP3

POP3 (Post Office Protocol version 3) je internetový protokol, který se používá pro stahování emailových zpráv ze vzdáleného serveru na klienta. Jedná se o aplikační protokol pracující přes TCP/IP připojení. POP3 protokol byl standardizován v roce 1996.

POP3 je následníkem protokolů POP1 a POP2. Ze vzdáleného serveru se stáhnou všechny zprávy, třeba i ty, které uživatel číst nechce, nebo spam (pokud ho již nefiltruje poštovní server). Většina POP3 serverů sice umožňuje stáhnout i pouze hlavičky zpráv (a následně vybrat zprávy, které se stáhnou celé), ale podpora v klientech vesměs chybí. POP3

neumožňuje zabezpečený přenos hesel, ale podporuje současně několik autentizačních metod tj. ověřování před neoprávněným přístupem k cizí poštovní schránce.

Komunikace protokolu probíhá na principu výměny zpráv mezi klientem a serverem. Příkaz vždy začíná na začátku řádky, v základní implementaci POP3 mají příkazy 3 nebo 4 znaky. Za příkazem můžou následovat další argumenty, oddělené mezerami. Každá odpověď od serveru musí začínat indikací stavu operace - buď +OK, nebo -ERR. Následovat může textový řetězec s popsaným důvodem stavu.

IMAP

IMAP (Internet Message Access Protocol) je internetový protokol pro vzdálený přístup k e-mailové schránce. Na rozdíl od protokolu POP3 vyžaduje IMAP trvalé připojení (tzv. on-line), avšak nabízí pokročilé možnosti vzdálené správy (práce se složkami, přesouvání zpráv, prohledávání na straně serveru a podobně). V současné době se používá protokol IMAP4. Na rozdíl od starších Internetových protokolů, má IMAP4 zabudovanou podporu šifrovaného přihlášení. Možný je i přenos nezakódovaného hesla.

Protokol IMAP vyžaduje trvalé (tzv. on-line) připojení k e-mailové schránce. Díky tomu je možné s celou poštovní schránkou plně pracovat z libovolného místa. Všechny zprávy a složky jsou uloženy na poštovním serveru a na počítač se stahují jen nezbytné informace, takže při zobrazení složky se stáhnou jen záhlaví zpráv a jejich obsah až v případě, že zprávu chce uživatel přečíst. U jednotlivých zpráv se uchovává jejich stav (nepřečtená, odpovězená, důležitá), uživatel může zprávy přesouvat mezi složkami, složky vytvářet, mazat, prohledávat na straně serveru apod. Protokol umožňuje současné připojení více klientů zároveň.

Výhody a nevýhody IMAP

Pokud používáme POP3, klienti se připojí na server pouze na tak dlouho, aby si stáhli novou poštu. Pro použití IMAP4 jsou klienti připojeni tak dlouho, dokud je aktivní uživatelské rozhraní, stahování zpráv je závislé na požadavcích. Pro uživatele s mnoha nebo s velkými e-maily je tento způsob rychlejší.

Protokol POP3 dovoluje připojení pouze jednoho uživatele ke schránce. IMAP dovoluje současné připojení více uživatelů k jedné schránce, a umožňuje vidět změny provedené ostatními klienty.

Poskytuje Informace o stavu zprávy zda byla přečtena, či bylo na ni odpovězeno, nebo byla smazána.

IMAP4 poskytuje klientům mechanismus, kterým mohou vyhledávat na serveru zprávy podle různých kritérií. Tento mechanismus dovoluje klientům vyhledávat přímo na serveru, bez nutnosti poštu stáhnout.

Mezi nevýhody protokolu IMAP je složitější implementace(začlenění do emailového klienta) s tím spojena větší možnost chyb.

Formát e-mailové zprávy

Původně je e-mail definován pro přenos pomocí 7bitové ASCII informace. Přesto je většina e-mailových přenosů 8bitových, kde ale nelze zaručit bezproblémovost. Z toho důvodu byla elektronická pošta rozšířena o standard MIME, který zabezpečuje kódování vkládaných HTML kódů, binárních příloh, obrázků, zvuků a videí.

Internetové e-mailové zprávy se skládají ze dvou hlavních částí:

Hlavička – předmět zprávy, odesílatel, příjemce a jiné informace o e-mailu

Tělo – Samotná zpráva, obyčejně obsahuje na konci blok s podpisem.

K e-mailu je možné přikládat jako přílohy i obrázky a jiné soubory. Bez problémů bývá doručování menších souborů typu dokumentu. Pokud však je ke zprávě přiložen velký soubor nebo příliš mnoho souborů nebo soubor typu programu, který by mohl být infikován virem nebo červem, mnohdy taková zpráva neprojde ochrannými filtry na doručovací cestě.

Hlavičky obvykle obsahují alespoň 4 pole:

Od (From): e-mailová adresa (popř. i jméno) odesílatele zprávy (zpravidla vyplňuje program automaticky)

Komu (To): e-mailová adresa (popř. i jméno) příjemce zprávy, adresátů může být více současně (vyplňuje odesílatel)

Předmět (Subject): stručný popis obsahu zprávy (vyplňuje odesílatel, nepovinně)

Datum (Date): místní datum a čas odeslání zprávy (vyplňuje program automaticky)

Pole „Od“ nemusí obsahovat adresu skutečného odesílatele. Je velmi jednoduché to zfalšovat a zpráva potom vypadá, že prišla z uvedené adresy. Je možné e-mail digitálně podepsat, aby bylo jisté, od koho zpráva pochází.

Další běžné součásti hlavičky:

Kopie (Cc): carbon copy – kopie (carbon proto, že psací stroje používají „kopírák“ (carbon paper) k vytvoření kopií dopisů) (vyplňuje odesílatel, nepovinná položka)

Slepá čili skrytá kopie (Bcc): blind carbon copy – neviditelná kopie (adresát bude vidět osoby uvedené v poli „Komu“ a „Cc“, ale ne adresy v „Bcc“) (vyplňuje odesílatel, nepovinná položka)

Received: přijato – trasové informace vytvořené servery, kterými zpráva prošla (automatické zápisy serverů)

(Fwd): přeposlaná zpráva (přišla od někoho a já jí pošlu někomu jinému)

E-mailová adresa

Každý uživatel musí mít pro příjem zpráv svoji e-mailovou adresu, která identifikuje jeho elektronickou poštovní schránku. Ta je fyzicky umístěna na nějakém internetovém serveru, populární jsou zejména servery, které nabízejí e-mailovou schránku zdarma a s webovým rozhraním (např. Centrum.cz, GMail, Seznam.cz). Pro odesílání zpráv není vlastní e-mailová adresa nutná, typickým příkladem jsou elektronické pohlednice.

E-mailové konference

Populární jsou diskuzní skupiny zvané e-mailové konference (mailinglisty), ve kterých probíhá hromadná výměna e-mailů mezi všemi účastníky.

Elektronický podpis

Nejjednodušší formou elektronického podpisu je prosté uvedení jména a dalších identifikačních a kontaktních údajů na konci těla zprávy. Obvykle se však pojmem elektronický podpis míní sofistikovanější nástroj, kdy pomocí speciálního kódu připojeného ke zprávě je možné ověřit jednak to, kdo zprávu skutečně odeslal (samotný údaj v položce From totiž není spolehlivý) a zpravidla i to, že obsah zprávy (tělo zprávy a přílohy) nebyl mezi odesláním a přijetím zprávy změněn.

Soukromí a šifrování

Bez osobních bezpečnostních opatření e-mail nezaručuje soukromí, protože e-mailové zprávy všeobecně nejsou šifrované. e-mailové zprávy musí projít cizími počítači v síti předtím, než dosáhnou cílový počítač, což znamená, že je relativně jednoduché je cestou zachytit a přečíst si cizí zprávu. Většina poskytovatelů internetového připojení (Internet service provider) ukládá na své servery kopie vašich e-mailových zpráv předtím, než je doručí. Existují kryptografické (šifrovací) aplikace. Šifrovací aplikace bývají obvykle funkčně propojené s aplikacemi vytvářejícími elektronický podpis.

Nejprve se vytvoří otisk (tzv. hash) dokumentu, což je poměrně krátký (typicky několik stovek bitů) výtah vytvořený specializovaným algoritmem z celého dokumentu. Tento hash se poté zašifruje autorovým tajným klíčem, čímž vznikne podpis. Ověření podpisu pak spočívá v dešifrování hashe (podpisu) pomocí veřejného klíče autora, nezávislého výpočtu hashe z dokumentu a porovnání obou hodnot. Pokud si odpovídají, pak je podpis ověřen a dokument je považován za důvěryhodný. Autor nemůže popřít své autorství - pokud k jeho tajnému klíči nikdo jiný nemá přístup, pak nikdo jiný nemůže zašifrovat hash dokumentu tak, aby po aplikaci autorova veřejného klíče vznikla správná hodnota. Pokud by byl dokument po podepsání změněn nebo poškozen, vyšla by jiná hodnota hashe, takže elektronický podpis by byl neplatný.

Nežádoucí zprávy

Užitečnost a použitelnost elektronické pošty ohrožují dva fenomény, spam a e-mailové červy.

Spam a hoaxy

Velkým problémem se naopak stává nevyžádaná obtěžující pošta zvaná spam (týká se především různých služeb, inzerátů, formulářů, atd.), kvůli kterému je vhodné být opatrný při zveřejňování e-mailové adresy na internetu.

Spam je nevyžádaná reklamní pošta. Nízké náklady na odeslání zprávy umožňují spammerům odeslat stovky miliónů elektronických zpráv denně pomocí laciného internetového připojení. Stovky aktivních spammerů způsobují přetížení počítačů v internetu, které takto dostávají desítky či stovky nevyžádaných e-mailů denně.

Dalším typem e-mailových zpráv jsou takzvané hoaxy. Tak se nazývají bludné a zplanělé zprávy kolující po internetu.

E-mailoví červi

E-mailové červy a viry používají elektronickou poštu k tomu, aby se mohly šířit do ostatních zranitelných počítačů. Přestože první e-mailový červ (en:Morris worm) infikoval UNIXové počítače, tento problém se v současnosti týká především Microsoft Windows.

Obrana před nežádoucími zprávami

Vliv těchto dvou faktorů způsobuje, že uživatelé dostávají více nevyžádané pošty, což snižuje použitelnost e-mailu.

Jedním ze zdrojů e-mailových adres je web a určitým specializovaným programem je možné hromadně extrahovat elektronické adresy vyskytující se v textu webových stránek. K zabránění těmto automatizovaným útoků se používá e-mailová adresa ve formě pochopitelné člověku, avšak nepochopitelné stroji. Například adresa „eva@domena.cz“ se zapíše jako „eva zavináč doména tečka cz“ a nebo se vygeneruje obrázek obsahující e-mailovou adresu a ten se uvede namísto textu.

V současné době existuje také mnoho programů (ať jsou to samostatné aplikace, součásti e-mailových klientů, nebo programy na serverech), které jsou schopny na bázi různých kritérií alespoň část spamu odfiltrovat.

Emailový klienti

Microsoft Outlook: asi nejpoužívanější klient, mimo základních funkcí poskytuje také RSS čtečku, kalendář, kontakty, poznámky a možnosti synchronizace s jiným zařízením

Microsoft Outlook Express: další klient od společnosti Microsoft, který poskytuje pouze základní funkce a na rozdíl od předcházejícího je poskytován s Microsoft Windows zcela zdarma.

Mozilla Thunderbird: k dispozici jako open source, umožňuje používat mnoho doplňků

The Bat!: proti předcházejícím klientům obsahuje i integrovaný HTML prohlížeč, možnost ovládání pomocí příkazového řádku a také podporuje doplňky

Opera: e-mailový klient integrovaný do internetového prohlížeče. Kódování obsahu e-mailu