УДК 004.35

В.Б. Дудикевич[1], Б.Д. Будз[1], М.А. Каріоті[1]

[1]*Національний університет «Львівська політехніка», Львів*

ПРОТИДІЯ КЛАВІАТУРНИМ АПАРАТНИМ КЕЙЛОГЕРАМ

У даній статті детально розглянуто основні можливі канали витоку інформації з клавіатури персонального комп'ютера (ПК). Подано принципи встановлення та роботи апаратних та програмних закладок клавіатури, способи та засоби встановлення локальних та віддалених кейлогерів. Ця стаття також присвячена розробці власного апаратно-програмного засобу для протидії апаратним кейлогерам клавіатури. В роботі подано проект майбутньої апаратної реалізації на основі мікроконтролера ATtiny13V фірми Atmel, а також програмний код написаний на мові програмування Turbo Pascal.

Ключові слова: кейлогер, апаратні та програмні закладки, вірус, високочастотне випромінювання, мікроконтролер.

Актуальність

З усе більшим розвитком електронної обчислювальної техніки та її впровадженням в усі сфери економіки та і загалом життя людини постає питання забезпечення захисту інформації записаної та введеної в пам'ять цих технічних засобів. В захисті інформації персонального комп'ютера важливо забезпечити три основні критерії характерні для будь-якої інформаційно-комунікаційної системи, такі як конфіденційність, цілісність та доступність. При чому не можна оминути, та не забезпечити один з них.

Оскільки основним засобом спілкування користувача з комп'ютером та власне його операційною системою є клавіатура тому основні атаки на конфіденційність без втручання в будову комп'ютерної та операційної систем можливі лише через неї.

Ми не будемо розглядати можливість перехоплення побічних електромагнітних випромінювань клавіатури, системного блоку чи монітора оскільки така діяльність є досить складною і потребує серйозних знань з боку зловмисника, вагомих технічних навичок та відносно дорогого обладнання хоча і є досить ефективною [1].

Простішим з точки зору зловмисника є впровадження апаратних та програмних закладок – так званих кейлогерів (keyloggers). В свою чергу впровадження програмних кейлогерів потребує знань операційної системи, та специфічних особливостей роботи програмного забезпечення чи хоча б наявності доступу до працюючого комп'ютера з правом встановлення програмного забезпечення.

Якщо ж такої можливості та знань зловмисник не має, то в нього залишається єдиний, і найпростіший шлях – при отриманні фізичного доступу до комп'ютера встановити апаратну закладку, яка записуватиме всі коди натиснутих клавіш клавіатури.

Один з можливих способів протидії такому виду атак на конфіденційність і буде розглянутий у цій статті.

Аналіз існуючих технологій кейлогерів

Як уже було сказано вище кейлогери загалом поділяються на апаратні та програмні. Програмні кейлогери є програмними закладками написаними на мовах програму-

вання високого рівня і встановленими в операційній системі комп'ютера. Апаратні закладки, що встановлюються між штепселем клавіатури та портом на материнській платі називаються апаратними кейлогерами.

Апаратні кейлогери є мініатюрними апаратними закладками, які можуть встановлюватися між клавіатурою і комп'ютером або вбудовуватися в саму клавіатуру, що у випадку підміни клавіатури важко помітити. Вони реєструють всі натиснення клавіш, здійснені на клавіатурі. Процес реєстрації абсолютно непомітний як для кінцевого користувача так і для комп'ютерної системи. Апаратні кейлогери не вимагають установки додаткового програмного забезпечення на комп'ютері для успішного перехоплення скан-кодів натиснутих клавіш. Коли апаратний кейлогер встановлюється не важливо, в якому стані знаходиться комп'ютер - ввімкненому чи вимкненому (комп'ютер, під управлінням деяких операційних систем може лише зависнути, що не так уже й помітно). Час його роботи не обмежений, так як він не вимагає для своєї роботи додаткового джерела живлення та власне живиться від лінії живлення клавіатури.

Обсяги внутрішньої енергонезалежної пам'яті даних пристроїв дозволяють записувати до 20 мільйонів натиснень клавіш, причому з підтримкою Unicode. Дані пристрої можуть бути виконані в будь-якому вигляді, так що навіть фахівець не в змозі іноді визначити їх наявність при проведенні інформаційного аудиту. В залежності від місця прикріплення апаратні кейлогери поділяються на зовнішні і внутрішні.

Існує також невелика кількість кейлогерів побудованих на нетипових принципах апаратної реалізації та застосування інших фізичних особливостей поширення сигналів.

Акустичні кейлогери являють собою апаратні пристрої, які спочатку записують звуки, створювані користувачем при натисненні клавіш клавіатури комп'ютера, а потім аналізують ці звуки і перетворюють їх у текстовий формат, проте такі пристрої є складними та дорогими і тому практично не застосовуються [2].

Аналіз роботи клавіатури

З точки зору розповсюдженості та передачі сигналів не варто описувати радіо клавіатури, популярні на сьогоднішній день у приватних користувачів. Більш поширені на сьогодні провідні клавіатури, і тому абсолютна більшість апаратних кейлогерів орієнтована на них.

Клавіатура – це по своїй суті матриця, на перетинах горизонталей і вертикалей якої розташовані клавіші. Але одних клавіш і провідників не достатньо, бо ще потрібно перетворити натисненні клавіші у коди призначені для передачі і якісного подальшого перетворення в електронній обчислювальній машині. Тож основну функцію в клавіатурі відіграє її «мозок» - мікроконтролер клавіатури (за типом відповідний мікроконтролеру Intel 8042). При натисканні будь якої клавіші на вхід мікроконтролера по відповідних провідниках подаються два сигнали, один з яких по лінії горизонталі а інший по вертикалі, з рівнями логічного «0». Відповідно до того, по яких лініях прийшли ці сигнали, за таблицею скан-кодів, умовно встановленою в мікроконтролері на вихідну шину видається мейк-код натиснутої клавіші. При відпусканні клавіші передається брейк-код, який, здебільшого, схожий на мейк-код та має деяку приставку (здебільшого F0). Таким чином комп'ютер знає коли натиснуто, а коли відпущено будь-яку з клавіш і може визначити чи вона затиснута та відповідно повторювати її введення. При початковому запуску комп'ютера відбувається опитування всіх складових, в тому числі і клавіатури. При цьому опитуванні клавіатура не тільки тестується а й встановлює свій стан (розкладку, Set), та інші параметри для обміну інформацією з системним блоком.

Основним же з цих, встановлених при тестуванні клавіатури параметрів, є стан (розкладка, Set) клавіатури.

За час існування електронних обчислювальних машин існувало три типові стани (розкладки, Set) [3]:

Стан 1 – оригінальна XT розстановка клавіш, підтримується лише деякими сучасними клавіатурами;

Стан 2 – розстановка за замовчуванням, для більшості сучасних клавіатур;

Стан 3 – опційна PS/2 розстановка, використовується вкрай рідко.

В кожному стані є свої, характерні скан-коди відмінні від решти станів, за чим і можна також встановити, в якому з них перебуває клавіатура.

Основним завданням кейлогера є перехоплення та запис скан-кодів надісланих з клавіатури на системний блок, та подальше їх розшифрування здійснюється за допомогою доданого програмного забезпечення.

Пропоновані заходи щодо усунення описаних вразливостей

Існує одне з можливих та оптимальне рішень – застосування процедури підміни скан-кодів, їх заміни з стандартних станів 1, 2 та 3 на інші непередбачені стани для передачі по лінії зв’язку клавіатури з системним блоком.

Для вирішення проблеми протидії апаратним кейлогерам можна застосувати пристрій для підміни скан-кодів з виходу мікроконтролера на певні скан-коди розміщені у випадковому порядку на період сесії користувача.

Такий підхід базується на створенні та застосуванні апаратного засобу основним призначенням якого і буде заміна вихідних скан-кодів мікроконтролера клавіатури на скан-коди нової нестандартної таблиці.

Апаратна частина такого технічного засобу складатиметься з мікроконтролера, в якому будуть прописані дві таблиці скан-кодів але не буде сталих зв’язків між елементами таблиць. Зв'язок між елементами таблиць встановлюватиметься шляхом фізичного перемикання ряду електричних контактів за допомогою тумблерів встановлених на клавіатурі для введення змінної складової до розташування скан-кодів у таблиці підміни. Мікроконтролер, що реалізовуватиме функцію підміни таблиці є зручним тим, що не потребує додаткового зовнішнього джерела живлення, а може використовувати лінію живлення клавіатури оскільки розрахований на такі ж самі напруги живлення та може забезпечити високу швидкодію перетворення кодів.

Також така реалізація зміни таблиці на базі мікроконтролера зручна тим, що його можна легко вбудувати в корпус клавіатури, та при можливості як масового так і дрібносерійного виробництва інтегрувати на друковану плату, де знаходиться контролер клавіатури, що не створюватиме завад нормальній роботі користувача.

Нами вже теоретично розроблено проект реалізації апаратної частини на базі мікроконтролера, проте реалізації лише одного мікроконтролера не достатньо, оскільки ми здійснили перетворення коду в нестандартну форму, непридатну для адекватного розпізнавання. Ми отримаємо набір символів та натиснутих кнопок у випадковому порядку, який не міститиме змістовної частини, оскільки всі символи будуть перемішані у таблиці.

Таким чином нам потрібно виробити методику зворотного перетворення скан-кодів за зміненою таблицею в скан-коди за таблицею використаною за замовчуванням.

Тут можливі два варіанти:

застосування мікроконтролера з зворотнім перетворенням скан-кодів підміненої таблиці на скан-коди таблиці обраної за замовчуванням;

написання програми для перехоплення підмінених скан-кодів, їх зворотне перетворення на оригінальні та видачу операційній системі.

Розглянемо обидва можливі варіанти.

У випадку виконання першого варіанту при застосуванні другого мікроконтролера потрібно його десь встановити та забезпечити доступ до нього на програмному або апаратному рівнях.

Забезпечити програмний доступ до такого мікроконтролера можливо, але це потребує значних зусиль і не є настільки необхідним.

В свою чергу забезпечити фізичний апаратний доступ простіше, але це створює певні незручності для оператора, якому тепер потрібно буде щоразу отримувати доступ до перемикачів встановлених на корпусі для переключення таблиці скан-кодів. А також такий блок може піддаватися зовнішнім шкідливим впливам або пошкодитись при застосуванні і тому подвійне застосування матиме певну недоречність та незручність у пропонованому способі.

Через це нами пропонується застосування другого підходу заснованого на програмному перетворенні скан-кодів отриманих з сполучної лінії від клавіатури та подальшої видачі вже перетворених кодів в середовище операційної системи.

Такі дії можна здійснювати кількома способами, такими як перехоплення скан-кодів на вході та подальше виведення змінених скан-кодів назад до системи. Проте цей спосіб видається нам не доцільним.

Оскільки скан-код при надходженні проходить через файли реєстру, де перетворюється в коди, придатні для сприйняття обчислювальною системою, то доцільніше здійснювати підміну змінених скан-кодів одразу в реєстрі вводячи двійкові значення параметрів заміни в вигляді записів.

Ця процедура ґрунтується на так званій функції ремапінгу клавіатури, часто використовуваній гравцями комп'ютерних ігор. Проте в випадку комп'ютерних ігор застосовуються окремі вже існуючі програмні продукти, як не здатні замінювати вхідні значення за певним законом, таблицею.

Тому нами було визначено за доцільне розробити програму здатну генерувати такий двійковий запис для внесення змін до реєстру. Цей запис генеруватиметься за визначеними користувачем величинами в випадковому порядку, відповідному генеруванню таблиць підстановки створених в мікроконтролері.

При виконанні програми від користувача буде вимагатися введення коду встановленого на клавіатурі після перезавантаження комп'ютера. Цей код застосовуватиметься для генерування таблиці підмін, яка запишеться у рядкову величину, що встановиться в створюваний програмним забезпеченням текстовий файл з розширенням *.reg, який користувачу потрібно буде активувати подвійним клацанням лівої клавіші маніпулятора миша та дозволити внесення змін до реєстру (рис. 1).

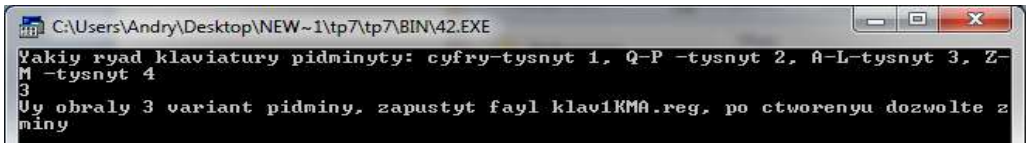

Рис. 1. Вікно створеної програми для виконання запису до змін системного реєстру.

Після цього користувач повинен перезавантажити комп'ютер та ввести код зміни таблиці скан-кодів на перемикачах клавіатури, якщо він не був встановлений раніше, та таким чином встановити однакові таблиці підміни як на клавіатурі так і в реєстрі операційної системи.

Відповідно після цього клавіатура з зміненими налаштуваннями таблиці скан-кодів «розмовлятиме спільною мовою» з операційною системою, та надіслані скан-коди будуть коректно розпізнані комп'ютерною системою.

Висновки

В цій статті описано загальні принципи роботи клавіатури та кейлогерів, запропоновано практичні методи протидії застосуванню апаратних кейлогерів, серед яких найактуальнішими є застосування комплексу програмно-апаратних засобів для генерування випадкових таблиць скан-кодів, за допомогою яких змінюватиметься дані про натиснуті на клавіатурі клавіші, які подаються по кабелю клавіатури на системний блок. Описано принципи роботи програмного забезпечення, яке може реалізовуватись на мові високого

рівня на зразок Turbo Pascal, і яке генерує двійковий запис до регістра, у встановленій формі, який підмінятиме вхідні скан-коди на істинні, за встановленим наперед законом.

Література

1. Михайло Каріоті, Богдан Будз – Електромагнітний канал витоку конфіденційної інформації. Комп'ютерні науки та інженерія : Матеріали IV Міжнародної конференції молодих вчених CSE-2010.-Львів: Видавництво Львівської політехніки, 2010. – 408с.
2. SarahYang - Researchers recover typed text using audio recording of keystrokes - www.berkeley.edu/news/media/releases/2005/09/14_key.shtml.
3. Adam Chapweske - The PS/2 Keyboard Interface - http://www.computer-engineering.org/ps2keyboard/

Надійшла до редколегії 12.11.2012 р.

Рецензент: д.т.н., проф. Петров А.С.

Дудикевич В.Б., Будз Б.Д., Каріоті М.А.
ПРОТИВОДЕЙСТВИЕ КЛАВИАТУРНЫМ АППАРАТНЫМ КЕЙЛОГЕРАМ
Рассмотрены основные возможные каналы утечки информации с клавиатуры персонального компьютера (ПК). Подано принципы установки и работы аппаратных и программных закладок клавиатуры, способы и средства установления локальных и удаленных кейлоггеров.
Ключевые слова: кейлогер, аппаратные и программные закладки, вирус, высокочастотное излучение, микроконтроллер.

Dudykevych V.B., Budz B.D., Karioti M.A.
COUNTERING THE KEYBOARD HARDWARE KEYLOGGERS
The article provides the details about the main channels of information leakage from the personal computer (PC) keyboard. Principles and installation of hardware and software keyboard shortcut, ways and means of establishing local and remote keyloggers are discussed.
Keywords: keylogger, hardware and software implementations, virus, high frequencies radiation, microcontroller.