DUM 6 téma: Elektronická pošta

ze sady: 3 **tematický okruh sady:** III. Ostatní služby internetu
ze šablony: 8 - Internet **určeno pro:** 3. ročník
vzdělávací obor: 18-20-M/01 Informační technologie
vzdělávací oblast: odborné vzdělávání
metodický list/anotace: viz VY_32_INOVACE_08306ml.pdf

Komunikace v sítích

Základní motivací k budování počítačových sítí je kromě sdílení hardwarových prostředků i vzájemná komunikace uzlů a jejich prostřednictvím pak uživatelů.

Postupem času se tato funkce stala jednou z hlavních funkcí sítě a elektronicky zprostředkovaná forma komunikace je nyní běžnou součástí komunikačního rejstříku moderního člověka – mnohdy jednou z nejužívanějších (samostatnému posouzení čtenáři ponechávám otázku zda je to dobře).

Variant a technologií, které umožňují přenos zpráv mezi lidmi prostřednictvím počítačů (či přesněji: „sítí elektronických komunikací“) je mnoho. Od jednosměrné komunikace zveřejňováním webových stránek, přes různé typy chatů nebo dokonce zcela bez přímé účasti počítačů – SMS a MMS … až po dnes nejznámější službu elektronické pošty e-mail (mnohdy uváděné jako „email“ nebo jen „mail“). Ostatně i tento posun názvosloví ukazuje význam této služby, kdy věta „pošlu to poštou“ je dnes mnohdy automaticky chápána ve smyslu elektronické pošty.

Lokální pošta a BBS

Původním významem elektronické pošty bylo předávání zpráv mezi uživateli v rámci jednoho počítače – střediskového/mainframe či serveru – ke kterému se uživatelé připojovali terminály. Každý účet byl spojen s poštovní schránkou, jednotliví uživatelé si mohli zasílat zprávy čistě uvedením uživatelského jména příjemce a krátkého textového obsahu. Jednalo se tedy spíše o jakési vzkazy.

Při použití v sítích firem byl pak stejný princip použit i na síťovém serveru (většinou v roli souborového serveru) a někdy i s využitím lokálních klientů. V tomto směru byl velmi rozšířený síťový systém Novell Netware.

Dalším stupněm vývoje pak byly síťové služby, přístupné prostřednictvím vytáčeného připojení – nejčastěji ve formě BBS (Bulletin Board System), kdy se k terminálovému serveru připojovali uživatelé modemy. V ČR byly největšími BBS Infima a následně i uzly sítě Fidonet, které umožňovali do určité míry i přenos zpráv mezi uživateli různých terminálových serverů vzájemně. Ve Francii pak podobně fungoval velmi populární systém Minitel.

E-mail v Internetu

Hlavní službou zajišťující off-line komunikaci v dnešních sítích (ať internetu nebo intranetu) je služba elektronické pošty popsaná v dokumentu RFC 821 (viz http://tools.ietf.org/html/rfc821) a následujících. Jedná se o jednu z nejstarších služeb v síti Internet a tomu odpovídá i její celková koncepce, systém ochrany a zabezpečení.

V dalším textu budeme výrazem „e-mail“ označovat právě službu založenou na RFC 821.

Konstrukce adresy e-mailu

Princip je velmi podobný jako u ostatních poštovních služeb, kdy je nutné jednoznačně identifikovat uživatele systému pošty, kteří jsou roztroušeni na různých serverech předem neurčeného počtu provozovatelů a ještě většího počtu sítí a klientů.

Centrální evidence uživatelských účtů by v takovém případě nemohla efektivně fungovat, nehledě na nekonečné konflikty požadavků na duplicitní jména v tak rozsáhlé síti, jakou internet bezesporu je.

Adresa uživatele je tedy u e-mailu strukturovaná, rozdělená na část jména uživatele a následně označení jeho domovského serveru. Jako oddělovací symbol byl zvolen znak @ - v angličtině „at“ čili „na“. V češtině se vžilo označení „zavináč“. Konkrétní adresu pak chápána jako uživatel *at* server, tedy uživatel *na* serveru, což zní i smysluplně.

Vytvoření a odeslání zprávy

Samotná zpráva služby e-mail je v principu prostý textový dokument, stvořitelný třeba v poznámkovém bloku či jiném čistě textovém editoru. Běžný uživatel však již dnes její správný formát a strukturu nemusí detailně ovládat, protože jsou k dispozici programy, schopné správně formátovanou zprávu za něj vytvořit. To je jedna z funkcí poštovních klientů – nejznámějšími jsou Mozilla Thunderbird či Microsoft Mail (dříve Outlook). Při tvorbě zprávy program požaduje zadání minimálně adresy příjemce, textu „předmětu“ (v originále „subject“) a pak samotného textu těla zprávy. Samotný poštovní program dále zprávu doplní řadou hlaviček, jako datum a čas vytvoření zprávy, název programu, který ji vytvořil, jménem a adresou odesilatele, adresou kam se má vrátit případná odpověď a jakékoliv další, které fantazie autora programu dovolí. Z toho vyplývá, že veškeré informace v takové hlavičce jsou pouze orientační a z principu nedůvěryhodné – zprávu může textově kdokoliv před odesláním, nebo v průběhu

přenosu, pozměnit; ať omylem či záměrně. Toto se týká samozřejmě i položek jméno a adresa odesilatele zprávy, s tímto vědomím je nutné veškeré příchozí zprávy kriticky posuzovat!

Adres příjemců může být uvedeno i několik a to hned 3 způsoby. Buď je více adres v sekci „To:“ (pro) a poštovní klient pak odesílá každou zprávu samostatně jednomu každému příjemci. Všechny adresy příjemců jsou ale zachovány v hlavičkách a každý z příjemců vidí komu dalšímu byla zpráva také poslána.

Druhou variantou je použití sekce „Cc:“ (carbon copy – kopie), kdy poštovní klient žádá poštovní server aby zajistil rozeslání zprávy všem uvedeným příjemcům, sám ale zprávu serveru posílá jen jednou. I zde všichni příjemci vidí, kdo další zprávu dostal.

Posledním způsobem je využití „Bcc:“ (Blind carbon copy – slepá či neviditelná kopie), kdy je seznam příjemců také předán serveru, který zprávu odešle každému z nich jednotlivě, bez uvedení seznamu dalších adresátů. Příjemce zprávy tak nemá šanci zjistit, komu dalšímu byla zpráva zaslána. Tento postup je při hromadném rozesílání dnes preferovaný, z důvodu častého zavirování počítačů – pro které je příchozí mail s desítkami adres vítanou potravou.

Ve firmách může být vynucené zasílání kopie mailů nastaveno i přímo na serveru, bez vědomí pracovníků. Vedoucí pak třeba dostává kopie veškeré pošty odeslané podřízenými a podobně. Takový postup je však na hraně či za hranou zákona; na e-mail se totiž vztahují stejná ustanovení o ochraně obsahu přenášených zpráv a zásilek, jako u papírové pošty.

Protokol SMTP to sice přímo nepožaduje, ale je vhodné aby nejméně jedna adresa byla uvedena v poli „To:“, některé server sice přijmou zprávu pouze s vyplněnými Cc: či Bcc:, nelze se na to ale spolehnout. Pokud chcete odeslat zprávu aniž by kdokoliv znal adresu byť jedinného příjemce – je třeba možné do „To:“ uvést vlastní adresu (kterou stejně všichni uvidí i v sekci „From:“ [od])

Zprávy může generovat i jakýkoliv program, bez účasti uživatele. Například systém elektronického obchodu, informující zákazníky o odeslání zboží, nebo knihovny upomínající klienty na nutnost vrátit zapůjčené knihy. Stejně tak může zprávy vytvářet robot či vir a rozesílat je jako nevyžádané či dokonce škodlivé (viz dále).

Jakýmkoliv způsobem vytvořenou zprávu pak většinou klient nedoručuje sám, ale využívá prostředníka – server elektronické pošty systému SMTP (existuje i několik privátních systémů jako Lotus a podobně, ty ale používají odlišné principy a nejsou veřejné).

Název systému je i názvem protokolu, kterým je přenos realizován, SMTP znamená Simple Mail Transfer Protocol a jeho hlavní myšlenkou je opravdu jednoduchost a funkčnost i na pomalých a méně spolehlivých linkách. Je to ostatně jeden z nejstarších protokolů, který ještě v internetu používá. Veškerá komunikace tímto protokolem je otevřená, neautorizovaná a čistě textová. Tím je tento protokol velmi snadno napadnutelný útokem typu man-in-the-middle a přímo odposlouchávatelná.

To je další vlastnost, kterou by si jakýkoliv uživatel měl uvědomit při používání této služby.

Vyhledání adresáta a přenos k cílovému serveru

První SMTP server, kterému klient zprávu předal ji nejprve analyzuje po formální stránce, zda obsahuje informace nutné k doručení – tedy adresu příjemce. V historických dobách internetu byl jakýkoliv SMTP server ochotný přijmout k doručení zprávu od kohokoliv a snažil se jej doručit. dnes už takový postup z řady důvodů (viz dále) možný není a uživatel tak musí využívat pouze SMTP server svého poskytovatele připojení, případně své firmy a podobně. součástí kontroly pak je i ověření že od daného odesilatele vůbec smí zprávu k doručení přijmout.

V další fázi pak server sleduje, zda náhodou není on sám cílem zprávy – tedy zda část adresy za „@“ není přímo jeho název, či název domény kterou má spravovat. V tom případě pouze zprávu přímo uloží do poštovní schránky jiného svého vlastního uživatele a proces je ukončen. To je typická situace při posílání zpráv v rámci jedné firmy či jiného typu organizace. Většina serverů také přijme e-mail s adresou bez „@“ a automaticky jej považuje za lokální (pokud uživatel takového jména na serveru existuje).

Poslední (a nejčastější) variantou je, že zpráva je určena pro příjemce na jiném serveru (v jiné doméně). V takovém případě SMTP server provede dotaz do DNS (Domain Name System) na MX (Mail Exchanger) pro tuto doménu. Do hlavičky zprávy přidá informaci – od koho zprávu přijal, kdy, případně zda s ní nějak manipuloval, a pokusí se ji předat zjištěnému MX serveru pro cílovou doménu. V ideálním případě tím přenos zprávy končí.

V praxi může oslovený MX server zprávu z nejrůznějších důvodů odmítnout (nejčastěji proto, že cílová schránka je plná), nebo ji podle svých vlastních pravidel předat k doručení jinému serveru-typicky ve větších organizacích, které navenek nechtějí zveřejňovat svoji

strukturu a pravidla pro přeposílání zpráv mají konfigurovaná interně. Další možnou variantou je požadavek samotného uživatele cílové schránky na přesměrování – kdy cílový server zprávu předá na jím určenou adresu.

U chyb doručení, které trvale znemožňují zprávu vyřídit, je zvykem aby poštovní server informoval odesilatele o chybě. Takové zprávy pak většinou poznáte podle hlavičky „Mail delivery system error…“ a je vhodné si je přečíst. Kromě plné schránky může být problémem třeba příliš velká příloha, kterou se odesilatel snažil poslat (v původním standardu SMTP je doručení zprávy větší jak 64 kByte označeno za nestandardní a nepodporovanou službu), nebo zakázaný obsah (programy, skripty) ve zprávě. Odeslání chybového hlášení je však pouze doporučené a poštovní server nic a nikdo nedonutí ho vrátit. Takový e-mail prostě zanikne a odesilatel nemá šanci zjistit, co se s ním stalo. V případě dočasných problémů s doručením (přetížený server, krátkodobý výpadek atd.) se SMTP servery pokouší zprávu doručit opakovaně, většinou až 4 dny. I proto by bylo chybou uživatele očekávat okamžité doručování mailů, běžné je doručení v desítkách minut.

Doručení a uložení zprávy v cíli

Když přes všechny tyto nesnáze zpráva nakonec skončí ve schránce adresáta, stane se z ní běžný textový soubor na disku poštovního serveru. Takový samozřejmě jistý diskový prostor zabírá a žádný disk nemá neomezenou kapacitu. Každý poštovní server proto více či méně omezuje množství prostoru, zabraného jednotlivými schránkami – případně také velikost jednotlivé zprávy. Poštovní (pro odlišení řekněme „schránkové“) servery provozují firmy či organizace pro své provozní a pracovní potřeby, někdy technicky zdatní jednotlivci či nadšenci a řada provozovatelů tzv. „freemailů“.

Každá varianta má své výhody a nevýhody, v případě studentů se bude jednat nejčastěji o poštovní schránku na školní síti – automaticky zřizovanou studentovi při nástupu do školy, kam jsou mu doručovány systémové zprávy školních systémů. Student je většinou povinen je pravidelně sledovat, nebo si zajistit přesměrování do schránky, kterou používá často. Školní schránky bývají omezeny co do celkové kapacity a důkladně filtrovány příchozí zprávy.

Nejčastěji bude mít čtenář vytvořenu schránku (nebo spíše několik schránek) na volném (free) serveru. Jejich provoz je sponzorován různými firmami a doplňkově je uživatelům zobrazována reklama a podobně. Dříve takové servery dokonce uměle vkládaly reklamu do zpráv z nich odesílaných, ale pro značnou nevoli uživatelů od této praxe upouštějí.

Podstatné je si uvědomit, že uživatel freemailového serveru (seznam.cz, gmail,com, email.cz, centrum.cz...) nemá s jejím provozovatel prakticky žádnou vymahatelnou smlouvu či dohodu a v případě problémů (ztráta dat, nefunkčnost schránky, prozrazení hesel…) nelze na provozovateli cokoliv vymáhat. Při užívání takové schránky je nutné počítat s možností prozrazení obsahu, nebo ztráty zpráv. Zcela nevhodné je takovou schránku používat jako podnikatelskou (nehledě k tomu, že uvedení freemailové adresy v obchodním styku působí velmi nedůvěryhodně – podobně jako třeba číslo telefonní budky na vizitce).

Převzetí zprávy ze schránky

Poslední fází cesty zprávy k adresátovi je vyzvednutí pošty ze schránky a přesun do počítače adresáta – pomocí poštovního klienta. Pro tento účel existují zejména dva protokoly – POP3 (definovaný v RFC 1939 viz http://www.ietf.org/rfc/rfc1939.txt) a IMAP (RFC 3501 http://tools.ietf.org/html/rfc3501). Oba protokoly podporují základní autentizační mechanismus, kdy pro přístup ke schránce musí uživatel předat uživatelské jméno a heslo.

POP3 – Post Office Protocol verze 3 zajišťuje jednoduché činnosti, zjištění seznamu zpráv na serveru a jejich přesun ze serveru ke klientovi. Standardním chováním protokolu je odstranění kopie zpráv ze serveru při každém připojení – zprávy jsou pak uloženy pouze u klienta lokálně. Tím zůstává poštovní schránka relativně volná a nehromadí se v ní historické zprávy. Zvláštním parametrem je možné zajistit zachování zprávy na serveru.

IMAP – Internet Message Access Protocol (dnes ve verzi 4) poskytuje výrazně složitější funkce pro práci s poštovní schránkou, která je na serveru. Základní odlišností je uložení zpráv na serveru a ke klientovi se přesunují pouze jejich kopie, když si je prohlíží. Zprávy jsou tak přístupné i z několika míst zároveň, po přečtení zůstávají na serveru. Přímo na serveru je možné vytvářet i strukturu v rámci schránek, ukládat i odesílané zprávy. Mazání zpráv probíhá dvoufázově – nejprve je zpráva označena jako smazaná a přesunuta do složky koš (či trash, bin a podobně) a teprve na zvláštní příkaz uživatele je trvale odstraněna. Tento přístup samozřejmě klade daleko větší nároky na diskovou kapacitu a výkon poštovního serveru. Řada freemailů také umožňuje přístup přes IMAP až jako nadstandardní a tedy i placenou službu.

Webmail

Zcela zvláštním způsobem přístupu ke schránce je webové rozhraní – webmail. Nejčastěji se používá u freemailů, ale svá webová rozhraní mají i profesionální a komerční poskytovatelé schránek.

Uživatel nepotřebuje speciální poštovní program – klienta – ale přistupuje ke schránce prostřednictvím www stránek, v klientovi služby www („internetovém prohlížeči“). Design stránek se velmi blíží vzhledu poštovního klienta a s využitím technologií JavaScript, Ajax či Flash umožňují i skoro interaktivní práci se schránkou. Mnohým uživatelům stačí webmail jako jediné pracovní rozhraní s poštovní schránkou a poštovního klienta vůbec nevyužívají.

Bezpečnost a zabezpečení

Jak bylo uvedeno výše – především protokol SMTP ve svém základě neuvažuje žádné zabezpečení, poštu lze odesílat jménem kohokoliv, přes jakýkoliv server, který je ochoten ji přijmout. Takový přístup vyhovoval v době, kdy internet byl technickou zajímavostí a jeho uživatelé technici a akademici. Dnes byly do SMTP doplněny s různou úspěšností zabezpečovací mechanismy. Nejjednodušší je „POP before SMTP“, kdy uživatel se musí nejprve pomocí POP3 připojit ke své schránce (tedy potvrdit jméno a heslo) a pak je mu umožněno odesílat poštu přes SMTP. Předpokládá to, že používá k odesílání stejný server, na kterém má on sám svoji schránku.

Jiným způsobem je SMTP Auth, kdy samotný SMTP server požaduje jméno a heslo, aby zprávu od uživatele přijal k doručení. Zdánlivě jednoduchý princip však musí správně reagovat na řadu situací – například vyřešit příjem zpráv od jiných SMTP serverů pro místní uživatele (kdy cizí SMTP server samozřejmě žádné jméno a heslo nezná).

Problémová situace nastává, pokud uživatel chce použít SMTP server například v zaměstnání pro odesílání pošty z domácího počítače. Standardně SMTP server zprávu k doručení nepřijme, protože klient je mimo jeho (firemní) síť. To lze omezit právě požadavkem na SMTP Auth. Opakem je blokace na straně internetového poskytovatele, který dovoluje svým klientům odesílat poštu pouze přes jeho SMTP server. Použít v takovém případě třeba firemní server není vlastně možné. Firma zase nemusí dovolit (pomocí techniky SPF-Sender Policy Framework) aby jejím jménem odesílaly poštu cizí SMTP servery. Zde pomůže jen rozumná dohoda administrátorů internetového poskytovatele a firemní sítě (která není vždy možná, pak je snazší změna internetového poskytovatele, než zaměstnavatele).

Krom toho je možné všechny protokoly doplnit o zabezpečovací vrstvu SSL či TLS – protokoly pak označujeme jako SMTPs, POP3s a IMAPs. Za předpokladu vzájemné výměny důvěryhodných certifikátů bude přenos mezi serverem a klientem (jak při odesílání, tak při příjmu) šifrován a útočník nebude moci zprávy číst, včetně případných hesel a podobně.

Přílohy a kódování

Jelikož je e-mailová zpráva pouhým textovým dokumentem, očekává se, že informace v ní bude obsažena jako jednoduchý text – nejlépe v ASCII kódování. Postupně bylo umožněno posílat e-maily i s národními znaky, kdy typ použitého kódování je uveden v hlavičce e-mailu. To je však dodnes spojeno s problémy, když odesílající program typ kódování neuvede, případně některý server po trase tuto informaci odstraní, nebo klientský program příjemce informaci o kódování ignoruje. Proto se i dnes můžeme setkat s nečitelnými maily, kde si jejich obsah musí příjemce domýšlet, nebo požádat odesílatele ale zprávu poslal znovu třeba bez diakritiky. Postupně problém vymizí, důsledným používáním kódování UTF-8 (k čemuž ale nelze nikoho donutit, zejména autory některých poštovních programů).

V souvislosti se zvyšováním kapacity komunikačních linek a velikostí disků, a hlavně nástupem multimédií, vznikl požadavek zasílat e-mailem i grafické, audio či dokonce audiovizuální soubory. Samotný standard SMTP na to nebyl připraven, určité řešení přineslo rozšíření MIME (Multipurpose Internet Mail Extensions RFC 2045 a následující http://tools.ietf.org/html/rfc2045).

Velmi zjednodušeně umožňuje uložit obsah souboru (přílohy e-mailu) do těla zprávy tak, aby jej příjemce z tohoto těla dokázal zpětně vyjmout a soubor rekonstruovat. Aby bylo možné ukládat jako přílohy i libovolná binární data (obrázky atd.), je příloha překódována systémem base64. Tím se sice odstraní možné problémy se speciálními znaky, tento kódovací systém je ale velmi neefektivní a výrazně zvětšuje objem dat k přenosu.

Zasílání souborů jako přílohy e-mailu je tedy z hlediska efektivity využití přenosových linek značně nevhodné a příloha o velikosti 1 MByte běžně zvětší samotnou e-mailovou zprávu o 1,5 MByte čistých dat a prodlouží čas ke zpracování i dopravě zpeávy.

Ve vlastním zájmu i s ohledem na ostatní uživatele by měl každý uživatel e-mailu zvážit, zda není lepší soubor předat druhé straně jinak (službou www, ftp, scp, přes úschovnu…) než jako přílohu e-mailu.

Spam, hoax, malware

S rozšířením služby e-mail se začaly objevovat i některé negativní jevy. Nejvýznamnějším je spam – česky překládaný jako „nevyžádaná pošta“ – lépe by bylo používat „nechtěná pošta“. Některé neočekávané zprávy totiž nemusí být vůbec nepříjemné (třeba pozvánka na schůzku ze seznamovacího serveru a podobně).

Z marketingového hlediska je e-mail dokonalým nástrojem, jak reklamní sdělení šířit bleskově, velkému okruhu osob a hlavně náklady na šíření přenést na příjemce zprávy. Je to totiž on, kdo platí internetovou konektivitu, přes kterou si doručenou poštu stahuje. Odesilatel pouze jedinou zprávu předá SMTP serveru. Jsou samozřejmě metody, jak se spamu bránit. Na první pohled jednoduché by bylo nepřijímat postu od SMTP serverů, přes které spamy odcházejí. Problém takového přístupu je v tom, že se jedná většinou o servery či počítače nic netušících lidí, které byly napadeny viry nebo crackery. V okamžiku rozeslání spamu jsou dále pro autora zpráv nezajímavé, pro příští kolo rozesílání si totiž zvolí zase jiný napadený stroj.

Jiný způsob obrany spočívá ve filtrech na straně příjemce. Ať na jeho poštovním serveru (přijímacím), nebo v jeho poštovním klientovi. Dnes často používané jsou inteligentní Bayesovské filtry, které příchozí zprávu hodnotí z mnoho různých hledisek a počítají pravděpodobnost, že se jedná o spam či ne. Jedná se o techniky pokročilé umělé inteligence, kdy počítač de-facto příchozí zprávu čte jako člověk a podle různých náznaků rozhoduje kam ji zařadit. Takovými vlastnostmi je třeba podíl velkých písmen v textu, počet vložených obrázků proti počtu znaků zprávy, výskyt nebo naopak absence určitých slov nebo dokonce smysl textu. Filtry lze dokonce postupně „učit“, kdy zpočátku propouštějí většinu zpráv, a uživatel některé sám označí jako spam. Příště už podobnou zprávu zahodí samotný filtr. Po kvalitním naučení se, je takový filtr velmi efektivní. Jeho chování totiž odpovídá konkrétnímu uživateli – jinak citlivý filtr bude mít uživatel komunikující pouze v rámci ČR, kdy jen výskyt anglických slov bude chápán jako podezření na spam, oproti mezinárodně komunikujícímu uživateli, kdy by takový přístup zahazoval i očekávané zprávy.

V nevýhodě jsou zde uživatelé freemailů, které většinou nastavují své filtry velmi ostře a ty pak někdy zahazují i neškodné a očekávané zprávy (o čemž se ale odesilatel nedozví). U nich uživatel většinou nemá šanci jejich nastavení změnit.

Úkoly pro samostatnou práci

- v poštovním klientovi nebo webmailu otevřete nějakou došlou zprávu a zobrazte kompletní hlavičky, sledujte - odkud byla zpráva odeslána a přes které servery procházela
- zjistěte, zda váš poskytovatel poštovní schránky podporuje přístup přes IMAP či POP3, pokud ano, nakonfigurujte nějakého poštovního klienta, aby se schránkou komunikoval (u POP3 zapněte ponechávání kopií zpráv na serveru)
- odešlete e-mailem některému spolužákovi soubor známé velikosti (třeba 1 MByte) a sledujte jaká je velikost vytvořené e-mailové zprávy
- najděte jiný způsob, jak předat uživateli přes internet soubor, bez použití přílohy k e-mailu

Zdroje:

- Archiv autora