Це ставить під питання подальшу доцільність витрачання коштів на придбання платних програмних продуктів. В першу чергу актуальним є своєчасне оновлення і модернізація комп'ютерів, які використовуються в навчальному процесі.

3. Лабораторні роботи з деяких курсів виконуються в Ms Windows не через доконечну потребу в цій ОС, а лише тому, що лектори, які читають ці лекційні курси не подбали про пошук аналогів програм для ОС Linux або запуск потрібних їм програм у системі Wine;

Джерела:

1) Апуневич С.Є., Злобін Г.Г., Рикалюк Р.Є., Шувар Р. Використання вільного програмного забезпечення у навчанні і наукових дослідженнях у Львіському національному університеті імені Івана Франка // Матеріали міжнар. наук.-практ. конф. FOSS Lviv-2011. – Львів, 2011, с. 135.
2) Батюк А.Я., Злобін Г.Г. Використання ВПЗ для тестування апаратного забезпечення ПЕОМ в навчальному процесі факультету електроніки ЛНУ імені Івана Франка // Матеріали другої міжнар. наук.-практ. конф. FOSS Lviv-2012. – Львів, 2012. с.23
3) Бойко Я., Ванькевич Д., Злобін Г. Використання технології віртуалізації в навчальному процесі факультету електроніки ЛНУ імені Івана Франка // Матеріали другої міжнар. наук.-практ. конф. FOSS Lviv-2012. – Львів, 2012. с.24
4) Рудий М.Ф., Використання крос-платформного інструментарію розробки програмного забезпечення Qt для створення навчальних програм Матеріали другої міжнар. наук.-практ. конф. FOSS Lviv-2012. – Львів, 2012. с.101
5) Шийка Ю.А., Шувар Р.Я. Виконання завдань розподіленої обробки зображення під управлінням системи CONDOR // Матеріали другої міжнар. наук.-практ. конф. FOSS Lviv-2012. – Львів, 2012. с.114
6) Столярчук О.В., Шувар Р.Я., Продивус А.М. Виконання завдань розподіленої обробки зображення під управлінням системи CONDOR //Матеріали другої міжнар. наук.-практ. конф. FOSS Lviv-2012. – Львів, 2012. с.127

Порівняльний аналіз OPENSOURCE менеджерів паролів

Гончарова Ю.В., Паличева Г.М.

Харківський національний університет імені В.Н. Каразіна
ann.palicheva@gmail.com, euphoria.silver@gmail.com

The proposed work is the result of a comparative analysis of the two most popular password storage managers: PasswordGorilla and KeePassPasswordSafe. Attempt a comprehensive review of these products, analysis of the results of their work.

Постановка проблеми: у сучасному світі дуже гостро стоїть питання безпеки інформації. Чимало інформаційних систем містять у собі велику кількість конфіденційної інформації, яку потрібно захистити. Це можуть бути, наприклад, банківські системи, соціальні мережі, інтернет-магазини, тощо. Традиційно їх захист здійснюється у двох напрямках: технічні засоби та криптографічні. До останніх відносяться апаратні,

програмні та апаратно-програмні засоби захисту інформації від несанкціонованого доступу, що використовують криптографічні алгоритми перетворення інформації[2, С. 268].

Дана робота розглядає проблему аутентифікації користувачів, а саме програмні методи її спрощення – менеджери паролів. Зважаючи на вимоги деяких інформаційних систем щодо складності та довжини останніх, а також особливості апарату людського запам'ятовування, використання менеджерів паролів, які зберігають у захищеному вигляді персональні ключі та іншу інформацію, доступ до якої повинен бути обмеженим, є досить доречним.

Ідея менеджеру паролів з відкритим програмним кодом може здатись на перший погляд дещо абсурдною, оскільки зловмисник, знаючи внутрішній алгоритм шифрування, може значно полегшити собі процес криптоаналізу. Але база даних паролів, яка зашифрована надійним ключем, забезпечує достатню криптографічну стійкість. І тому відкриті програмні менеджери паролів мають переваги перед комерційними.

Який же менеджер паролів вибрати для користування? Яким критеріям він повинен відповідати? Ця стаття є спробою відповісти на ці питання.

Метою роботи є порівняльна характеристика двох менеджерів паролів: PasswordGorilla та KeePassPasswordSafe.

Основний матеріал дослідження. Для порівняння було обрано два найбільш розповсюджених програмних продукти, які використовують ліцензію GPU [3, 4], при чому обидві версії є користувацькими, тобто не для професіоналів. Критерії порівняння відповідають вимогам навіть найбільш обізнаних користувачів. Результати порівняння надано у таблиці 1.

Табл. 1 Порівняльна характеристика менеджерів паролів

Версія програми	PasswordGorilla 1.5.x	KeePass1.x
Ліцензія	OpenSourceSoftware (GPLv2)	OpenSourceSoftware (GPLv2)
Вартість	безкоштовно	безкоштовно
Активний розвиток	+	+
Інсталяція/Робота		
Операційні системи, що підтримуються	Windows 98, 98SE, ME, 2000, XP, 7, Linux, Mac OS X 10.5.8/Lion	Windows 98, 98SE, ME, 2000, XP, 2003, Vista, 7, Wine
Вимоги	Intel/PPC, Mac OS X ≥ 10.5.8	немає
Запуск без інсталяції	+	+
Робота з USB Stick	+	+
Повна підтримка Unicode	+	-
Робота з базою даних		
Алгоритми шифрування	Twofish	Rijndael,Twofish
Пароль Hash	SHA-256	SHA-256
Стискування	немає	немає

Внутрішній формат	XML	бінарний
Захист від атак зі словником і підбором	+	+
Ключи		
Майстер-пароль	+	+
Ключовий файл	+	+
Функції безпеки		
Захист процесів в пам'яті	+ (тільки паролів)	+ (тільки паролів)
Розширене керування засобами безпеки	+	+
Групи та Записи		
Фіксовані поля (заголовок, им'я користувача, пароль, URL, примітки)	+	+
Створення полів користувачем	-	-
Прикріплення файлів	+ (багатократно за один вхід)	+ (1 за один вхід)
Вбудовані додатки Перегляд/Правка	-	-
Зв'язок між полями різних записів	-	+
Історія входжень	+ (дата зміни поля)	+ (час створення, час останньої модифікації, час останнього доступа та час закриття програми)
Імпорт власних іконок	-	-
Примітки груп	-	-
Наявність Корзини	-	-
Пошук		
Пошук паролів записів	+	+
Групування результатів	-	-
Сортування результатів пошука	-	-
Інтеграція		
Копіювання у буфер обміну	+	+
Drag&Drop	-	+
Авто-вхід	+	+
Розширюваність та автоматизація		
Застосування плагінов	-	+

Обидва програмні продукти відповідають вимогам GNU, а саме безкоштовні та мають ліцензію OpenSourceSoftware (GPLv2). Активний розвиток – це критерій життя програми, актуальності її використання та якості як програмного забезпечення, адже програмою користуються доки

не знайдуть недоліки або кращу версію, і наявність такого дає надію, що світ ще побачить покращені версії цих продуктів.

Як видно з порівняльної таблиці, на жаль, KeePass 1.x не підтримує роботу з ОС Linux, хоча ця система є дуже поширеною та зручною, проте не можна зневажати цим програмним продуктом (оскільки більш ніж 50% користувачів ще досі використовують комерційні ОС, наприклад, MicroSoftWindows). На жаль, ця програма не повністю підтримує Unicode, що дещо ускладнює користування, проте це не є показником абсолютної невалідності.

Обидва менеджері паролів мають Portable-версії, що полегшує роботу з ними, адже не потребують інсталяції. Також KeePass 1.x та PasswordGorilla 1.5.x підтримують роботу з USB Stick, тобто файл у зашифрованому вигляді може бути збережений локально, на жорсткому диску або на USB Stick. Щоб переглянути файл, потрібно мати програму, у якій він створений, ключовий файл або/та знати майстер-пароль (треба обрати при створенні бази паролів). Майстер-пароль полегшують задачу запам’ятовування усіх паролів, що має користувач. Йому потрібно ввести лише майстер-пароль задля доступу до бази, в якій зберігаються інші паролі. Але якщо користувач забув майстер-пароль, то вже ніхто не зможе прочитати зашифрований файл, навіть метод грубої сили не допоможе.

Інший метод захисту доступу до файлу – ключовий файл. Щоб розблокувати усю бази паролів треба лише вказати на ключовий файл. Але якщо користувач організував доступ до шифрованого файлу ключовим файлом, то його втрата призводить до наслідків, що і втрата майстра-пароля, тобто, доступ до бази стає неможливим. Для більшої безпеки у KeePass 1.x можна комбінувати вищевказані методи.

Продукти використовують симетричні шифри, що є гарантом надійності. PasswordGorilla 1.5.x. використовує Twofish, що має ефективну програмну та апаратну реалізацію. KeePass 1.x використовує як Twofish , так і Rijndael. Користувачеві надається вибір алгоритму шифрування. Обидва алгоритма використовуються у банківських системах, що є підтвердженням їх надійності. Але алгоритм Twofish має складну структуру та вимагає більше часу на виконання, аніж Rijndael, до того ж Rijndael прийнятий в якості стандарту шифрування владою США [1]. Тому KeePass 1.x має переваги у швидкості шифрування. Але, оскільки шифрувати треба відносно невелику кількість даних, тому різниця у часі буде несуттєва для користувача.

Використання геш-функції зміцнює впевненість у надійному зберіганні паролів користувачів та іншої конфіденційної інформації. Майстер-пароль хешується з використанням цього алгоритму.

Особливістю KeePass 1.x є розширена історія входжень. Користувач може побачити, хто та коли відкривав програму та створював базу паролів або змінював поля. PasswordGorilla 1.5.x також надає можливість слідкуванням за змінами у базі, але цей менеджер паролів вказує лише останню дату зміни поля. Таким чином, якщо хтось проглядав базу, але не

модифікував її дані, то користувач не дізнається про це. Тобто, це є значним недоліком.

Обидва програмних продукти безпечно працюють з буфером обміну Windows. Це дає змогу мінімізувати введення інформації в авторизації. У KeePass 1.x є авто-очистка буфера обміну: менеджер паролів через зазначений час після копіювання даних у буфер обміну очищує його задля підвищення безпеки. Також усі поля, паролі та URL можна перетягнути в інші вікна за допомогою функції Drag&Drop, що також мінімізує введення даних.

Окрім відкритого програмного коду KeePass 1.x має змінну архітектуру, що реалізується у плагінах. Вони дозволяють розширити функціональність менеджера паролів. Деякі з них забезпечують методи додаткового імпорту/експорту інших форматів файлів. PasswordGorilla 1.5.x не пристосована до підключення плагінів, тому в деякому сенсі це обмежує функціональність програмного продукту.

Висновки. Розглянута порівняльна характеристика дозволяє користувачу обрати серед представлених менеджерів паролів той, що задовольняє потреби користувача. Обидві програми схожі за своєю функціональністю, але KeePass 1.x все ж має більш розширений набір функцій, який задовольнить вибагливого користувача. Але даний порівняльний аналіз не є остаточнім, бо обидві програми відповідають критерію активного розвитку – з’являються нові версії з покращеним набором функцій. Тому є сенс розглядати порівняльну характеристику після виходу кожної нової версії зазначених менеджерів паролів.

Подальшим розвитком пропонованої роботи є розширення кількості менеджерів паролів та критеріїв у порівняльній характеристиці задля більш детального аналізу.

Джерела:

1) Nechvatal J., Barker E., Bassham L., Burr W., Dworkin M., Foti J., Roback E. «Report on the Development of the Advanced Encryption Standard (AES)» — National Institute of Standards and Technology.
2) Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Монографія. Харків, ХНУРЕ, Форт, 2012 р., 1 та 2 видання, 878 с.
3) Password Gorilla – a cross-platform password manager - https://github.com/zdia/gorilla/wiki
Вікіпедія. Вільна енциклопедія. KeePass. http://ru.wikipedia.org/wiki/KeePass