



PB169 – Operační systémy a sítě

Anonymní komunikace – praktické příklady

Marek Kumpošt, Zdeněk Říha

Motivace pro anonymitu

- Ochrana osobních dat
- Anonymita uživatele, lokace, transakce
- 4 funkčnosti systémů pro ochranu inf. soukromí
 - anonymita
 - pseudonymita
 - nesledovatelnost
 - nepozorovatelnost

Motivace pro anonymitu

- Nutnost zajistit anonymitu v mnoha případech
 - informace o zdravotním stavu (anonymita vs. pseudonymita)
 - elektronické volby
 - svoboda slova
 - udání informací o trestné činnosti apod.

Anonymita vs. pseudonymita

- Anonymita – chování zcela anonymní, neexistuje možnost zjištění skutečné identity subjektu
 - např. informace o zdravotním stavu bez vazby na identitu skutečného pacienta
- Pseudonymita – chování je anonymní, existuje možnost zpětného zjištění skutečné identity subjektu
 - stanovení diagnózy – jednoznačné spojení s pacientem
 - lékař zná pouze nějaké ID pacienta
 - v systému existují záznamy (ID, jméno), ke kterým ale ošetřující lékař nemusí mít přístup

Příklady systémů pro anonymní komunikaci

- Mixminion
- Onion routing
- TOR
- Projekt AN.ON
- Anonymní proxy

Mixminion

- Mixovací síť pro odesílání anonymních emailových zpráv
- Uživatel má možnost specifikovat cestu v síti
- SURB – Single use reply block
 - Možnost odpovědět na anonymní zprávu
 - Omezená platnost „odpovědního lístku“
 - Zašifrovaná informace o „zpáteční cestě“
 - Odpověď je v síti nerozlišitelná od normální zprávy
- Volně dostupný systém – www.mixminion.net

Mixminion

- Praktická ukázka (formou screenshotů)
 - Odeslání anonymní zprávy
 - Jak vypadá anonymní zpráva po doručení
 - Zejména její hlavička
 - Možnost provozu vlastního mixovacího uzlu

Mixminion version 0.0.7.1

This software is for testing purposes only. Anonymity is not guaranteed.

Mixminion version 0.0.7.1

Type 'help' for information, or 'exit' to quit.

mixminion>

Mixminion version 0.0.7.1

This software is for testing purposes only. Anonymity is not guaranteed.

Mixminion version 0.0.7.1

Type 'help' for information, or 'exit' to quit.

mixminion>help

Usage: mixminion <command> [arguments]

where <command> is one of:

	(For Everyone)
version	[Print the version of Mixminion and exit]
send	[Send an anonymous message]
queue	[Schedule an anonymous message to be sent later]
flush	[Send all messages waiting in the queue]
inspect-queue	[Describe all messages waiting in the queue]
clean-queue	[Remove old messages from the queue]
import-server	[Tell the client about a new server]
list-servers	[Print a list of currently known servers]
update-servers	[Download a fresh server directory]
decode	[Decode or decrypt a received message]
generate-surb	[Generate a single-use reply block]
inspect-surbs	[Describe a single-use reply block]
ping	[Quick and dirty check whether a server is running]
	(For Servers)
server-start	[Begin running a Mixminion server]
server-stop	[Halt a running Mixminion server]
server-reload	[Make running Mixminion server reload its config (Not implemented yet; only restarts logging.)]
server-republish	[Re-send all keys to directory server]
server-DELKEYS	[Remove generated keys for a Mixminion server]
server-stats	[List as-yet-unlogged statistics for this server]
server-upgrade	[Upgrade a pre-0.0.4 server homedir]
	(For Developers)
dir	[Administration for server directories]
unittests	[Run the mixminion unit tests]
benchmarks	[Time underlying cryptographic operations]

For help on sending a message, run 'mixminion send --help'

NOTE: This software is for testing only. The user set is too small to be anonymous, and the code is too alpha to be reliable.

mixminion>

NOTE: This software is for testing only. The user set is too small to be anonymous, and the code is too alpha to be reliable.

mixminion>list-servers

Mixminion version 0.0.7.1

This software is for testing purposes only. Anonymity is not guaranteed.

Feb 02 12:12:19.824 +0100 [INFO] Downloading directory from http://mixminion.net/directory/Directory.gz

Feb 02 12:12:22.968 +0100 [INFO] Validating directory

Feb 02 12:12:24.500 +0100 [WARN] This software is newer than any version on the recommended list.

```
almercy:mbox relay      (ok)
antani:smtp relay      (not recommended)
banana:mbox smtp relay frag (ok)
bigapple:smtp relay    (ok)
cassandra:relay (ok)
cside:mbox relay       (ok)
dantooine:smtp relay   (ok)
debsun:relay (ok)
deuxpi:smtp relay frag (ok)
devilmixmin:mbox smtp relay (ok)
flutic:mbox relay      (ok)
frell:smtp relay frag  (ok)
frell2:relay (ok)
geonosis:smtp relay    (ok)
grove:mbox relay frag  (ok)
gurski:mbox relay frag (ok)
hermes:mbox relay frag (ok)
Hume:mbox relay frag   (not recommended)
KisanganiToo:relay    (not recommended)
laforge:mbox smtp relay frag (ok)
mercurio:mbox smtp relay (not recommended)
mordor:mbox relay frag (ok)
nefarion:smtp relay    (ok)
nixon:mbox relay        (ok)
noisebox:relay (ok)
nowwhat:mbox relay frag (ok)
osen:relay (ok)
paranion:mbox smtp relay (ok)
pbox-level-2:smtp relay (not recommended)
pboxlevel3:smtp relay  (ok)
phobos:relay (ok)
PObox:relay (ok)
psycocat2:mbox relay   (ok)
pyradic:relay (ok)
Rivendell:relay (ok)
rot26:relay (ok)
rufus:relay (ok)
snorky:relay (ok)
straylight:mbox smtp relay (ok)
sumatra:relay (ok)
Tonga:smtp relay frag  (ok)
vidorz:relay (ok)
winnie:smtp relay (ok)
wiredyne:mbox relay frag (ok)
xbox:smtp relay (ok)
yog:relay (ok)
```

mixminion>

```
cassandra:relay (ok)
cside:mbox relay (ok)
dantooine:smtp relay (ok)
debsun:relay (ok)
deuxpi:smtp relay frag (ok)
devilmixmin:mbox smtp relay (ok)
flutic:mbox relay (ok)
frell:smtp relay frag (ok)
frell2:relay (ok)
geonosis:smtp relay (ok)
grove:mbox relay frag (ok)
gurski:mbox relay frag (ok)
hermes:mbox relay frag (ok)
Hume:mbox relay frag (not recommended)
KisanganiToo:relay (not recommended)
laforge:mbox smtp relay frag (ok)
mercurio:mbox smtp relay (not recommended)
mordor:mbox relay frag (ok)
nefarion:smtp relay (ok)
nixon:mbox relay (ok)
noisebox:relay (ok)
nowwhat:mbox relay frag (ok)
osem:relay (ok)
paranion:mbox smtp relay (ok)
pbox-level-2:smtp relay (not recommended)
pboxlevel3:smtp relay (ok)
phobos:relay (ok)
PObox:relay (ok)
psycocat2:mbox relay (ok)
pyradic:relay (ok)
Rivendell:relay (ok)
rot26:relay (ok)
rufus:relay (ok)
snorky:relay (ok)
straylight:mbox smtp relay (ok)
sumatra:relay (ok)
Tonga:smtp relay frag (ok)
vidorz:relay (ok)
winnie:smtp relay (ok)
wiredyne:mbox relay frag (ok)
xbox:smtp relay (ok)
yog:relay (ok)
```

```
mixminion>send -t xkumpost@fi.muni.cz
```

```
Mixminion version 0.0.7.1
```

```
This software is for testing purposes only. Anonymity is not guaranteed.
```

```
Feb 02 12:13:20.751 +0100 [WARN] This software is newer than any version on the recommended list.
```

```
Enter your message now. Type Ctrl-Z, Return when you are done.
```

```
testovaci zpravicka
```

```
^Z
```

```
Feb 02 12:13:28.022 +0100 [INFO] Generating payload(s)...
```

```
Feb 02 12:13:28.072 +0100 [INFO] Selected path is grove,noisebox,nixon:grove,nefarion
```

```
Feb 02 12:13:28.172 +0100 [INFO] Packet queued
```

```
Feb 02 12:13:28.172 +0100 [INFO] Connecting...
```

```
Feb 02 12:13:30.856 +0100 [INFO] ... 1 sent
```

```
mixminion>
```

Mixminion version 0.0.7.1

This software is for testing purposes only. Anonymity is not guaranteed.

Mixminion version 0.0.7.1

Type 'help' for information, or 'exit' to quit.

mixminion>ping grove

Mixminion version 0.0.7.1

This software is for testing purposes only. Anonymity is not guaranteed.

=====
WARNING: Pinging a server is potentially dangerous, since
it might alert people that you plan to use the server
for your messages. Even if you ping *all* the servers,
an attacker can see when you pinged the servers and
use this information to help a traffic analysis attack.

This command is for testing only, and will go away before
Mixminion 1.0. By then, all listed servers will be
reliable anyway. <wink>

=====
Feb 02 12:16:08.462 +0100 [WARN] This software is newer than any version on the
recommended list.

>>> Server seems to be running

grove is up

mixminion>

Přijatý mail - hlavičky

Received: from <remailer@dizum.com> for <xkumpost@mail255.centrum.cz>

Received: from localhost ([127.0.0.1])

by localhost (Centrum Mailer) with SMTP

;Wed, 13 Apr 2005 07:49:07 +0200

X-SpamDetected: 0

Received: from outpost.zedz.net ([194.109.206.210]:48546 "EHLO

outpost.zedz.net") by data2.centrum.cz with ESMTP id S15926716AbVDMFpO
(ORCPT <rfc822;xkumpost@mail255.centrum.cz>);

Wed, 13 Apr 2005 07:45:14 +0200

X-SpamDetected: 0

Received: from localhost (outpost [127.0.0.1])

by outpost.zedz.net (Postfix) with ESMTP id F143F50335

for <xkumpost@centrum.cz>; Wed, 13 Apr 2005 02:39:51 +0200 (CEST)

Received: by outpost.zedz.net (Postfix, from userid 1009)

id 3069050E68; Tue, 12 Apr 2005 22:30:02 +0200 (CEST)

From: Nomen Nescio <nobody@dizum.com>

Comments: This message did not originate from the Sender address above.

It was remailed automatically by anonymizing remailer software.

Please report problems or inappropriate use to the
remailer administrator at <abuse@dizum.com>.

To: xkumpost@centrum.cz

Subject: Type III Anonymous message

X-Anonymous: yes

Message-ID: <d1e6d5c363fc0e8b86f2d0974257f1f5@dizum.com>

Date: Tue, 12 Apr 2005 22:30:02 +0200 (CEST)

X-Virus-Scanned: by outpost.zedz.net (amavis-20020300)

Přijatý mail – tělo zprávy

-----BEGIN TYPE III ANONYMOUS MESSAGE-----

Message-type: plaintext

testovací zprava

cas 11:22

-----END TYPE III ANONYMOUS MESSAGE-----

Charakteristika Onion Routing systémů

- Onion routing – Cibulové směrování
 - Anonymní komunikace ve veřejné síti
 - Poskytuje obousměrné anonymní spojení
 - Téměř real-time anonymní spojení pro různé služby (www, ssh, ftp, ...)
- Proč Onion Routing, když máme mixy?
 - Zpoždění u mixů pro real-time aplikace nepřijatelné
 - OR poskytuje anonymní přenos bez nutnosti modifikace použitých služeb – pracuje jako proxy
- TOR – The Onion Routing
 - Systém druhé generace – řada vylepšení

Zpracování dat v OR

- Přes sérii Onion Routerů namísto přímého spojení klient-server
 - Každý OR zná pouze svého předchůdce a následníka
 - Vzájemné spojení OR je permanentní
 - Komunikační cesta (okruh) je definována při sestavení komunikačního kanálu
 - Data jsou důsledkem dešifrování na každém OR „změněna“

Zpracování dat v OR

- Alice – [[zpráva]] → OR – [zpráva] → OR – zpráva → Bob
- Každý průchod přes OR „sloupne“ (odšifruje) jednu vrstvu
- K OR síti se přistupuje přes speciální proxy
 - V původním návrhu nutná proxy pro každou službu – podpora omezeného počtu aplikací
 - Aplikace se spojí s aplikační proxy
 - Apl. proxy transformuje data do podoby srozumitelné pro OR síť
 - Apl. proxy vytvoří spojení s OR proxy
 - dojde k vytvoření komunikačního okruhu
 - Okruh je připraven pro přenos dat

Zpracování dat v síti OR

- Komunikační okruhy
 - OR proxy vytvoří vrstvenou datovou strukturu a pošle ji do sítě (využívá se PKC)
 - Každý OR odstraní vrchní vrstvu; získá materiál pro ustavení sym. klíče a zbylá data pošle na další OR
 - Takto projde „cibule“ až na poslední OR
 - Výsledkem je vytvořený komunikační okruh (ustavení sym. klíčů mezi odesilatelem a každým OR)

Obrana proti reply útokům

- Každý OR si ukládá seznam přeposlaných paketů dokud nevyprší jejich platnost
 - Případné duplicity jsou zahozeny

TOR – The Onion Router

- Systém pro anonymní komunikaci založený na komunikačních okruzích s malou latencí
 - Následník původního OR návrhu
 - Implementace nových funkcionalit

TOR

- TOR přináší následující vylepšení
 - dokonalé „dopředné“ utajení
 - není nutné vyvíjet specializované apl. proxy
 - podpora většiny TCP-based aplikací bez modifikace
 - více TCP proudů může sdílet komunikační okruh
 - data mohou opustit síť v libovolném místě
 - kontrola možného zahlcení sítě
 - podpora adresářových serverů – info o síti
 - end-to-end testování integrity přenesených dat
 - ochrana proti tagging útokům
 - „místa setkání“ a skryté služby
 - nevyžaduje změny v jádře operačního systému
 - volně dostupný systém

TOR – perfect forward secrecy

- Klíče sezení nejsou ohroženy, pokud by někdy v budoucnu došlo k vyzrazení hlavního klíče
 - v původním návrhu mohl útočník ukládat data a následně přinutit uzly data dešifrovat
- Jiný způsob budování komunikační cesty
 - Teleskopické ustavení okruhu
 - odesílatel ustanoví symetrické klíče se všemi uzly v okruhu
 - po smazání klíčů nelze dešifrovat starší data
- Proces budování kom. cesty více spolehlivý

Místa setkání a skryté služby

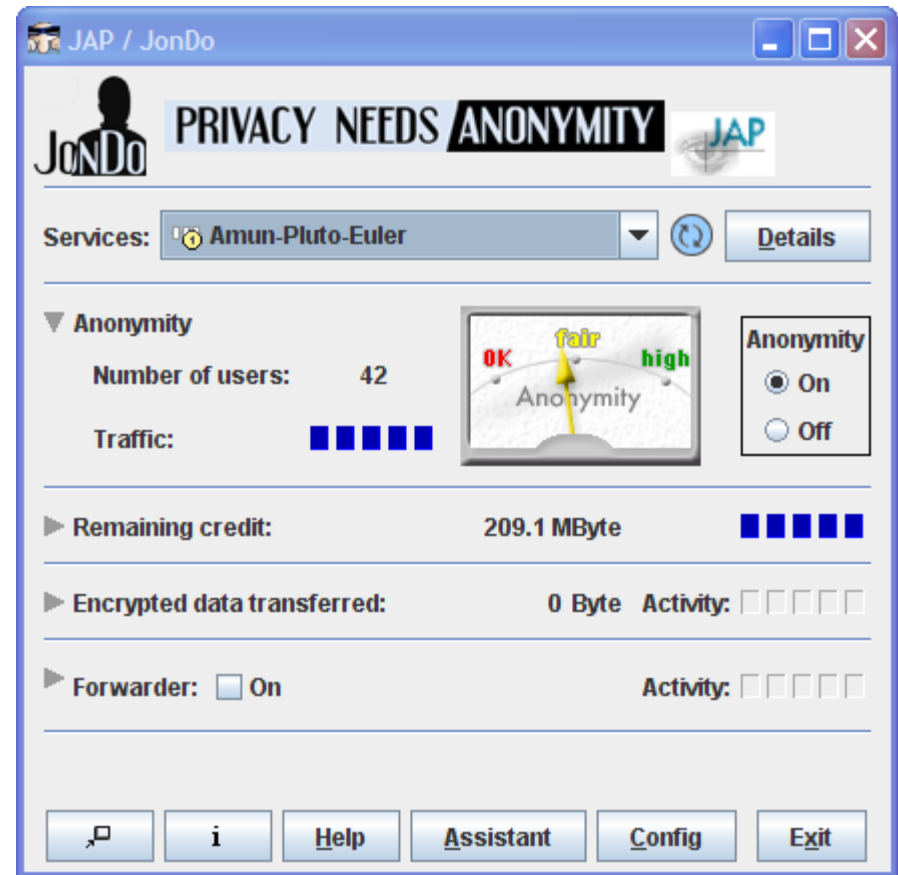
- Pro zajištění anonymity příjemce (serveru, služby...)
 - Možnost řízení příchozího datového toku
- Zabrání Denial of Service (DoS) útokům
 - Útočník neví, kde je daný server
 - Server je skrytý za několika OR
- Klient zvolí místo setkání v OR síti, přes které se spojí se „serverem“, resp. na OR, který server zveřejní
 - Informace o serveru prostřednictvím adresářové služby
 - Klient se dozví, na jakých OR server „čeká“ na spojení

TOR – analýza provozu

- George Danezis a Steven J. Murdoch, 2005
- Nová technika analýzy provozu pro TOR
 - TOR nepoužívá zpoždění pro předávané zprávy
 - Související proudy dat jsou zpracovávány stejnými uzly
- Útočníkovi stačí pouze omezená informace ze sítě
- Silně snižuje anonymitu provozu v TORu

Anonymity online – projekt AN.ON

- Technical university dresden
- Institute for system architecture

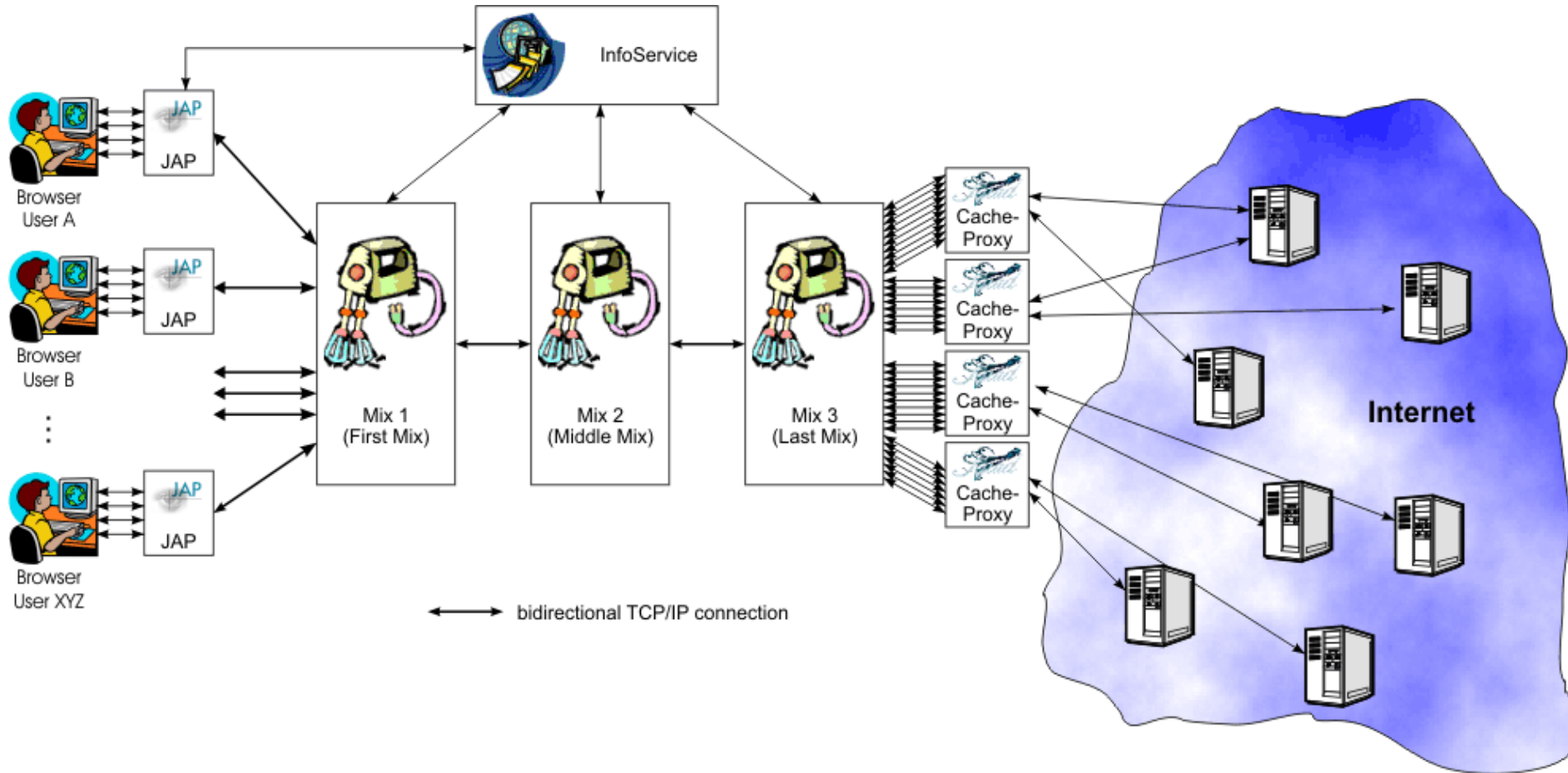


<https://www.jondos.de/en/>

Anonymity online – projekt AN.ON

- Služba poskytující anonymitu
- Nepřímé spojení s cílovým serverem
- Spojení přes *kaskády mixů*
- Kaskády pevně dané, uživatel si může zvolit
 - Některé kaskády zpoplatněné – lepší propustnost
- Mixy využívá množství uživatelů současně
- Mixy provozují nezávislé organizace
- Podpora služeb – HTTP(S), FTP

AN.ON – použití



AN.ON - použití

- Instalace klientské aplikace JonDo
- Připojení přes proxy – browser se připojuje přes tuto proxy
- JonDoX – instalace celku (prohlížeč + JonDo)

Anonymní proxy

- Co je to proxy server
 - Aktivní síťový prvek, který vyřizuje požadavky klientů
 - Klient požaduje webovou stránku, požadavek vyřídí proxy, ta mu předá výsledek
 - Proxy ukládá výsledky požadavků po nějakou dobu v cache
 - Cílový server zpravidla vidí pouze komunikaci s proxy serverem

Anonymní proxy

- Použijeme v případě, kdy nechceme zveřejnit svoji IP adresu
- Existuje řada anonymních proxy, viz. google
- <http://www.atomintersoft.com/products/alive-proxy/proxy-list/>
- <http://www.proxz.com/>

Použití anonymního proxy serveru

- Zvolíme proxy
 - V případě SSL připojení musíme použít proxy podporující SSL
 - Pozor na změnu certifikátů!!!
- Např. 128.223.6.112:3128
 - Nastavíme do prohlížeče
- Můžeme otestovat naší vnější IP
 - <http://anoncheck.security-portal.cz/>

Security-Portal :: Anonymity checker

užíváte prohlížeč Firefox/1.5!

š počítač běží pod operačním systémem Windows XP!

š IP adresa: 147.251.51.215

stname: wireless-215.fi.muni.cz

užívaný jazyk:

šel jste sem ze stránky:

pojil jste se z portu: 4285

porované jazyky prohlížeče: cs

porované znakové sady: ISO-8859-2,utf-8;q=0.7,*;q=0.7,UCS-2;q=0, UCS-4;q=0, UTF-1;q=0

porované typy kódování: gzip,identity

ceptovatelné MIME typy: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5

užitý typ http konexe: dose

rze protokolu: HTTP/1.1

obis cookie:

ny název prohlížeče: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8) Gecko/20051111 Firefox/1.5

[- Hlavičky zasílané proxy serverem -]

vička která nejčastěji vyrazí vaši pravou IP (X_FORWARDED_FOR):

rze protokolu a název proxy serverů, přes které šla data:

vička CLIENT_IP:

vička FORWARDED:

užívaný typ proxy konexe:

xy autorizace, která se skládá z base64(uživatel:heslo):

o hlavička nám zobrazí nastavení cachování proxy serveru či klienta: no-cache

vička EXTENSION:

ximální počet proxy serverů, přes které může požadavek jít:

rze MIME (Multipurpose Internet Mail Extensions), defaultně v1.0:

ecifické direktivy, které "musí" každý proxy server splnit: no-cache

ne všechna pole musí obsahovat hodnoty. Důvodem je prostě to, že v nich klient ani proxy server nic neodesílá.

Security-Portal :: Anonymity checker

užíváte prohlížeč Firefox/1.5!

š počítač běží pod operačním systémem Windows XP!

š IP adresa: 131.215.45.72

stname: planlab2.cs.caltech.edu

užívaný jazyk:

šel jste sem ze stránky:

pojil jste se z portu: 58308

porované jazyky prohlížeče: cs

porované znakové sady: ISO-8859-2,utf-8;q=0.7,*;q=0.7,UCS-2;q=0, UCS-4;q=0, UTF-1;q=0

porované typy kódování: gzip,identity

ceptovatelné MIME typy: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5

užitý typ http konexe: keep-alive

ze protokolu: HTTP/1.0

bis cookie:

ny název prohlížeče: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8) Gecko/20051111 Firefox/1.5

[- Hlavičky zasílané proxy serverem -]

vička která nejčastěji vyzradí vaši pravou IP (X_FORWARDED_FOR):

ze protokolu a název proxy serverů, přes které šla data:

vička CLIENT_IP:

vička FORWARDED:

užívaný typ proxy konexe:

xy autorizace, která se skládá z base64(uživatel:heslo):

o hlavička nám zobrazí nastavení cachování proxy serveru či klienta: no-cache

vička EXTENSION:

ximální počet proxy serverů, přes které může požadavek jít:

ze MIME (Multipurpose Internet Mail Extensions), defaultně v1.0:

ecifické direktivy, které "musí" každý proxy server splnit: no-cache

ne všechna pole musí obsahovat hodnoty. Důvodem je prostě to, že v nich klient ani proxy server nic neodesílá.

Otázky?