УДК 004.7

Ганна ПОГРОМСЬКА
pas012@ukr.net
Геннадій ЧЕРНИЩУК
genaloner@gmail.com
м. Миколаїв

РЕАЛІЗАЦІЯ АПЛЕТУ ДЛЯ АНОНІМІЗАЦІЇ ТРАФІКУ ЗА ДОПОМОГОЮ МЕРЕЖІ TOR

У статті проведено аналіз засобів анонімізації трафіку (VPN, проксі-сервер, I2P, SSH-тунель, виділений сервер) та окреслено їх переваги та недоліки. Було обрано мережу Tor як найбільш універсальний та гнучкий метод. Зараз не існує жодного доданка з інтерфейсом для зручного налаштування віртуального проксі-сервера Tor. Метою статті постала розробка програмного забезпечення для зручної роботи та налаштування локального проксі Tor з інтеграцією у середовище робочого столу.

Програмний продукт «Tor Button» є аплетом для середовища робочого столу Cinnamon, написаний на мові програмування JavaScript з використанням API для взаємодії з середовищем. Призначенням «Tor Button» є зручний запуск та налагодження віртуального проксі-сервера для Tor, що дозволяє пропускати будь-який трафік через нього. Пропонований програмний продукт забезпечує: зручний доступ для запуску проксі-сервера; можливість вибору шляху до самого сервера та файлу конфігурації; можливість запуску сервера від імені користувача мережі Tor; можливість швидкої перебудови мережевого ланцюга. Програмний продукт «Tor Button» розташовано на офіційному сайті аплетів для Cinnamon (https://cinnamon-spices.linuxmint.com/applets/view/298) під іменем автора.

Практичність аплету забезпечується завдяки простому та ергономічному інтерфейсу. Відкритий сирцевий код та доступ до сторінки на GitHub надає можливість кожному користувачу розширити функціонал або додати переклад на рідну мову. Вже зараз аплет переведений на датську, російську, турецьку та китайську мови.

***Ключові слова**: Tor, аплет, мережа, проксі-сервер, інтерфейс, браузер, Cinnamon, GitHub.*

Постановка проблеми

З розвитком Інтернет в наш час набуває все більшої актуальності тема анонімності в мережі. Це пов'язано з тим, що з його популяризацією починає приходити цензура, інформаційні злочини та шпіонаж за особистими даними користувачів. Наприклад, багато сайтів збирають персональні данні, які можуть використовуватися для будь-яких цілей – починаючи від реклами та закінчуючи кіберзлочинами. Розкриття IP-адреси та операційної системи може зробити вас уразливим для кібератак. Користувачі повинні мати право на анонімний пошук інформації в Інтернет, в тому числі приховувати свої IP-адреси і відправляти повідомлення анонімно. Як свідчить практика, підвищення анонімності часто робить перебуванння в Інтернет менш зручним. Найчастіше користувачі, яких турбує власна анонімність, шукають «золоту середину» між анонімністю та зручністю використання.

Саме для вирішення вищезазначених проблем існують методи анонімізації в мережі. Але зручність налаштування багатьох віртуальних проксі-серверів досі залишається невирішеним питанням.

Аналіз останніх досліджень і публікацій

Засобів для анонімізації дуже багато (Tor, I2P, Dissent, SSH-тунелі, різноманітні проксі- та VPN-сервіси) і у кожного з них є свої переваги і недоліки. Наприклад, на сторінках сайту Cryptoworld (cryptoworld.su) – сайт з практичної безпеки, пропонується

7 основних методів. На сайті Хабрахабр (habrahabr.ru), який є колективним блогом для аналітичних статей та новин з галузі інформаційних технологій, представлена серія статей під назвою «Методи анонімності в мережі», де розглядаються позитивні сторони та недоліки різних методів анонімізації.

Проксі-сервер – це проміжний сервер, який є посередником між групою користувачів і мережею Інтернет [13]. Серед способів застосування проксі-серверів виділимо: кешування даних, одержуваних з мережі; анонімізація в мережі. До *переваг* проксі можна віднести простоту в роботі, їх поширеність і наявність безкоштовних серверів. До *недоліків* – безкоштовні проксі найчастіше продають дані користувачів третім особам.

Автор Лавин Д. [7] пропонує наступне визначення *VPN* (Virtual Private Network – віртуальна приватна мережа) – це віртуальна мережа (криптосистема), що дозволяє захищати дані при передачі їх по незахищеній мережі, такі як Інтернет. Відмінність VPN від проксі-серверів полягає в тому, що VPN передає дані через зашифровані тунелі, що анонімізує трафік користувача від провайдера або уряду. Останні можуть тільки встановити, яким сервером VPN користуються, тому що ваша IP-адреса і трафік перед потраплянням в тунель шифруються. Але такі сервера коштують дорожче, ніж проксі-сервера і зазнають більш високе навантаження через наявність шифрування.

За стандартом архітектури протоколу RFC 4251 [9] *SSH тунель* (або SSH Port Forwarding) – це тунель, який створюється за допомогою опціонального функціоналу SSH (Secure SHell) з'єднання для шифрування даних, які передаються. Особливість полягає в тому, що незашифрований трафік будь-якого протоколу шифрується на одному кінці SSH з'єднання і розшифровується на іншому. До *переваг* SSH-тунелів віднесемо простоту налаштування між будь-якими ОС і гнучкість. До *недоліків* – непоширеність та вартість останніх.

Виділений сервер (*dedicated server*) – вид хостингу, який надає в користування фізично віддалену машину [12]. Виділений сервер може використовуватися для приховування своєї особистості в мережі, хоч і основний його функціонал – це хостинг додатків і сервісів.

З *переваг* можна виділити більш високий рівень анонімності, ніж у попередніх методів, захист від атак через Flash, JavaScript, Java і контроль історії запитів. Серед *недоліків* – висока вартість оренди (вона набагато вище, ніж у методів, описаних вище), проблема недовіри до Інтернет-провайдера хостинга, а також необхідність вказувати свої дані при реєстрації.

Практик з галузі мережевого та системного адміністрування Лавин Д. зазначає, що *I2P* – анонімна мережа, яка надає простий шар, який може використовуватися програмами для анонімного і безпечного обміну повідомленнями [7]. Сама мережа заснована на повідомленнях (як IP), але є і бібліотека для організації гарантованого потокового зв'язку поверх мережі (як TCP). Всі комунікації використовують наскрізне шифрування (всього використовується чотири шари шифрування при відправці повідомлення), і навіть самі абоненти («напрями») є криптографічними ідентифікаторами (по суті парою публічних ключів).

Із *переваг* I2P можна виділити високий рівень анонімності клієнта (при обережному користуванні); повну децентралізацію, що робить мережу дуже стійкою; конфіденційність даних через крізне шифрування між клієнтом і адресатом; дуже високу ступінь анонімності сервера (його IP-адреса невідома). Але I2P має такі *недоліки*: низька швидкість, довший час відгуку, незахищеність від атаки через Java, Flash і JavaScript (тому для більшої анонімності їх потрібно відключати).

На офіційному сайті проекта *Tor* [10] зазначено, що Tor – це безкоштовне програмне забезпечення та відкрита мережа, яка допомагає захищатись від аналізу трафіку – форми мережевого спостереження,

що загрожує особистій свободі та конфіденційності, конфіденційній діловій діяльності, а також державній безпеці [10]. Tor відрізняється від I2P наступним: основним завданням Tor'а є приховати справжню IP-адресу клієнта, а I2P, навпаки, власників серверів. Таким чином, Tor є мережею клієнтів, а I2P – серверів. Звичайно, є і onion-сайти в Tor, і вихідні вузли в I2P, проте це скоріше побічні технології.

До *переваг* такого способу анонімізації можна віднести високу гнучкість у налаштуванні, тому що користувач самостійно обирає для себе оптимальні параметри між анонімністю і швидкістю роботи; простоту у використанні; безкоштовність та відкритий сирцевий код. До *недоліків* – відносно низьку швидкість, тому що трафік проходить через ланцюг серверів (їх також називають нодами); можливість прослуховування вихідного трафіку; можливість деанонімізації при увімкнених Flash, Java і JavaScript (саме тому ці компоненти вимкнуті в Tor Browser). Саме гнучкість Tor у налаштуванні робить його доречним для більшої кількості користувачів. Наприклад, в залежності від потреб можна збільшити або кількість серверів у ланцюжку для збільшення анонімності або навпаки, зменшити їх кількість і вибрати найближчі за розташуванням країни серверів для збільшення швидкості.

15 років тому, до появи кібератак і масового розкрадання даних через Інтернет, люди не особливо замислювалися про шифрування будь-якої інформації в мережі. На думку Сіверсона П. [1] Tor є актуальним і затребуваним засобом, для безпечного серфінгу в Інтернеті.

На офіційному сайті Tor [10] пропонується для завантаження спеціальний браузер, заснований на Firefox, в якому весь трафік проходить через мережу Tor та внесені зміни для поліпшення приватності. Наприклад, в ньому відключені плагіни браузера, такі як Flash (для запобігання атак), видалена синхронізація, аналітика та інші сервіси від Firefox, вимкнено збереження Cookies та паролів та, за замовченням, у браузері є спеціальні доданки, які потрібні для більшої безпеки та налаштування Tor: HTTPS Everywhere, NoScript, Torbutton та TorLauncher.

Для перенаправлення трафіку іншого доданка, розроблений Tor Expert Bundle, який теж можна завантажити з офіційного сайту [10]. Він включає в собі тільки віртуальний проксі, це дозволяє не запускати у фоні цілий браузер, що потребує багато ресурсів, заради одного проксі, через який потрібно направити трафік. На відміну від браузера, який має інтуїтивно зрозумілий інтерфейс, Tor Expert Bundle являє собою консольну утиліту з налаштуваннями у текстовому файлі, що є інколи не дуже зручно для кінцевого користувача.

Раніше розроблялась утиліта для зручної конфігурації з інтерфейсом – Vidalia, проте її розробка була припинена ще у 2012 році [11].

Постановка завдання

Зараз не існує жодного доданка з інтерфейсом для зручного налаштування віртуального проксі-сервера Tor. Тому, завданням статті постала розробка програмного продукту для зручної роботи та налаштування локального проксі Tor з інтеграцією у середовище робочого столу.

Виклад основного матеріалу

Анонімність в мережі залежить від багатьох факторів, одним із яких є вибір операційної системи. Зараз найпопулярнішою ОС для настільних комп'ютерів є Windows, але вона не є еталоном безпечності. Навпаки, починаючи з 2014 року компанія Microsoft збирає дані майже про все, що є у користувача на комп'ютері [8]. Через цю політику конфіденційності багато користувачів почало замислюватись над альтернативними ОС. Одною з найбезпечніших являє собою GNU/Linux.

Дистрибутив Linux – загальне визначення операційних систем, що використовують ядро Linux, готових для кінцевого встановлення на призначене для користувача обладнання [2].

За даними distrowatch.com найпопулярнішим дистрибутивом на грудень 2017 року є Linux Mint. Через те, що Linux є відкритою ОС, для нього існують різноманітні середовища робочого столу (desktop environments або DE), що відповідають за інтерфейс. Linux Mint поставляється з трьох DE на вибір: Cinnamon, Mate та XFCE. Cinnamon є розробкою самих дистриб'юторів і має дуже гнучкий інтерфейс з можливістю зручного написання аплетів, тому саме він був обраний як кінцеве середовище.

У розробці саме аплета є багато *переваг*. Виділимо інтеграцію інтерфейса користувача з системою та легкість у написанні. З *недоліків* відзначимо – вузький спектр застосування такого програмного забезпечення.

Наші орієнтири були направлені на використання програмного забезпечення у безпечній системі, яка сама по собі не збирає дані о користувачах. В якості такої було обрано один з самих популярних дистрибутивів Linux Mint та DE їхньої розробки – Cinnamon.

Проведемо опис пропонованого програмного продукту.

Програмний продукт «Tor Button» є аплетом для середовища робочого столу Cinnamon, написаний на мові програмування JavaScript з використанням API для взаємодії з середовищем.

Призначенням «Tor Button» є зручний запуск та налагодження віртуального проксі-сервера для Tor, що дозволяє пропускати будь-який трафік через нього.

Програмний продукт має забезпечувати

– зручний доступ для запуску проксі;

– можливість вибору шляху до самого сервера та файлу конфігурації;

– можливість запуску сервера від імені користувача мережі Tor;

– можливість швидкої перебудови мережевого ланцюга.

У програмного продукта «Tor Button» є своя сторінка на офіційному сайті аплетів для Cinnamon [4] (див. рис. 1). Також в самій DE є функціонал встановлення аплетів з Інтернету, тому якщо аплет є в офіційному каталозі, то його можна завантажити безпосередньо в системі.

Практичність аплету забезпечується завдяки простому та ергономічному інтерфейсу, зрозумілому користувачеві з першого погляду. Відкритий сирцевий код та доступ до сторінки на GitHub надає можливість кожному розширити функціонал або додати переклад на рідну мову. Вже зараз аплет переведений ентузіастами на датську, російську, турецьку та китайську мови.

Для *реалізації* інтерфейсу аплету був використаний Cinnamon API для роботи інтерфейсу аплета та бібліотека Glib на мові JavaScript.

В файлі `metadata.json` знаходиться інформація, яка потрібна Cinnamon API для ідентифікації аплету:

```
{
   "description" :
   "Applet for Tor network management",
   "version" : 1.2,
   "uuid" : "tor-button@shatur",
   "name" : "Tor Button"
}
```

Для додавання меню налаштувань для аплету потрібно створити файл `settings-schema.json` і додати потрібні пункти меню згідно з документацією. Кожний елемент має ідентифікатор і поля, залежно від його типу [5]:

```
"torPath" : {
   "type" : "entry",
   "default" : "/usr/bin/tor",
   "description" : "Tor location path",
   "tooltip" :
   "Specify the command to launch Tor.",
   "indent" : true
},
```

Також кожен аплет повинен містити в собі логіку для роботи. Для цього служить файл `applet.js`. В ньому обов'язково повинна бути основна функція main, яка викликається при звертанні до коду аплета. В ній описано створення об'єкта типу «аплет», який вона повертає (лістінг 1).

Для кожного елементу меню, описаному в `settings-schema.json`, створюється змінна, до якої стає можливим доступ з коду, та пов'язуються пункти меню в залежними функціями (лістінг 2).

Далі в коді створюються функції. Деякі з них викликаються при певних подіях, наприклад натискання на аплеті. При виконанні цієї події Tor Button показує меню взаємодії (лістінг 3).

Деякі з функцій виконуються при натисканні на відповідний пункт меню. Наприклад, в прототипі до пункту меню «Мережа Tor» прив'язана функція `launch_tor`, яка запускає локальний проксі-сервер. Якщо Tor не запущений, то функція ініціалізує завершення процесу через стандартну утиліту `kill` для операційних систем сімейства UNIX через сигнал SIGTERM, який ця команда передає за замовченням. Також в аплеті реалізована функція перебудови ланцюга серверів шляхом посилання сигналу SIGHUP через утиліту `kill` в функцію `rebuild_chain` (лістінг 4).

Для можливості перекладу аплету на інші мови був використаний `gettext`. Задля його підтримки в коді була реалізована функція `_(str)` (лістінг 5).

Лістінг 1

```
function main(metadata, orientation, panelHeight, instance_id) {
    let myApplet = new MyApplet(metadata, orientation, panelHeight, instance_id);
    return myApplet;
}
```

Лістінг 2

```
MyApplet.prototype = {
    __proto__: Applet.TextIconApplet.prototype, // Now TextIcon Applet
    _init: function (metadata, orientation, panelHeight, instance_id) {
        Applet.TextIconApplet.prototype._init.call(this, orientation,
                                                   panelHeight, instance_id);
        // Part of l10n support;
        Gettext.bindtextdomain(UUID, GLib.get_home_dir() + "/.local/share/locale");
```

Лістінг 3

```
on_applet_clicked: function() {
    this.menu.toggle(); // Show popup menu
},
```

Лістінг 4

```
rebuild_chain: function() {
    if (this.pid != null) { // Check if Tor is running
        let command = "kill -1 " + this.pid; // Command to rebuild chain
        if (this.runAsRoot == true)  command = "pkexec " + command;
        // If "run as root" enabled in applet settings add to aforementioned command
        // "pkexec " to run as root
            GLib.spawn_async(null, this.parse_command(command), null, FLAGS, null);
            // Rebuild Tor chain
    }
    else GLib.spawn_command_line_async('notify-send "' + _('Error') + '" "' +
                            _('Tor is not running.') + '" --icon=error'); // Show error
}
```

Лістінг 5

```
function _(str) {
    let customTrans = Gettext.dgettext(UUID, str);
    if (customTrans !== str && customTrans !== "")
        return customTrans;
    return Gettext.gettext(str);
}
```

Для створення перекладу шаблон було згенеровано автоматично, завдяки стандартній утиліті `cinnamon-spices-makepot`. За цим шаблоном, який знаходиться у папці po аплету і має розширення `.pot`, можна створити свій переклад, використовуючи програми для автоматизації перекладу `gettext` або вручну через блокнот і зберегти у файл з розширенням `.po`.

Розглянемо інтерфейс програми. Для роботи аплету потрібен сам Tor. Для його установки слід встановити пакет tor. Наприклад, для Linux Mint потрібно відкрити термінал та набрати `sudo apt get install tor`. Також можна використовувати проксі-сервер, який поставляється з браузером Tor [16].

Далі потрібно встановити аплет в систему. Для цього можна скористатися офіційним сайтом [4] або встановити через меню аплетів системи (рис. 1).

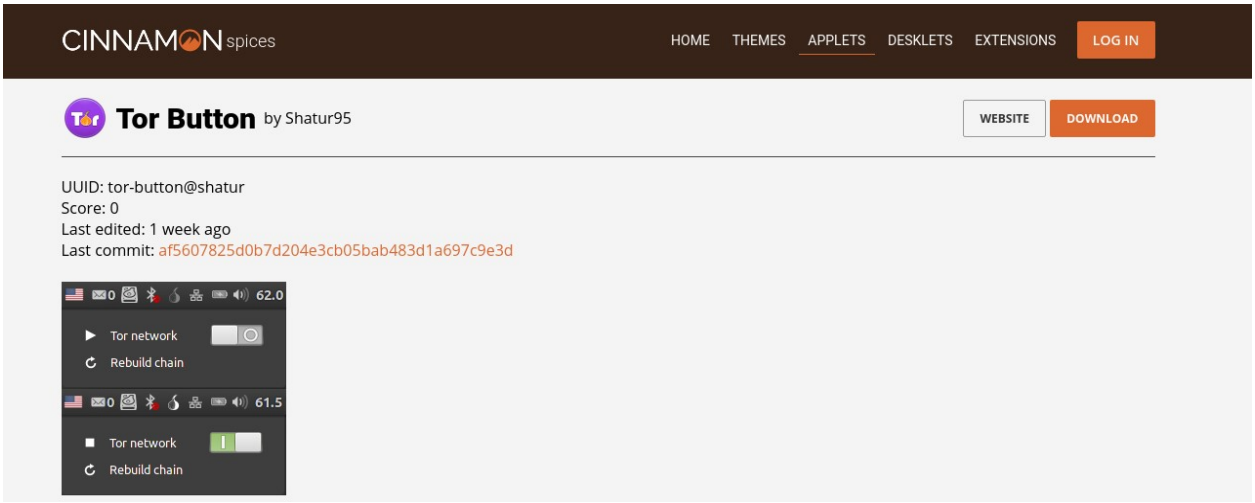

Рис. 1. Офіційна сторінка Tor Button на Cinnamon Spices

Після установки аплета в систему потрібно додати його на будь-яку панель. Аплет має простий та зрозумілий користувачу інтерфейс. Далі для запуску серверу потрібно просто нажати на аплет та обрати мережу Tor. Також в цьому меню доступна функція «Перебудувати ланцюг», що дозволяє змінити вихідний IP-адрес (рис. 2).

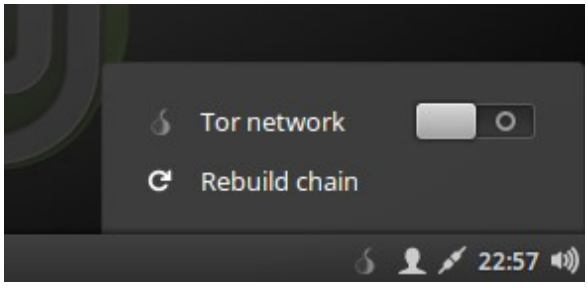

Рис. 2. Меню аплету Tor Button

Також як і всі аплети в Cinnamon він має власне меню налаштування при натисканні на ньому правою кнопкою миші.

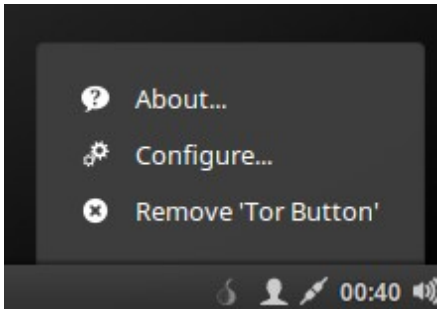

Рис. 3. Меню налаштувань аплету в Cinnamon

В меню «Про аплет» можна знайти інформацію про аплет та авторство, а меню «Налаштування» пропонує налагодження, пов'язані з Tor. В них можна знайти вимкнення повідомлень, вказівку шляху до проксі-серверу та файлу з налагодженнями, а також можливість запускати Tor від користувача tor (потрібно, якщо проксі сервер встановлювався як пакет).

ISSN 2520-2820 (online)
ISSN 2524-0978 (print)

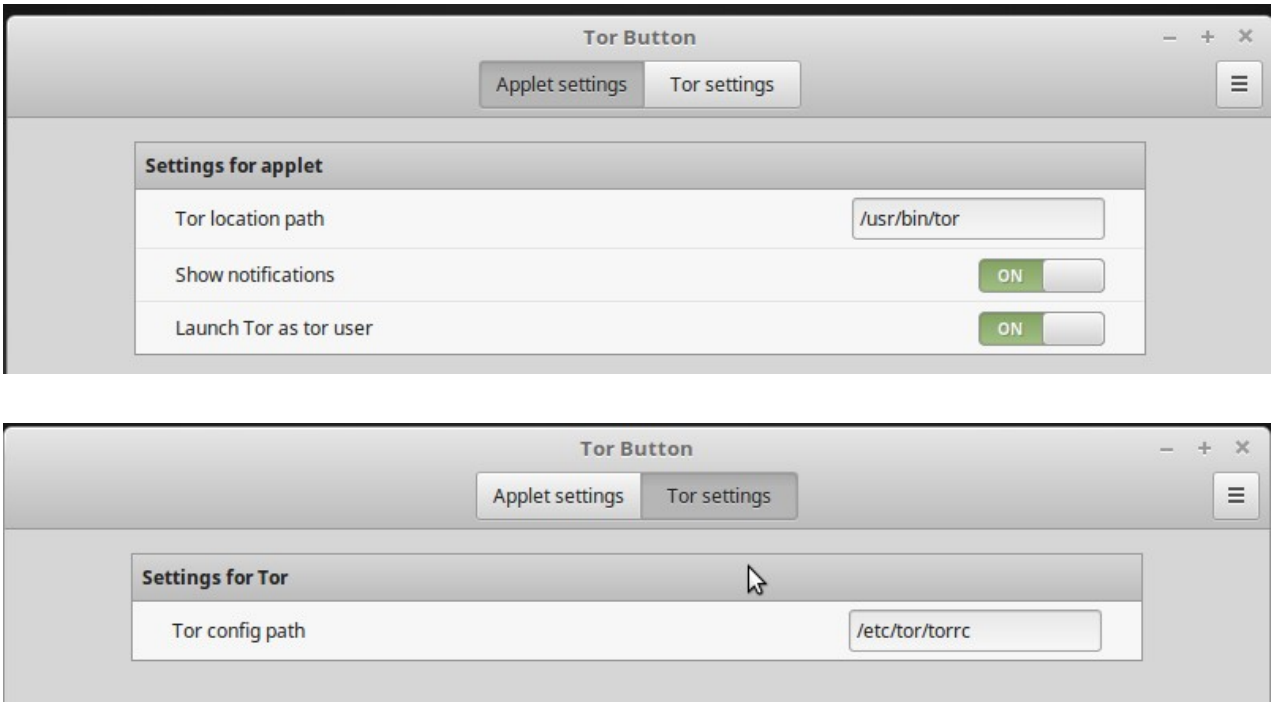

Рис. 4. Налаштування Tor Button

Після запуску локального серверу він стає доступним за адресою 127.0.0.1 через порт 9050.

Висновки і перспективи досліджень

Таким чином, проведений аналіз засобів анонімізації трафіку, такі як VPN, проксі-сервер, I2P, SSH-тунель, виділений сервер дозволив обрати мережу Tor як найбільш універсальний та гнучкий метод. Зроблено висновок, що зараз відсутні зручні методи налаштування віртуального локального проксі для анонімізації трафіку доданків через мережу Tor.

Розроблено аплет «Tor Button» для середовища робочого столу Cinnamon, написаний на мові програмування JavaScript з використанням API для взаємодії з середовищем. Призначенням «Tor Button» є зручний запуск та налагодження віртуального проксі-сервера для Tor, що дозволяє пропускати будь-який трафік через нього. Пропонований програмний продукт забезпечує: зручний доступ для запуску проксі-сервера; можливість вибору шляху до самого сервера та файлу конфігурації; можливість запускати сервер від користувача мережі Tor; можливість швидкої перебудови мережевого ланцюга.

Програмний продукт «Tor Button» розташовано на офіційному сайті аплетів для Cinnamon (https://cinnamon-spices.linuxmint.com/applets/view/298) під іменем автора. Практичність аплету забезпечується завдяки простому та ергономічному інтерфейсу, зрозумілому користувачеві з першого погляду. Відкритий сирцевий код та доступ до сторінки на GitHub (https://github.com/linuxmint/cinnamon-spices-applets/tree/master/tor-button@shatur) надає можливість кожному користувачу розширити функціонал або додати переклад на рідну мову. Вже зараз аплет переведений на датську, російську, турецьку та китайську мови.

Перспективність роботи полягає в інтеграції з системою, безкоштовності, доступності та відкритості коду розробленого ПЗ, що надає можливість для вдосконалення продукту та використання одержаних наробок в інших проектах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Буров, К. Создатель браузера Tor о его пользе [Електронний ресурс]. – Режим доступу: https://torify.me/blog/the-creator-of-the-tor-browser-about-its-benefits.html
2. Дистрибутив Linux / Wikipedia [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Дистрибутив_Linux
3. Best Proxies / База знаний о прокси [Електронний ресурс]. – Режим доступу: https://best-proxies.ru/kb/
4. Cinnamon Spices / Tor Button [Електронний ресурс]. – Режим доступу: https://cinnamon-spices.linuxmint.com/applets/view/298
5. GitHub / cinnamon-spices-applets [Електронний ресурс]. – Режим доступу: https://github.com/linuxmint/cinnamon-spices-applets
6. I2P Annonymous Network [Електронний ресурс]. – Режим доступу: https://geti2p.net/
7. Lavigne, D. VPNs and IPSec Demystified [Електронний ресурс]. – Режим доступу: http://www.onlamp.com/pub/a/bsd/2002/12/12/FreeBSD_Basics.html
8. Privacy Statements / Офіційний сайт Microsoft [Електронний ресурс]. – Режим доступу: https://privacy.microsoft.com/ru-RU/preview-privacy-statement
9. SSH туннелирование / Викиучебник [Електронний ресурс]. – Режим доступу: https://ru.wikibooks.org/wiki/SSH_туннелирование
10. Tor Project | Privacy Online [Електронний ресурс]. – Режим доступу: https://www.torproject.org
11. Vidalia (software) / Wikipedia [Електронний ресурс]. – Режим доступу: https://en.wikipedia.org/wiki/Vidalia_(software)
12. Wikipedia / Выделенный сервер [Електронний ресурс]. – Режим доступу: https://best-proxies.ru/kb/
13. Wikipedia / Прокси-сервер [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Выделенный_сервер

Hanna POHROMSKA, Hennadi CHERNYSHCHUK
Mykolayiv

DEVELOPMENT AN APPLET TO ANONYMIZE TRAFFIC USING THE TOR NETWORK

The article analyzes anonymization methods of traffic (VPN, proxy server, I2P, SSH-tunnel, dedicated server) and outlines their advantages and disadvantages. Tor was chosen as the most versatile and flexible method. Now there is no application with the interface for convenient configuration of the virtual proxy server Tor. The purpose of the work was to develop software for convenient operation and configuration of the local Tor proxies through the desktop environment.

The «Tor Button» software is an applet for the Cinnamon desktop environment, written in the JavaScript programming language using the API for interacting with the environment. The goal of «Tor Button» is to conveniently launch and configure the Tor virtual proxy, which allows you to pass any traffic through it. The offered software product provides: convenient access to launching a proxy server; the ability to choose the path to the server and the configuration file; the ability to start the server on behalf of the user of the network; the ability to quickly rebuild the network chain.The software product «Tor Button» was posted on the official website of applets for Cinnamon (https://cinnamon-spices.linuxmint.com/applets/view/298) under the author's name.

The practicality of the applet is provided by a simple and ergonomic interface. Open source and access to the page on GitHub provides an opportunity for each user to expand the functionality or add a translation into their native language. The applet already is translated into Danish, Russian, Turkish and Chinese.

Keywords*: Tor, applet, network, proxy server, interface, browser, Cinnamon, GitHub.*

Анна ПОГРОМСКАЯ, Геннадий ЧЕРНЫЩУК
Николаев

РЕАЛИЗАЦИЯ АППЛЕТА ДЛЯ АНОНИМИЗАЦИИ ТРАФИКА С ПОМОЩЬЮ СЕТИ TOR

В статье проведен анализ средств анонимизации трафика (VPN, прокси-сервер, I2P, SSH-туннел,, выделенный сервер) и выделены их преимущества и недостатки. Была выбрана сеть Tor как наиболее универсальный и гибкий метод. Сейчас не существует ни одного приложения с интерфейсом для удобной настройки виртуального прокси-сервера Tor. Целью работы стала разработка программного обеспечения для удобной работы и настройки локального прокси Tor через окружение рабочего стола.

Программный продукт «Tor Button» является апплетом для окружения рабочего стола Cinnamon, написанный на языке программирования JavaScript с использованием API для взаимодействия со средой. Целью «Tor Button» является удобный запуск и настройка виртуального прокси-сервера Tor, что позволяет пропускать через него любой трафик. Предлагаемый программный продукт обеспечивает: удобный доступ запуска прокси-сервера; возможность выбора пути к самому серверу и файлу конфигурации; возможность запуска сервера от имени пользователя сети Tor; возможность быстрой перестройки сетевой цепочки. Программный продукт «Tor Button» размещен на официальном сайте апплетов для Cinnamon (https://cinnamon-spices.linuxmint.com/applets/view/298) под именем автора.

Практичность апплета обеспечивается благодаря простому и эргономичному интерфейсу. Открытый исходный код и доступ к странице на GitHub предоставляет возможность каждому пользователю расширить функционал или добавить перевод на родной язык. Уже сейчас апплет переведен на датский, русский, турецкий и китайский языки.

***Ключевые слова**: Tor, апплет, сеть, прокси-сервер, интерфейс, браузер, Cinnamon, GitHub.*
Стаття надійшла до редколегії 14.03.2018