CENSORSHIP IN THE INTERNET

Jakub Tomaga
Master Degree Programme (2), FIT BUT
E-mail: xtomag00@stud.fit.vutbr.cz

Supervised by: Pavel Očenášek
E-mail: ocenaspa@fit.vutbr.cz

Abstract: This paper deals with Internet censorship. Various technical solutions for Internet censorship are presented together with censorship analysis options. Several possibilities for blocked content access and censorship circumvention in general are discussed. The topic is analysed from the global point of view and is related to the People's Republic of China.

Keywords: Internet censorship, censorship circumvention, surveillance, blocking, filtering

1 ÚVOD

Veľký nárast Internetu v posledných rokoch umožnil bežným užívateľom pristupovať k užitočným informáciám bez obmedzení. Internet ale neobsahuje len relevantné a užitočné informácie. Je rovnako prístupný každému bez ohľadu na úmysly, a nie je možné zabrániť zákernému správaniu sa užívateľov. Kvôli pozitívam a negatívam, ktoré Internet postupne za roky fungovania prebral z reálneho sveta, sa objavili iniciatívy kontrolovať ako ho ľudia využívajú. Súbežne s ochranou detí pred nevhodným obsahom sa objavila cenzúra. Tento článok sa zaoberá Internetovou cenzúrou v Čínskej ľudovej republike.

2 INTERNETOVÁ CENZÚRA

V moderných počítačových sieťach ako je Internet sú cenzúra a sledovanie (monitorovanie komunikácie a aktivít ľudí) v praxi často prepojené. Mnoho poskytovateľov Internetu (ISP – *Internet Service Provider*) monitoruje užívateľov za účelom účtovania služieb a ochrany proti spamu (nevyžiadanej pošte). ISP často zaznamenávajú užívateľské mená spolu s IP adresami. Pokiaľ užívatelia sami nevyužívajú nástroje na zvýšenie bezpečnosti a anonymity je jednoduché na strane ISP zaznamenávať všetky informácie o tokoch, spolu s presným obsahom komunikácie jednotlivých užívateľov. Takéto sledovanie je predpokladom na technickú cenzúru [1].

2.1 CENZORSKÉ PROSTRIEDKY

Jedným zo spôsobov blokovania prístupu k informáciám na webových stránkach je zabrániť prístupu na základe URL, IP adresy alebo kľúčových slov. Ďalším spôsobom je blokovanie na základe DNS (*Domain Name System*). V prípade, kedy webový prehliadač žiada preklad zakázanej adresy, DNS server vráti nesprávnu alebo žiadnu odpoveď [2].

Medzi ďalšie možnosti cenzúry patrí blokovanie na základe portov, *traffic shaping* v prípade VoIP (*Voice over IP*) alebo celkové odstavenie Internetu, ku ktorému dochádza v prípade citlivých politických a sociálnych udalostí.

2.2 ANALÝZA A OVEROVANIE CENZÚRY

V dnešnej dobe je analýza cenzúry Internetu zjednodušená vďaka existencii projektov, ktorých cieľom je sprístupniť Internet z pohľadu užívateľa, ktorého komunikácia podlieha cenzúre. Združenie OpenNet Initiative sa snaží skúmať, odhaľovať a analyzovať praktiky filtrovania Internetu a dohľadu nad jeho užívateľmi dôveryhodným a nezaujatým spôsobom (doplňujúce informácie o neziskovom združení OpenNet Intiative je možné nájsť na `http://opennet.net/`).

Medzi ďalšie projekty patrí WatchMouse. Je možné testovať správanie a dostupnosť webových stránok, služieb a aplikácií využitím infraštruktúry, ktorá zahŕňa 62 monitorovacích staníc po celom svete a sieť kontrolných uzlov v 26 krajinách (detaily na `http://www.watchmouse.com`).

Chinese Firewall Checker je produkt, ktorý umožňuje veľmi jednoducho overiť dostupnosť webových stránok z piatich rôznych lokalít v Číne. Zaujímavosťou tejto služby je rebríček najviac overovaných stránok (otestovať službu je možné na `http://www.bestvpnservice.com/`).

2.3 SPÔSOBY OBÍDENIA CENZÚRY

Existuje niekoľko techník ako prekonať blokovanie Internetu. Ak je cieľom jednoducho len získať prístup k webovým stránkam alebo internetovým službám, ktoré sú nedostupné len z istej lokality a v danom momente nie je podstatné, či sú pokusy o obídenie cenzúry detekovateľné, je možné využiť protokol HTTPS alebo technológie ako proxy servery, VPN (*Virtual Private Network*) a TOR (*The Onion Router*) [1].

Takisto je možné skúsiť pristúpiť na špeciálne verzie, ktoré niektoré stránky vytvárajú pre zariadenia typu *smartphone*. Vo väčšine prípadov majú rovnakú URL s pridaným "`m`"alebo "`mobile`"na začiatku.

Ďalším spôsobom obídenia cenzúry sú služby ako *Google Cache*, *RSS agregátory*, prekladače webových stránok (*Google Translate*, *Bing Translator*, ...) alebo webové archívy (*Wayback Engine*).

3 MOTIVÁCIA

V súčasnosti existuje niekoľko projektov na analýzu a overovanie cenzúry. Vo všetkých prípadoch ide o jednoúčelové aplikácie, ktoré spoločne dokážu vytvoriť ucelený obraz o stave cenzúry v konkrétnych krajinách. Komplexný pohľad na cenzúru Internetu v Čínskej ľudovej republike nie je dostupný, resp. je dostupný na teoretickej úrovni. Mnohé aspekty blokovania prístupu k informáciám nie sú známe.

4 RIEŠENIE

Základom praktického overenia cenzúry sú dve aplikácie. Jedna v domácom (českom) prostredí a jedna v čínskom prostredí. Aplikácia v českom prostredí sa pripája do Číny pomocou dostupných proxy serverov a umožňuje overiť dostupnosť webových stránok a služieb (zobrazuje jednotlivé presmerovania). Výhodou aplikácie je jej umiestnenie mimo čínske prostredie. Nehrozí tak zablokovanie prístupu samotnej webovej aplikácie. Zablokovaný ostane aktuálne využitý proxy server.

Druhá aplikácia umiestnená na čínskom webhostingu umožňuje získať relevantnejšie informácie o blokovaní a prístupe k jednotlivým službám. Riziko zablokovania je pomerne veľké, preto je jednotlivé testy potrebné vykonávať až po ich dôkladnom otestovaní z českého prostredia.

Nastavenie webhostingu neumožňuje spúšťať príkazy ako je `ping` a `traceroute` (PHP na serveri má aktivovaný safe mode – bezpečnostný prvok navrhnutý za účelom ochrany pred hackerskými pokusmi spúšťať príkazy na úrovni operačného systému [3]). Výsledky uvedených príkazov by

URL	Proxy server			
	Hong Kong (14.102.253.251)	**Beijing** (112.25.13.36)	**Shanghai** (210.13.71.77)	**Guangzhou** (121.8.124.42)
facebook.com	OK	Conn Reset	Timeout	Conn Reset
twitter.com	OK	ConReset	Conn Reset	Conn Reset
vutbr.cz	OK	OK	OK	Timeout
google.com	OK	Conn Reset	Conn Reset	Conn Reset
google.com.hk	OK	OK	OK	OK
google.com.hk/?q=freedom	OK	Conn Reset	Conn Reset	Conn Reset

Tabulka 1: Ukážka dosiahnutých výsledkov z českého postredia

umožnili presnejšie geograficky lokalizovať pozíciu čínskych firewallov. Využitý webhosting poskytuje len webové rozhranie na nahrávanie súborov.

Možnosťou riešenia tohto problému je spustiť uvedené príkazy v druhom smere (IP adresa na strane čínskeho poskytovateľa je známa). V tomto prípade hrozí riziko, že bude komunikácia smerovaná inou cestou. Analýzou jednotlivých uzlov je možné identifikovať webové, resp. iné servery.

Hlavným výstupom práce je lokalizácia čínskych firewallov a analýza ich funkčnosti (odhad na základe blokovania, resp. prepustenia istého typu komunikácie). Overenie cenzúry je rozšírené o analýzu e-mailových protokolov, protokolov NNTP a FTP, pomocou ktorých je možné napr. testovať prenos príloh so zakázaným obsahom v smere z a do Číny.

5 ZÁVER

V súčasnosti je implementovaná aplikácia v českom prostredí, pomocou ktorej je možné overiť dostupnosť webových stránok v prípade pripojenia cez proxy server. Dosiahnuté výsledky sú porovnateľné s výsledkami existujúcich projektov, ale výrazne závisia na stabilite a dostupnosti zvolených (konfigurovateľných) proxy serverov. Výsledky sú v niektorých prípadoch skreslené kvôli odozve konkrétnych proxy serverov a tým pádom je možné dosiahnuť nepravdivé výsledky (aplikácia prehlási istú webovú stránku za nedostupnú aj v prípadoch, že je z čínskeho prostredia bez problémov prístupná). Tabuľka 1 obsahuje ukážku dosiahnutých výsledkov.

POĎAKOVANIE

Táto práca vznikla za podpory následujúcich projektov: MŠMT ČR Výzkum informačních technologií z hlediska bezpečnosti (MSM0021630528), IT4Innovations Centre of Excellence (CZ.1.05/1.1.00/02.0070) a FIT-S-11-1.

REFERENCE

[1] Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, Jonathan Zittrain: Access Denied - The Practice and Policy of Global Internet Filtering. The MIT Press, 2008, ISBN 0-262-54196-3

[2] William Stallings: Cryptography and network security: principles and practice. Prentice Hall, 1999, ISBN 0-13-869017-0

[3] Ed Lecky-Thompson, Seven D. Nowicki, Thomas Myer: Professional PHP6. Wiley Publishing, Inc., 2009, ISBN 978-0-470-39509-7