Název: Anonymizační proxy systém

Vedoucí: Leo Galamboš

Počet řešitelů: 5

Abstrakt:

V dnešní době je kvalitní anonymizace bežnou, legitimní a velmi poptávanou službou. Bohužel žádný z aktuálně existujících anonymizérů (ToR, JonDonym) neuspokojuje požadavky značné části zájemců o anonymizaci a to z mnoha důvodů. Prvním důvodem je nedostatečná transparentnost stávajících systémů (anonymizují pouze TCP spojení, nikoliv UDP a ICMP pakety), druhým problémem je velmi omezená distributivita, která se projevuje buď centrálním katalogem proxy serverů nebo centrální certifikační autoritou. Dalším nedostatkem je nemožnost dostatečně silného řízení toku (volby rychlosti a latence uzlů a především volby koncového uzlu, jehož IP adresou bude klient vůči druhé straně spojení vystupovat), a chybějící podpora pro IPv6 protokol. Poslední významnější slabina stávajících systémů spočívá v anonymizaci na vyšších IP vrstvách, bez možnosti ovlivnění podoby paketů vystupujících z anonymizační sítě.

Charakteristika řešení:

Výsledný anonymizér bude fungovat jako plně P2P síť, v níž bude každý počítač plnit roli (nebo několik těchto rolí):

- klient: uzel, který je vstupem uživatelské konekce do anonymizační sítě
- gateway (relay): uzel, který přeposílá pakety uživatelské konekce v rámci anonymizační sítě
- výstupní gateway: uzel, který odesílá pakety uživatelské konekce ven z anonymizační sítě

Veškerá komunikace mezi uzly anonymizační sítě bude šifrována, například za použití RSA (pro navazování spojení a autorizaci) a blokové symetrické šifry (pro samotné šifrování komunikace).

Autorizace jednotlivých strojů v systému bude řešena pomocí technologie Web of Trust, aby byla zajištěna jednak plná distributivita a jednak možnost spojování nebo naopak rozdělování výsledných sítí.

Klient bude mít možnost výběru cesty svých paketů:

1.počtem gatewayí, přes něž je vedena,

2.konkrétní definicí gatewayí v rámci anonymizační sítě,

3.detailními parametry cesty v rámci anonymizační sítě (propustnost, latence, výstupní gateway, ap.)

Cíl projektu:

Cílem projektu je naimplementovat anonymizační systém splňující následující požadavky:

- perfect forward secrecy
- podpora a přenos TCP, UDP i ICMP nad IPv4 a Ipv6
- ustanovování bezpečných cest (okruhů) na bázi "web of trust"
- možnost parametrizace otevíraného spoje a řízení toku (propustnost, latence, poloha výstupního uzlu)
- plně transparentní napojení na vytvořený anonymizační prostředek pro všechny uživatelské aplikace, zejména pro webový prohlížeč
- multiplatformová serverová aplikace (minimálně pro Linux, FreeBSD a OpenBSD)