ANALÝZA EFEKTIVITY GRAYLISTINGU JAKO JEDNÉ Z METOD OCHRANY PŘED SPAMEM

František Zeman

katedra informatiky a počítačů, Přírodovědecká fakulta Ostravské univerzity, 30. dubna 22, 701 03 Ostrava, email: Franx.Zeman@seznam.cz

Abstrakt

Úvod

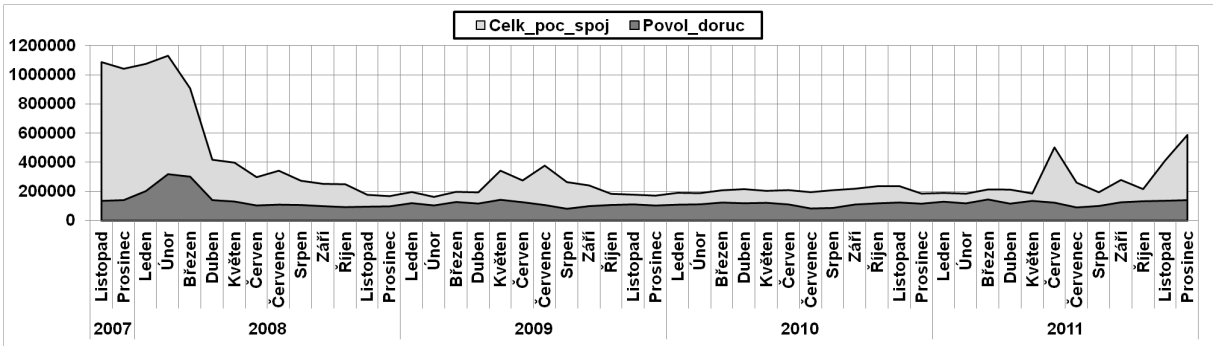
Cílem této činnosti bylo vyhodnocení výsledků antispamového filtru, využívajícího metodu graylistingu, v delší časové řadě, a srovnání získaných údajů s odbornými pracemi, zabývajícími se touto problematikou. Analýza účinnosti filtrace spamu metodou graylistingu byla provedena v rámci vědecké stáže na Ostravské univerzitě na zdejším poštovním serveru. Graylisting je metoda, využívaná jako jeden z článků ochrany poštovních serverů před nevyžádanou poštou, rozpoznávající spam na základě chování odesílatele.

Metody

Výchozími hodnotami pro vyhodnocování efektivity filtrování byly logové soubory z hlavního poštovního serveru Ostravské univerzity mailer.osu.cz z období od listopadu 2007 do prosince 2011. Logové soubory byly načteny do databáze MySQL, ze které byla pomocí SQL dotazů extrahována data potřebná ke zhotovení analýzy účinnosti filtrování. Z databáze byly užitečné hodnoty exportovány do Microsoft Excelu, kde došlo ke konečnému zpracování a znázornění výsledných hodnot graficky.

Výsledky

Nejdůležitější část získaných výsledků je reprezentována grafem níže. Světlá část zobrazuje počet pokusů o doručení zprávy (dále spojení), které byly kontrolovány Postgreyem, programem využívajícím graylistingovou metodu, nasazeném na zdejším serveru. Tmavá část grafu znázorňuje část pokusů o doručení, které kontrolou graylistingu úspěšně prošly. Na grafu můžeme vidět, že celkový počet spojení se v jednotlivých částech sledovaného období značně liší. Největší rozdíl oproti zbytku sledovaného období byl zaznamenán u hodnot na začátku sledovaného období. V první části roku 2008 se počet spojení příchozích na Postgrey snižují a to především proto, že v tomto období byl na síti Ostravské univerzity nasazen nový bezpečnostní prvek (IPS), který dále velké množství příchozích spojení blokoval a tyto požadavky se ke kontrole graylistingem vůbec nedostaly. Ve tmavé části grafu, která znázorňuje počet povolených doručení zpráv, se v jednotlivých měsících sledovaného období hodnoty příliš neliší. Jediný nezanedbatelný výkyv je na začátku roku 2008 a je přisuzován průniku několika IP adres odesílajících spam na seznam umožňující zprávám s danou IP vynechat kontrolu Postgreyem, nazývaný automatický whitelist.



Závěr

Na základě získaných údajů bylo konstatováno, že metoda graylisting je stále efektivním a spolehlivým řešením filtrování nevyžádané pošty, což koresponduje s míněním odborné veřejnosti. Nakonec byla formulována doporučení pro zlepšení účinnosti filtrace, především byl rozpracován návrh automatického blacklistu, nástroje který by měl zamezit doručování zpráv propuštěných na základě slabého automatického whitelistu.

Klíčová slova: *graylisting, e-mail, spam, filtrace*

Poděkování

Tímto bych chtěl poděkovat RNDr. Tomáši Sochorovi, CSc. za pomoc při zpracovávání výsledků a poskytování odborných konzultací.