E-mail a centrální poštovní server Masarykovy univerzity

Miroslav Ruda, ÚVT MU

Prudký nárůst objemu elektronické pošty, zapříčiněný bohužel zejména vzrůstem podílu spamu, si vyžádal v poslední době změny konfigurace centrálního poštovního serveru MU (serveru `relay.muni.cz`). Cílem tohoto článku je popsat současnou konfiguraci poštovního serveru a poskytované služby, se zaměřením na novou službu – greylisting [1].

Poštovní server relay.muni.cz je centrální bod e-mailové komunikace Masarykovy univerzity se světem. Přes tento server prochází každý e-mail ze světa na adresy MU, každý e-mail posílaný ze strojů MU do světa, ale i každý e-mail putující mezi jednotlivými fakultami MU.

Pro doručování pošty je použit program sendmail[1]. Vedle bohaté možnosti konfigurace samotného serveru umožňuje tento program i implementaci dalších kontrol pomocí samostatně stojících služeb, které s centrálním poštovním programem komunikují přes standardizované rozhraní API milter[2]. I většina našich kontrol e-mailových zpráv je implementována jako milter služby. Některé z nich jsou převzaty ze světa, jiné jsou vyvinuty přímo na ÚVT MU. Je potřeba si uvědomit, že již před nasazením greylistingu zpracovával tento server přibližně milión (!) e-mailů denně, a že kontroly musí být proto pečlivě navrženy tak, aby je bylo možné provádět v reálném čase a na hardware, který je k dispozici[3].

Kontroly na našem poštovním serveru můžeme rozdělit do kategorií antivirová kontrola, antispamová kontrola a další kontroly validity e-mailu, a budou postupně popsány v dalších kapitolách. Na konci článku pak popíšeme, jak lze použít server relay.muni.cz pro odesílání pošty i na cestách, z míst mimo MU.

[1] www.sendmail.org

[2] www.milter.org

[3] V současnosti je to 2xdual core Xeon, s 8GB RAM a operačním systémem Linux

1 Antivirová kontrola

Centrální server provádí antivirovou kontrolu pro veškerou poštu přicházející do domény `muni.cz`, a pro všechnu poštu odcházející z jednotlivých fakult do světa nebo na jiné fakulty MU. Pro kontrolu je použit antivirus firmy Kaspersky Lab[4], komunikace se samostatně stojícím antivirovým programem je zajištěna vlastním milter klientem.

Vedle samotné antivirové kontroly jsou všechny e-maily kontrolovány dalším filtrem, který odmítá veškeré e-maily s přílohami, které jsou potenciálně nebezpečné pro klienty na operačním systému MS Windows (spustitelné `.exe` soubory, přílohy typu `.vbs` apod.). Pro testy je použit program vbsfilter[5]. Seznam odmítaných příloh je dostupný na webu ÚVT MU[6].

2 Antispamová kontrola

Na centrálním serveru není vhodné kontrolovat každý e-mail antispamovými filtry typu Spamassasin. Důvodem jsou jednak vysoké nároky na hardwarové vybavení, které je vhodné rozprostřít mezi více podřízených serverů, a hlavně nemožnost konfigurace specifické pro každého uživatele – vlastnost u heuristického rozpoznáváni spamů velice žádaná. Je nutné si uvědomit, že na univerzitě je skladba uživatelů velice pestrá, a že u mnoha jednoduchých antispamových testů často používaných v komerčních firmách lze najít v našem prostředí protipříklad (lékaři opravdu mohou diskutovat o VIAGŘE, na katedry jazyků mohou chodit e-maily v ruštině nebo čínštině, IT oddělení může uvítat nevyžádaný e-mail o slevách serverů firmy XXX, nelze přijímat e-maily jen z domény `.cz` apod.).

Antispamová kontrola je proto rozdělena na několik fází. Na centrálním serveru je odfiltrována pošta, která je spamem prokazatelně, a heuristické analýzy typu program Spamassasin jsou ponechány až na poštovní servery jednotlivých fakult, kde si už uživatelé mohou nastavení ovlivňovat. Na centrálním serveru proto provozujeme dva filtry: dopřednou kontrolu existence

[4] `http://www.kaspersky.com`

[5] `http://aeschi.ch.eu.org/milter/vbsfilter.c`

[6] `http://www.ics.muni.cz/techinfo/abuse.html`

adresy příjemce a nově, od 1.března 2007, i greylisting.

2.1 Dopředná kontrola

Dopředná kontrola, poskytovaná programem milter-ahead[7] funguje tak, že adresa příjemce je překontrolována na podřízených poštovních serverech již v průběhu přijímání pošty ze světa, ještě před přijmutím těla e-mailu. Pokud je adresa neplatná, je e-mail okamžitě odmítnut. Tím je zaručeno i to, že centrální server nepřijme e-mail s podvrženou adresou odesílatele a po zjištění, že adresa příjemce je neplatná, neposílá e-mail neplatnému odesílateli, a tím se sám nepodílí na rozesílání spamu.

2.2 Greylisting

Druhá antispamová kontrola, greylisting, vychází z předpokladu, že spammer rozesílá poštu v takovém množství, že je pro něho obtížné přeposlat znovu e-mail, který je poprvé dočasně odmítnut.

Centrální poštovní server MU proto při prvním pokusu o doručení pošty odpoví druhé straně dočasnou chybou, s odpovědí „pošta nemůže být přijata, zkuste to znovu za 25 minut". Dočasné odmítnutí pošty je při e-mailové komunikaci na Internetu standardní věc, používá se např. při přeplněném disku, přetíženém serveru apod.

Při dočasném odmítnutí pošty si poštovní server MU uloží do své greylistové databáze trojici údajů: „adresa odesílatele, adresa příjemce, IP vzdáleného stroje". Pokud do pěti dnů dorazí e-mail se stejnou trojicí (zpravidla ten samý e-mail při druhém pokusu o doručení), je už přijat a trojice je na 180 hodin (o trošku víc než týden) uložena do *whitelistové* databáze. Pokud se vzdálený server pokusí o druhé doručení dříve než po 25 minutách, je opět odmítnut, opět dočasně, jen je mu prozrazeno, kolik minut ještě musí čekat.

Pokud již je trojice údajů ve whitelistové databázi a přijde další e-mail se stejnou trojicí, poštovní server MU takový e-mail propustí okamžitě a opět prodlouží platnost položky ve whitelistové databázi.

Zpoždění při e-mailové komunikaci tak nastane jen při prvním výskytu trojice „příjemce, odesílatel, server", tj. při prvním e-mailu z neznámé adresy. Pokud pak z této adresy chodí alespoň jeden e-mail týdně, zpoždění už by nemělo nastat. Výsledné počáteční zpoždění je zpravidla kratší než hodina (záleží na poštovním serveru druhé strany, jak brzy po uplynutí 25minutového nepřijímacího intervalu MU přepošle dočasně odmítnutý e-mail znovu).

Greylisting se nevztahuje na stroje z domény muni.cz, neaplikuje se na spojení, při kterém se uživatel nejdříve prokázal heslem nebo certifikátem (viz. 4) a neaplikuje se na domény vyjmenované v permanentní whitelistové databázi (viz níže).

Problémy mohou nastat u nestandardních poštovních serverů, které reagují špatně na dočasnou chybu. Použití metody greylistingu je však ve světě poměrně rozšířené, a proto by podobně problémy měly být vzácné. Další kategorie problémů může nastat u domén, které odesílají e-maily přes farmu několika strojů (např. `gmail.com`): pokud se odmítnutý e-mail pokusí podruhé doručit jiný stroj, s jinou IP než ten původní, je opět zařazen do greylistové databáze. Podobné problémy je nutné nahlásit správcům na ÚVT a můžeme je buď řešit nebo je možné přidat stroj/celou doménu na trvalý whitelistový seznam. Velké domény, které jsou tímto problémem známé, jsou již vyjmenovány v greylistovém programu, který používáme.

Aby se zpomalení komunikace s většími servery ještě více předešlo, testujeme i variantu, kde je automatický whitelisting platný pro všechny e-maily pocházející ze stejného stroje. Idea je taková, že pokud server zopakoval jeden e-mail po 25 minutách, dá se předpokládat, že se stejně zachová i k další poště. Při takové konfiguraci pak stačí jediný e-mail z domény `seznam.cz`, a všechny další e-maily z poštovního serveru domény `seznam.cz` jsou již přijímány bez zpoždění.

Pro implementaci byl použit program `milter-greylist`[8]. V současné době je greylisting apli-

[7] `http://www.milter.info/sendmail/milter-ahead/`

[8] http://hcpnet.free.fr/milter-greylist/

kován na veškerou poštu do domén muni.cz a linux.cz.

S nasazením greylistingu bylo také nutné vyřešit problém záložního poštovního serveru. Tuto službu nám dosud poskytoval server rs.cesnet.cz na CESNETu. S nasazením greylistingu by ale bylo nutné implementovat stejný greylisting i na tomto serveru a v ideálním případě i synchronizovat greylistovou databázi mezi těmito stroji. To se ukázalo jako neschůdné, a proto byl záložní server zrušen. V současné době provádíme finální testy synchronizace greylistové databáze mezi dvěma servery na ÚVT MU (což při milionech záznamů v databázi a řádově deseti změnami za vteřinu je samo o sobě zajímavý problém) a v nejbližší době začneme provozovat oba servery v plně zástupném režimu.

2.3 Černé listiny

Jednou z metod používaných ve světe je metoda „černých listin" (blacklists) – veřejně dostupných služeb, kde jsou vyjmenovány IP adresy serverů, přes které byl spam rozesílán. Vzhledem k nespolehlivosti těchto služeb (i vzhledem k tomu, jak často se na podobných serverech objevují adresy našich serverů nebo serverů největších českých e-mailových poskytovatelů) centrální server nekontroluje IP adresu odesílatele proti černým listinám typu spamcop.net. IP adresa stroje komunikujícího s naším poštovním serverem je uložena do hlavičky X-Muni-Spam-TestIP a podřízené fakultní servery si mohou takový test provést později. Navíc programy typu Spamassasin už takový test nabízí pro všechny servery, přes které daný e-mail prošel.

3 Další testy validity e-mailu

Centrální server detekuje i několik dalších „podezřelých" typů e-mailu a odmítá jejich přijetí. Vedle standardních testů (typu test na platnost domény z adresy odesílatele) používáme vlastní filtr, který detekuje zacyklení při přeposílání pošty (ať už mezi doménami MU, na veřejné poštovní servery nebo na SMS servery), příliš vnořené MIME maily používané občas i na zmatení antivirových či antispamových programů a k dispozici je i filtr milter-regex[9], který umožňuje specifikovat libovolný regulární výraz, jehož výskyt je pak testován ve hlavičkách i celém těle každého e-mailu.

4 Autentizace při odesílání pošty

Poštovní server relay.muni.cz přijímá poštu pro příjemce v doméně muni.cz a linux.cz od libovolného stroje. Pro odesílání pošty poskytuje tuto službu všem strojům jen z IP rozsahu 147.251.0.0/16 (doméně muni.cz). Aby mohl být server použit také pro rozesílání pošty i uživateli na cestách nebo z domácího připojení, umožňuje server autentizaci odesílatele. V takovém případě přijímá server libovolnou poštu i od strojů mimo doménu muni.cz a např. také obchází greylisting.

Poštovnímu serveru je možné se prokázat heslem do kerberovských realmů IS.MUNI.CZ (sekundární heslo ISu, tedy heslo poštovní schránky na mail.muni.cz), ICS.MUNI.CZ a META. V takovém případě je nutné nakonfigurovat poštovního klienta tak, aby si vynutil TLS (šifrované spojení) a jako login pak použít např. učo@is.muni.cz.

Druhou možností je autentizace uživatelským nebo serverovým certifikátem – v současné době podporujeme pouze certifikační autoritu CESNETu[10], ale nebráníme se podpoře i dalších certifikačních autorit.

5 Závěrem pár čísel

Závěrem pár čísel o provozu a účinnosti jednotlivých filtrů (podrobnější informace viz článek Radima Peši v tomto čísle Zpravodaje).

Před nasazením greylistingu se centrální server MU zabýval denně přibližně miliónem e-mailů (směrem do MU i ven z MU, včetně hostovaných domén typu linux.cz, včetně opakovaných pokusů o doručení apod.). Z tohoto počtu bylo asi 250.000 e-mailů odmítnuto dopřednou kontrolou, přes 270.000 e-mailů překontrolováno antivirem (v té době největším konzumentem výpočetního výkonu) a přibližně 265.000 e-mailů bylo zasláno podřízeným fakultním serverům.

Několik dní po nasazení greylistingu bylo z více než miliónu e-mailů propuštěno přibližně 40.000

[9] http://www.benzedrine.cx/milter-regex.html
[10] http://www.cesnet.cz/pki/cs/ch-intro.html

e-mailů a dalších 40.000 nebylo greylistingem kontrolováno (pocházelo z domény muni.cz, přišlo ze serveru rs.cesnet.cz – v té době ještě záložního apod.). Přibližně 60.000 e-mailů bylo překontrolováno antivirem a přibližně 45.000 e-mailů bylo zasláno podřízeným fakultním serverům. V greylistové databázi bylo přibližně sedm a půl miliónu záznamů, z nich jen 5 procent prošlo do whitelistové databáze.

V současné době již nepoužíváme záložní server rs.cesnet.cz, testujeme uvolněnější whitelisting a byl dále optimalizován provoz některých filtrů. Počet e-mailů, kterými se server denně zabývá, narostl na 1,7 miliónu, na podřízené servery na fakultách prošlo přibližně 70.000 e-mailů a antivirus překontroloval přibližně 80.000 e-mailů. Počet odhalených virů nadále kolísá mezi 2.000 a 4.000 denně, počet odmítnutých příloh se pohybuje mezi 1000 a 2000 denně, počet e-mailů odmítnutých dopřednou kontrolou zůstává nad 200.000. Greylistová databáze obsahuje více než 8 miliónů záznamů, poměr e-mailů, které přes greylisting projdou, zůstává okolo 5 procent.

V době psaní článku zůstává otevřenou otázkou výhodnost uvolnění whitelistingu. Dalšími experimenty bude potřeba ověřit, jak velké množství spamu projde díky této metodě, a zda by nebylo výhodnější použít klasickou metodu a staticky vyjmenovat domény, kterým důvěřujeme.

Literatura

[1] Satrapa P.: *Greylisting: nová metoda boje proti spamu*. Server Lupa, 23. 4. 2004. ISSN 1213-0702, `http://www.lupa.cz/clanky/greylisting-nova-metoda-boje-proti-spamu/` □