Jemný úvod do (anti)spamové problematiky

Marcel Kolaja (FI MU), Miroslav Bartošek (ÚVT MU)

Se slovem spam se s rozšiřováním Internetu a elektronické pošty (hlavně do komerční sféry) setkáváme stále častěji. Mnozí se bohužel se spamem nesetkávají již jen jako s novým abstraktním pojmem, ale jsou konfrontováni s jeho konkrétními (nepříjemnými) dopady. Stále větší část uživatelů začíná pociťovat každodenní odstraňování nežádoucího balastu ze svých poštovních schránek jako činnost přinejmenším obtěžujícící, a začíná se zajímat o to, zda se dá s tímto soudobým nešvarem elektronické komunikace něco dělat. Tento článek přináší obecný úvod do spamové problematiky; navazující článek pak seznamuje s antispamovými opatřeními připravovanými na celouniverzitní úrovni.

Co je spam

Stručně řečeno, termín „spam“ označuje *zneužití digitální komunikace, při kterém je na množství adres zasílána jedna a tatáž příjemcem nevyžádaná zpráva, zpravidla komerčního charakteru.* Běžný uživatel se setkává se spamem nejčastěji v podobě nevyžádaného elektronického dopisu rozeslaného do světa nějakou firmou či osobou, která se tímto způsobem snaží informovat o novém, často dosti pochybném, produktu. Typickým spamem bývají též návody na „rychlé zbohatnutí“ či různé nabídky podivných (ne)legálních služeb, například pornografického charakteru. Je zřejmé, že většina příjemců nemá o tyto zprávy sebemenší zájem a takové zprávy je jednak obtěžují, jednak doslova okrádají – o čas i peníze. Spammeři si samozřejmě neetičnost svého počínání uvědomují. Někteří ve snaze předstírat zdání serióznosti připojují ke svým zprávám lživé formulace typu: „toto není spam“ nebo „na základě Vámi projeveného zájmu . . . “ a nabízí (obvykle fiktivní) možnost vyžádat si odstranění adresy příjemce z databáze adres používané spammerem k rozesílání jeho zpráv[1].

Důvody, které vedou spammery ke zneužívání elektronické komunikace, jsou zřejmé. Rozeslání spamu v drtivé většině případů spammera téměř nic nestojí, zato tímto způsobem dokáže vnucovat své produkty či služby obrovskému množství lidí. Výhodou z pohledu spammera je také možnost ukrýt svou identitu. Je poměrně snadné zfalšovat údaje v hlavičce elektronického dopisu, použít neplacenou, a tedy anonymní službu poštovních serverů či zneužít k rozesílání spamů cizí server[2], takže vystopovat skutečného původce spamu bývá velmi obtížné. Rovněž současné legislativní, organizační a technické možnosti obrany proti tomuto způsobu „marketingu“ jsou zejména v České republice značně omezené.

Druhy spamu

V dnešním digitálním světe existuje vícero typů globální digitální komunikace; všechny jsou potenciálně ke spamu zneužitelné – ať již jde o rozesílání spamů faxem, pomocí zpráv SMS či elektronickou poštou. Z legislativních i praktických důvodů jsou však dnes nejsnáze zneužitelné právě tradiční komunikační služby Internetu – email a Usenet news, protože jsou spojeny s nejmenšími náklady na straně rozesílatele.

Usenet-spam je zpráva zveřejněná současně ve velkém množství newsových skupin, obvykle bez ohledu na jejich tématické zaměření. Nemusí jít přitom vždy jen o zlovolné aktivity klasických spammerů: praktické zkušenosti ukazují, že každá zpráva zaslána již do více než 20 skupin je pro většinu uživatelů nerelevantní, a získává tak – bez ohledu na obsah – charakter spamu. Klasický Usenet-spam je cílen na ty uživatele, kteří čtou newsy, ale zřídkakdy posílají elektronické dopisy či skrývají své e-mailové adresy.

E-mailový spam zasahuje individuální uživatele přímo e-mailem. Spammer získává adresy svých obětí většinou automatickým prohledáváním newsů, elektronických konferencí nebo

[1] Často však použití doporučeného způsobu odstranění vede k intenzivnější spamové záplavě, neboť se tímto způsobem ověřila platnost a funkčnost konkrétní elektronické adresy – viz. dále.

[2] Uvádí se, že většina nejaktivnějších spamerů pochází ze Spojených států, přitom však téměř 70% jimi generované pošty přichází prostřednictvím zahraničních serverů.

webových stránek[3]. Takto vytvořené databáze elektronických adres bývají cenným artiklem pro obchod s dalšími zájemci. Velice ošklivou variantou e-mailového spamu je zasílání spamu do elektronických konferencí typu listserv, neboť tím se již tak velké množství spamem zasažených uživatelů ještě násobí.

Proč je spam špatný

Spam je špatný hned z několika důvodů. Velmi názorně to popisuje [2]:

1. *Peníze:* Jak jsme zmiňovali výše, spammera rozeslání spamu téměř nic nestojí, přenáší náklady své činnosti na příjemce. Typicky je spammer připojen k Internetu linkou, na níž se neúčtuje ani doba připojení k Internetu ani množství přenesených dat, nebo využívá takových technik šíření spamu, které mu umožňují minimalizovat dobu připojení k Internetu či množství přenesených dat. Příjemce však často takové podmínky nemá a za obdržený spam platí on sám. Jakýkoli jiný „klasický“ způsob šíření inzerce je postaven na přesně opačném finančním principu.[4]
2. *Rozsah:* Spam obtěžuje příjemce a okrádá ho o čas. Pokud by se jen jedno promile uživatelů Internetu rozhodlo rozesílat spam v relativně skromném počtu 100.000 zpráv denně (což je množství docela dobře zvládnutelné i s obyčejným PC a komutovaným připojením – ze slušného osobního počítače lze rozeslat až kolem čtvrt miliónů dopisů za hodinu), pak všichni uživatelé Internetu budou v průměru dostávat stovku spamů denně. Představte si, že byste museli každý den mazat stovky či tisíce spamů. Používali byste pak ještě elektronickou poštu?
3. *Krádež:* Stále větší množství spammerů posílá spamy přes cizí systémy – nevinné prostředníky[5], aby se vyhnuli blokaci svého vlastního systému. Tyto cizí systémy jsou tímto způsobem okrádány o svůj výkon, šířku pásma i čas správců při řešení následků zneužití.
4. *Balast:* Většina spamů jsou reklamy na pochybné produkty, pro které jiný způsob inzerce ani nemá smysl. Spam je ideální cestou, jak zkusit štěstí, jestli se někdo „nechytí“; vždyť spammera to prakticky nic nestojí.
5. *Nelegálnost:* Určité druhy spamu mohou být v některých zemích nelegální (například spamy s dětskou pornografií).

Příkladů závadnosti spamu lze uvést ještě mnohem víc; avšak každý z výše uvedených důvodů je již sám o sobě dostatečným důvodem k tomu, aby byl spamming zařazen do kategorie aktivit krajně nežádoucích.

Jak se spam šíří

Pokud by spammer používal k rozesílání spamů svůj vlastní systém, riskoval by jeho umístění na *černou listinu spammerů* a následně jeho blokování ze strany mnoha cílových uživatelských systémů. Proto spammeři velmi často zneužívají cizí systémy. Samozřejmě nemohou použít jakýkoliv SMTP server na Internetu. Jako prostředníka pro šíření spamu lze využít pouze ty SMTP servery, které mají povoleno doručování pošty pro všechny domény v Internetu – pracují v režimu *open relay*. Každý takto nakonfigurovaný SMTP server má poměrně vysokou šanci, že bude zapsán na černou listinu spammerů, a to nezávisle na svém původním, často zcela nevinném, určení.

Rychlý úvod do SMTP

Při přenosu e-mailu od odesílatele k příjemci dochází k následujícímu scénaři: poštovní server MTA (Mail Transfer Agent) na straně odesíla-

[3] Zaregistrovány již byly i případy „slovníkových spamových útoků“, kdy příslušný software generuje milióny potencionálních emailových adres nahodilou kombinací znaků, slov a domén s tím, že v dostatečně velkém vygenerovaném souboru bude vždy nezanedbatelné množství adres platných.

[4] Ilustrativní je příklad společnosti America Online, která běžně připojuje domácí uživatele k Internetu prostřednictvím modemu a placeného telefonního spojení: svého času registrovala AOL ve své síti až 1,8 miliónů spamů denně od firmy Cyber Promotions, a to tak dlouho, dokud soud nenařídil dané firmě tyto její aktivity ukončit. Za předpokladu, že typickému uživateli trvá v průměru 10 sekund, než jeden jediný spam identifikuje a vymaže, pak to jen v síti AOL představovalo 5000 hodin denně, po které byli její uživatelé zcela zbytečně připojeni, a samozřejmě za toto připojení také zaplatili.

[5] Tyto systémy tak zcela nevinné nejsou, neboť v důsledku příliš liberální konfigurace toto zneužití umožňují.

tele kontaktuje jiný MTA (většinou na straně příjemce), který e-mail doručuje dále. Každý MTA by měl sloužit pouze pro svoji doménu a doručovat poštu pouze z/do této domény. Tomu se říká poskytovat pro danou doménu *relaying*. Pokud poskytuje MTA relaying pro celý Internet, jedná se právě o open relay zmíněnou výše.

Využití open relay spammery

Spammer pomocí svého MTA požádá nějaký jiný MTA o rozeslání spamů. Pokud je onen MTA typu open relay, požadavku vyhoví. Největší výhodou z pohledu spammera je fakt, že stačí požádat o doručení jednoho jediného e-mailu na určené adresy. Spammer tedy přenese e-mail pouze jednou a pak se již může klidně odpojit od Internetu (používá-li vytáčené připojení). Veškerou zátěž převedl na cizí MTA s open relay, který rozesílá a rozesílá a ...

Z historie spamu

Jeden z prvních známějších spamů se objevil již v roce 1988 (viz [6]). Tehdy jistý student na univerzitě v Marylandu poslal do newsových skupin řetězovou zprávu patřící do kategorie „pyramidových her“, v jejímž předmětu se vyskytovala slova „MAKE MONEY FAST“. Od té doby se pro zprávy s podobným obsahem vžilo označení MMF (neplést s českou zkratkou jedné ctihodné mezinárodní instituce!).

Druhou velice známou spamovou aférou je případ z roku 1994, kdy jedni manželé, právníci v oblasti amerického imigračního práva, použili spam jako způsob reklamy pro podávání přihlášek do „Green Card Lottery“. Rozeslali tehdy nevyžádanou reklamní nabídku údajně do všech v té době existujících newsových skupin (kterých bylo tehdy cca 6.000). Jako „odměnu“ za tento čin obdrželi 35 000 silně odmítavých reakcí, které zaplnily 73 GB diskového prostoru providera těchto dvou manželů. Tento případ bývá uváděn jako jeden z prvních příkladů „střetu kooperativního, značně liberálního a v zásadě nezištného způsobu fungování s mnohem drsnějším způsobem fungování komerčního světa, založeného na konkurenci a snaze prosadit se a zvítězit nad druhým. Skutečnost, že první byli právníci, byla velmi příznačná“ [6].

Obrana proti spamu

Absolutně účinná a obecně aplikovatelná obrana proti spamům v současnosti v podstatě neexistuje. Existuje však několik přístupů, které mohou pomoci problémy v dané oblasti alespoň zmírnit. Zahrnují jednak přístupy individuální usilující o omezení množství spamů, které dostává daná konkrétní osoba či skupina osob[6] (filtrování pošty a blokování spamovských zdrojů, skrývání adres, žaloby proti spamerským firmám), jednak přístupy tak říkajíc „všeobecně prospěšné“ snažící se bojovat s fenoménem spamu obecně (osvětou, tlakem na providery a správce systémů aby neposkytovali spamerům prostor pro jejich činnost, lobováním za přijetí účinnější antispamové legislativy, apod.). Zmiňme alespoň v obecné rovině přístupy, které jsou nejpoužívanější.

Stížnost providerovi

Jednou z věcí, kterou může – alespoň teoreticky – podniknout každý příjemce spamů, je zaslání stížnosti providerovi spammera (stěžovat si přímo pachateli nemá obvykle žádný efekt). Nejdříve je však třeba zjistit, komu si vlastně stěžovat – a to již může být v praxi bohužel komplikovanější a ne pro každého použitelné. Existují specializované programy a služby, které umožňují proces identifikace správných adres a „hlášení spamu“ provádět za uživatele. Stačí jim zaslat příslušný dopis-spam (např. služba *SpamCop* `http://spamcop.net/`).

Odkud spam přichází, lze zjistit z polí `Received` v záhlaví dopisu. Seznam těchto polí shora dolů poskytuje jména systémů, přes které spam prošel (avšak v přesně opačném pořadí). Jakmile najdete podezřelou doménu, pokuste se zjistit, o jakou se jedná organizaci. Zkuste se podívat na různé antispamové WWW stránky, newsy nebo další zdroje. Pokud se jedná o organizaci, která se snaží bojovat proti spamu, stěžujte si u ní.

[6] Ukazuje se, že spamem bývají více zasaženi uživatelé, jejichž emailová adresa je v abecedním řazení blíže začátku abecedy. Je to důsledek toho, že proces rozesílání obrovského kvanta dopisů podle abecedně setříděné databáze adres často nedoběhne do konce, protože je dříve či později zastaven – ať již zásahem providera či správce zneužitého poštovního serveru, nebo jiným mechanismem.

Jestliže je o této organizaci známo, že ignoruje stížnosti ohledně spamů, stěžujte si u jejich providera. Pokuste se najít jejich WWW stránky (například přidáním `www.` před doménové jméno). Uvidíte-li stránku podobnou spamu, který jste obdrželi, našli jste pravděpodobně přímo spammery. Narazíte-li na stránku nabízející služby související s připojením na Internet, identifikovali jste pravděpodobně místo, kam si máte stěžovat. Pokud jste indentifikovali doménu spammerů a chcete najít jejich providera, použijte program `traceroute`.

Jestliže si nejste jisti, zda si stěžujete na správnou adresu, je dobré připojit ke stížnosti žádost o přeposlání stížnosti na to pravé místo. Nevíte-li, na jakou adresu v dané doméně máte stížnost poslat, zkuste ji najít na WWW stránkách. Alternativou je služba `abuse.net` (`http://abuse.net/`). Pokud není žádná z těchto možností použitelná, lze vždy ještě zkusit adresu `postmaster@<daná_doména>`.

Při své stížnosti buďte slušní – ten, komu si stěžujete, často za spam vůbec nemůže. Ve stížnosti pošlete všechny hlavičky spamu, který ohlašujete. Bez nich provider nic nezjistí. Na svoji stížnost pravděpodobně nedostanete žádnou odpověď. To ale nemusí znamenat, že provider nepodniká patřičné kroky. Může se stát, že bude provider zavalen stížnostmi a nebude v jeho silách na všechny odpovídat. Na druhé straně jsou známy i případy pozitivní reakce, nejde tedy a-priori o zbytečnou činnost. Rostoucí záplava spamů nutí i velké providery a provozovatele veřejných poštovních služeb podnikat protiopatření, a to čistě z ekonomických důvodů.[7]

Filtrování a blokování spamu

Jednou z nejpoužívanějších metod obrany proti spamu, je rozeznání spamu při jeho příchodu a jeho následné ošetření. Existují v zásadě dva způsoby, jak spam rozeznat: na základě černé listiny odesilatelů nebo podle obsahu zprávy. Se zprávou, která byla identifikována jako spam, lze pak nakládat různým způsobem. Může být SMTP serverem přímo zahazována, nebo může být pouze označkována a postoupena k dalšímu zpracování (likvidaci, uložení do vyhrazené poštovní schránky, apod).

Černé listiny

Na Internetu existuje několik černých listin spammerů. Správce může poštovní server (MTA) nakonfigurovat tak, aby při příchodu každého dopisu vyslal dotaz, zda stroj, od kterého zprávu přijímá, nemá záznam v některé černé listině a v kladném případě poštu z daného místa odmítnout (blokovat). Dotaz do černé listiny se typicky provádí jako DNS dotaz.

Jedním z velice zajímavých projektů v této oblasti je *MAPS* (Mail Abuse Prevention System, `http://mail-abuse.org/`). Ten obsahuje hned několik černých listin. Další černé listiny spravují například *SpamCop* zmíněný již výše nebo *ORDB* (`http://ordb.org/` – Open Relay DataBase, seznam open relay serverů).

Blokování podle obsahu zprávy

Pro identifikaci spamu je možno také využít některého specializovaného programu, který se pokouší odhalit spam – nejčastěji na základě výskytu určitých slov či frází v textu dopisu. Dokonalejší programy se pokouší využívat heuristické postupy a metodu „učení se“ na základě předkládaných příkladů. Obecně se však dá říci, že spolehlivost takovýchto filtrovacích programů nemusí být vždy uspokojivá, u těch nejlepších se pohybuje kolem 60-70% (důležitý je přitom nejen co nejvyšší počet zachycených spamů, ale také co nejnižší počet falešných hlášení, kdy je jako spam označena pro uživatele důležitá relevantní zpráva).

Filtrovacích anti-spamových programů existuje velké množství, mezi ty nejznámější patří: *Spam Eater Pro* (`http://www.hms.com/spameater.asp`) dostupný ve verzi freeware a shareware pro POP3 poštovní schránky, *Brightmail* (`http://www.brightmail.com/`), který dnes na svých serverech provozují i někteří nejvýznamnější američtí Internetovští připojovatelé (AT&T Broadband, EarthLink či Microsoftí MSN), nebo *SpamKiller* (`http://www.mcafee.com/myapps/msk/default.asp`).

[7] Některé odhady uvádějí ztráty Internetovských providerů plynoucí z odchodu spamem znechucených uživatelů až na 1 milión USD na každých 7 miliónů zákazníků.

Poměrně častý způsob je využití obou přístupů současně – blokace za podpory černých listin i filtrování. Na tomto principu funguje například i volně dostupný filtrovací program pro unixové uživatele *SpamAssassin* (`http://spamassassin.org/`). Uživatel si přitom obvykle může stanovit jak vlastní kritéria filtrování, tak i zdroje, z nichž nechce poštu nikdy přijímat a naopak zdroje, jejichž poštu chce přijímat vždy, bez ohledu na její obsah.

Některé filtrovací programy bývají současně provázány i s antiviry. S tím, jak trh antispamových filtrovacích nástrojů získává na objemu a důležitosti, přitahuje pozornost i těch největších firem z oblasti antivirové ochrany a bezpečnostního software: firma Network Associates (nabízející mimo jiné známý antivir McAfee) koupila v dubnu letošního roku norskou společnost Novasoft vyvíjející antispamový systém SpamKiller; společnost Symantec (obchodující s antivirem Norton AntiVirus) ohlásila svůj vlastní antispamový systém na podzim tohoto roku.

Skrývání adres

Jednou z často používaných preventivních metod obrany proti záplavě spamů je snaha snížit riziko toho, aby se elektronická adresa uživatele dostala do spamerských databází adres. Mezi obvyklá doporučení patří:

- neposkytujte svou elektronickou adresu kdekomu na potkání (např. jejím uváděním při vyplňování různých formulářů na webu; efekt takového počínání může být podobný zveřejnění telefonního čísla na plakátovací ploše v centru města)
- neuvádějte svou adresu v textu příspěvků do news a jiných forem elektronických diskusních klubů
- maskujte svou emailovou adresu v podpisu tak, aby nebyla rozpoznatelná automatickými sběrači adres, ale člověk ji dokázal stále ještě správně interpretovat; nejčastěji se používá přístup nahrazující znak „@“ jiným znakem či řetězem znaků; např. namísto `novak@muni.cz` lze uvést „`novak AT muni.cz`“[8]
- zřiďte si alternativní adresu na některém veřejném serveru a tu používejte pro rizikovější případy, při nichž se veřejnému uvedení své elektronické adresy nemůžete vyhnout. Poštovní schránku na této veřejné adrese postačí kontrolovat s podstatně nižší frekvencí (třeba jednou za měsíc), než u běžné privátní/pracovní adresy.

I když takováto opatření spamům nezabrání, pomohou alespoň problémy s nimi zmenšit. Bohužel za cenu určitých komplikací při používání elektronické pošty.

Další obecná doporučení

Nepoužívejte „remove“

Mnoho spamů obsahuje pokyn nabádající zaslat email s příkazem „`remove`“ či provést analogickou akci na udané www-stránce, pokud si příjemce nepřeje dostávat další zprávy od zasílatele. Ponechme stranou skutečnost, že nás někdo žádá o odstranění ze seznamu, do kterého jsme se sami nikdy nezapsali, ale uvědomme si základní pravidlo: *Spammer vždy lže.* V tom lepším případě nezpůsobí provedení akce `remove` nic (opravdový spammer nemá v úmyslu se odstraňováním adres jakkoliv zatěžovat, smyslem jeho vyhlášení je pouze vyhovět liteře příslušného zákona na ochranu proti spamům a/nebo dodat svému počínání zdání věrohodnosti). V tom horším případě poskytne příjemce akcí `remove` spammerovi potvrzení o tom, že daná adresa je skutečně „živá“ a výsledek bude přesně opačný – bude dostávat ještě více spamů než kdykoli předtím.

Zachovejte důstojnost

Ačkoliv je spamming činnost krajně zavrženíhodná, nedoporučuje se používat v boji s ním aktivní prostředky namířené přímo proti spammerům (nejvýše s výjimkou upozornění na tuto aktivitu), tim méně snižovat se na jeho úroveň. Mimo jiné to znamená:

- nesnažit se v odvetu zahltit druhou stranu záplavou e-mailů (e-mail bombing)

[8] Takovéto maskování adres se označuje termínem „munging“ – od anglické zkratky MUNG: „Mash Until No Good“. Více k technikám mungingu lze nalézt na `http://members.aol.com/emailfaq/mungfaq.html`

- nepoužívat vůči spammerům (ať již skutečným či domnělým) ani žádné jiné útoky typu DoS (Denial of Service)
- nesnažit se druhou stranu cracknout
- nesnažit se druhou stranu poškodit nějakým nelegálním způsobem
- a především: nebojovat proti spamu spamem.

Dlouhodobě účinnějšími nástroji obrany jsou osvěta, dokonalejší technické nástroje a kvalitnější legislativa.

Boj proti spamu na poli legislativy

V řadě zemí se diskutuje či přijímá nová legislativa upravující možnosti šíření a získávání informací prostřednictvím Internetu, zahrnující mimo jiné i problematiku spamu. V principu lze zvažovat dvě základní varianty poskytování informací – „bez souhlasu“ a „na vyžádání“. První model (stávající stav) přepokládá, že uživatel s poskytováním (propagačních) informací automaticky souhlasí a pokud si nepřeje informace dostávat, musí svůj nesouhlas výslovně uvést. Druhý model vychází z opačného přepokladu – informace je možné aktivně zasílat pouze tomu uživateli, který s tím vyslovil explicitní souhlas *předem*. Současná, v řadě zemí již existující, i připravovaná legislativa je z hlediska účinnější ochrany proti spamům většinou bohužel nedostatečná; i ty pokrokovější antispamové zákony se zaměřují spíše na to, jak postavit mimo zákon falšování elektronické identity či nevyhovění požadavku na zastavení proudu zpráv, než na radikální změnu právního postavení stávajícího modelu poskytování nevyžádaných informací.

Užitečné odkazy

[1] Network Abuse Clearinghouse
`http://abuse.net/`

[2] Fight Spam On The Internet!
`http://spam.abuse.net/`

[3] Bojujte proti spammingu!
`http://antispam.cz/`

[4] Net Abuse FAQ `http://www.cybernothing.org/faqs/net-abuse-faq.html`

[5] spam.org `http://spam.org/`

[6] články na pcworld.cz `http://www.pcworld.cz/` – 12.2000, 08.2001

[7] Usenet news `news:alt.spam` □