Справа в тому, що кожна соцмережа є безцінним джерелом інформації для зловмисників, які збирають персональні дані, які вони потім використовують для обману і шахрайства. Тому дуже важливо правильно налаштувати конфіденційність профілю користувача будь-яких соцмережах.

7. Захищеність електронної Пошти. Як правило в електронній поштовій скриньці зберігаються "ключі" від більшості облікових записів користувача, так як процедура відновлення пароля найчастіше здійснюється саме за допомогою email-повідомлень. Тому життєво необхідно захистити свою основну поштову скриньку, до якої прив'язані інтернет-банк і найважливіші мережеві сервіси. Якщо користувач бажає зареєструватися на сайті знайомств або в якомусь сумнівному сервісі, краще створити запасну поштову скриньку.

В статті 24 Закону України "Про захист персональних даних" вказано що "Власники, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкової втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних" [3]. Тобто, по-перше, користувачі самі несуть відповідальність за збереження їх персональних даних.

Отже, якщо користувач будете дотримуватись вказаних вимог тоді його персональні дані будуть більш захищеними.

Список використаних джерел:

1. Безпека в Інтернеті, що потрібно знати. URL: https://pon.org.ua/novyny/5427-bezpeka-v-nternet-scho-potrbno-znati.html
2. 5 шляхів захисту особистих даних в Інтернеті. URL: https://beetroot.academy/blog/general/5-shlyahiv-zahistu-osobistih-danih-v-interneti
3. Законодавство України. Закон України "Про захист персональних даних". URL: https://zakon.rada.gov.ua/laws/show/en/2297-17#Text

Науковий керівник: доцент Задерейко О.В.

АНАЛІЗ АКТИВНОСТІ КОРИСТУВАЧА ЗА ПРОФІЛЕМ БРАУЗЕРА CHROME

Малюта В. В.

студент 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Років 20 тому, коли Інтернет з долі обраних почав стрімко перетворюватися в масове явище, перед тисячами новоспечених користувачів виникло питання: яку пошукову систему використовувати?

Тепер ми користуємося улюбленої пошуковою системою швидше в силу звички, не замислюючись про те, що від вибору пошуковика залежить комфорт користувача, його конфіденційність і якість пошукової видачі.

Веббраузер доставить вас в будь-яке місце в Інтернеті, дозволяючи переглядати текст, зображення і відео з будь-якої точки світу. Інтернет – це величезний і потужний інструмент. Протягом декількох десятиліть Інтернет змінив те, як ми працюємо, як ми граємо і як ми взаємодіємо один з одним.

Залежно від того, як він використовується, він пов'язує нації, стимулює торгівлю, розвиває відносини, стимулює інноваційний двигун майбутнього.

Важливо, щоб у всіх був доступ до мережі, але також важливо, щоб ми всі розуміли, які інструменти ми використовуємо для доступу до неї. Ми використовуємо веббраузери, такі як Mozilla Firefox, Google Chrome, Microsoft Edge і Apple Safari, кожен день, але чи розуміємо ми, що це таке і як вони працюють? За короткий проміжок часу ми перестали дивуватися здатності відправляти електронні листи кому-небудь по всьому світу і змінили наше уявлення про інформацію. Питання в тому, який браузер або додаток може допомогти вам швидше отримати інформацію.

Останнім часом користувачі все частіше почали звертати увагу на те, які саме дані про них збирають у застосунках та на вебсайтах. Саме тому великі корпорації намагаються робити систему збору інформації більш прозорою для звичайних користувачів. Зокрема, компанія Google впровадила нову функцію, завдяки якій за декілька простих кроків можна налаштувати конфіденційність власних даних [1].

Користуючись Інтернетом, ви напевно багато разів помічали такі «збіги»: зайдете на сайт автосалону, а потім вам всюди показують рекламу машин. Або після відвідування сайту для батьків вас починає переслідувати реклама підгузків і дитячих сумішей.

Все це можливо тому, що найбільші рекламні мережі і безліч інших інтернет-сервісів по збору інформації («брокери даних») намагаються скласти максимально повний портрет кожного інтернет-користувача на основі всіляких – і часто відкритих – даних. Зазвичай це у них виходить. В інтернеті за вами може стежити хто завгодно – як законними способами, так і з порушенням прав на захист особистої інформації. Від одних способів стеження захиститися важко, від інших – потрібно. Але навіть озброївшись усіма засобами для протидії, пам'ятайте: гарантовано уникнути інтернет-стеження можна лише якщо фізично відключилися від доступу до інтернету. Але і то не факт.

Як боротися? Користуватися новітніми версіями браузерів. Chrome, анонсував і впровадив низку функцій для боротьби зі стеженням [2].

Радикальне рішення – відключити Javascript, мову, яка використовується для збору даних; але більшість сайтів тоді відразу «зламаються». Можна спробувати «пересісти» на найпопулярніший смартфон-планшет-ноутбук у відповідному регіоні і не персоналізувати налаштування.

Список використаних джерел:

1. Steve Rura/ A fresh take on an icon/ Google Inc.
2. Julia Angwin / Sun Valley: Schmidt Didn't Want to Build Chrome Initially, He Says. *WSJ Digits Blog*.

Науковий керівник: доцент Ахмаметьєва Г.В.

ПРОТОКОЛ АВТЕНТИФІКАЦІЇ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ НАД РОЗШИРЕНИМ ПОЛЕМ $GF(2^m)$ ЕЛІПТИЧНИХ КРИВИХ

Онацький О. В.

кандидат технічних наук, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

Жарова О. В.

кандидат фізико-математичних наук, доцент кафедри вищої математики Національного університету «Одеська політехніка»

В роботі запропоновано протокол автентифікації з нульовим розголошенням (zero-knowledge) на основі математичного апарату еліптичних кривих (elliptic curves – EC) з використанням особистих даних користувача та секретних ключів абонентів. Безпека криптосистем на еліптичних кривих (elliptic curves cryptography) [1], заснована на труднощах розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої (elliptic curve discrete logarithm problem) [2]. У криптосистем на EC запропоновано використовувати криптоперетворення, що базуються на перетвореннях у групі точок еліптичних кривих над полями $GF(p)$, $GF(2^m)$, $GF(p^m)$ [1, 2].

У криптосистемах над розширеним полем $GF(2^m)$ рівняння EC має вигляд [1, 2]:

$$y^2 + xy \equiv (x^3 + ax^2 + b) \bmod (f(x), 2) \text{ – несуперсингулярна крива;}$$

$$y^2 + cy \equiv (x^3 + ax + b) \bmod (f(x), 2) \text{ – суперсингулярна крива,}$$

де x, y – точки EC, $x, y \in E(GF(2^m))$; a, b, c – коефіцієнти EC; $f(x)$ – незведений поліном над полем $GF(2)$ вигляду

$$f(x) = x^m + h_1 x^{m-1} + h_2 x^{m-2} + \ldots + h_{m-1} x^1 + h_m,$$

причому $h_i \in GF(2)$.

Визначимо над точками з $E(GF(2^m))$ операцію складання та подвоєння. Нехай відомі координати двох точок $P = (x_1, y_1)$ і $Q = (x_2, y_2)$, то сума $P + Q = (x_3, y_3)$ визначається згідно з правилами [1, 2]:

1) несуперсингулярна крива

$$x_3 \equiv (\lambda^2 + \lambda + x_1 + x_2 + a) \bmod (f(x), 2);$$

$$y_3 \equiv [\lambda(x_1 + x_3) + x_3 + y_1] \bmod (f(x), 2);$$

2) суперсингулярна крива