методів оцінки пожежної небезпеки обігрівальних електричних приладів // Автореферат дисертації на здобуття наук. ступеня канд. техн. наук: спец. 21.02.08 "Пожежна безпека" / Р.І.Кравченко. – Український науково-дослідний інститут пожежної безпеки – К., 2003. – 26 с. 6. Технічний регламент з підтвердження відповідності безпеки низьконапружного обладнання. Затверджено наказом Держспоживстандарту України № 284 від 31.12.2003 – Нормативні акти України – Режим доступу: http//www.nau.kiev.ua.articles/2003/03.htm. *7. Перелік національних стандартів, які в разі добровільного застосування є доказом відповідності продукції вимогам Технічного регламенту з підтвердження відповідності безпеки низьконапружного обладнання. Затверджено наказом Держспоживстандарту України від 31.12.2006. – Нормативні акти України – // www.nau.kiev.ua. 8. ГОСТ 27924-88 (МЭК 695-2-3-84). Испытания на пожароопасность. Методы испытаний. Испытания на плохой контакт при помощи накальных элементов. – Введ. 01.01.90. – М.: Издательство стандартов, 1989. – 16 с. 9. ГОСТ 27483-87 (МЭК 695-2-1-80). Испытания на пожароопасность. Методы испытаний. Испытания нагретой проволокой. – Введ. 01.01.89. – М.: Издательство стандартов, 1988. – 8 с. 10. ГОСТ 27484-87 (МЭК 695-2-2-80). Испытания на пожароопасность. Методы испытаний. Испытания горелкой с игольчатым пламенем. – Введ. 01.01.89. – М.: Издательство стандартов, 1988. – 8 с. 11. Гудим В.І., Столярчук П.Г., Рудик Ю.І. Аналіз стану та причин виникнення пожеж електричного походження у побутовому секторі / В.І. Гудим, П.Г. Столярчук, Ю.І. Рудик – Зб. наук. пр. ЛІПБ. – Львів: СПОЛОМ, 2004. – №5. – С.116–121.*

УДК 004.35

Б.Д. Будз, В.Б. Дудикевич
Національний університет "Львівська політехніка",
кафедра захисту інформації

ТЕХНІЧНІ КАНАЛИ ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В СУЧАСНИХ КОМП'ЮТЕРНИХ КЛАВІАТУРАХ

Розглянуто основні причини виникнення та здійснено класифікацію технічних каналів витоку конфіденційної інформації у сучасних клавіатурах, що використовують протокол PS/2. Надано рекомендації для протидії виникненню розглянутих технічних каналів витоку інформації.

This paper describes the main causes of the appearance confidential information of technical channels of leakage in modern keyboards which use protocol PS/2. The paper provider recommendations on preventing the appearance of the studied technical channels of information leakage.

Актуальність. Сьогодні в державі досить інтенсивно відбувається розвиток малих і великих підприємств, між якими ведеться конкурентна боротьба. На деяких секторах ринку тісняться організації з вітчизняним й іноземним капіталом, які ставлять перед собою завдання бути лідерами ринку. Для боротьби з конкурентами, поряд із законними (менеджмент, промоції, акції), використовуються відверто злочинні (рейдерські атаки, викрадення комерційної інформації) способи боротьби. Оскільки переважна більшість конфіденційної інформації зберігається і обробляється автоматизованими системами (персональними комп'ютерами (ПК)), то, очевидно, одним з найнебезпечніших каналів витоку комерційної таємниці є технічні канали. Сприяє цьому

наявність портативного чутливого обладнання для ведення технічної розвідки, технічно грамотні спеціалісти, яким важко знайти роботу, і недостатня увага з боку керівників організації до питань захисту інформації.

Як зазначалось, більшість інформації про діяльність організації обробляється на комп'ютерах. Під час її створення, оброблення і зберігання, інформація трансформується, змінюючи форми, стани, місце розташування, що сприяє виникненню каналів витоку інформації. Як зазначається в [1], найвразливішим місцем в інформаційній технічній системі є пристрої введення інформації, оскільки вона (інформація) постає у відкритому вигляді і лише надалі може бути зашифрована для унеможливлення несанкціонованого перегляду. Найнебезпечнішим пристроєм вводу є клавіатура, оскільки відкритий текст, паролі користувачів і адміністраторів, можуть згодом бути використані як аналітична інформація і спосіб доступу до ресурсів обчислювальних засобів, тобто вразливість цих апаратних засобів знівелює захист будь-якої системи аутентифікації, яка ґрунтується на введенні паролю. На цей час багатьма дослідниками з різних країн [2–6] розглянуто і продемонстровано на технічних конференціях різні методи і підходи до перехоплення натиснень клавіш на клавіатурі, завдання яких – загострити увагу на питаннях інформаційної безпеки. Метою публікації є аналіз впливу конструктивних особливостей побудови клавіатур на виникнення технічних каналів витоку конфіденційної інформації.

Мета і задачі дослідження. Мета дослідження – проаналізувати вплив конструктивних особливостей побудови клавіатур на виникнення технічних каналів витоку конфіденційної інформації, на основі виконаного аналізу запропонувати класифікацію технічних каналів витоку і виробити рекомендації для протидії виникненню цих каналів.

Аналіз роботи інтерфейсу клавіатури. Стандартна клавіатура ПК складається з сенсорів натиснень клавіш, які об'єднані в матрицю, послідовним інтерфейсом для зв'язку з системною платою і одним із стандартних роз'ємів. Як інтерфейс можуть використовуватись як асинхронні, так і синхронні послідовні шини, такі як PS/2, RS-232, I^2C, а також шина USB. У цій роботі розглядається протокол PS/2, який використовується найчастіше.

Інтерфейс PS/2 оперує чотирма сигналами: Ground, +5V, Data і Clock. Шина PS/2 – це послідовний двонаправлений синхронний інтерфейс, де кожен біт даних Data тактується одним імпульсом сигналу Clock. Шина +5V забезпечує живлення схеми клавіатури від материнської плати, джерела сигналів Data і Clock виконані за схемою з відкритим колектором, тому в неактивному стані є рівень логічної 1. Максимальна частота тактового сигналу – не більше за 33 кГц. Пакет містить 11 бітів, де 1 – стартовий біт (завжди 0), 8 бітів даних (молодший біт перший), 1 біт кратності, 1 стоп-біт (завжди 1) [7].

Опитування матриці клавіатури здійснює внутрішній контролер, який також забезпечує внутрішню діагностику і зв'язок з системною платою по лініях Data і Clock. Внутрішній контролер клавіатури визначає факти натиснення і відпущення клавіш, навіть при натисненні декількох клавіш одночасно. Під час натиснення клавіші контролер передає її скан-код. Якщо тримати клавішу в натисненому стані, через деякий час клавіатура здійснить автоповтор передачі скан-коду цієї клавіші. Час затримки між автоповтором задається програмно, під час ініціалізації клавіатури при увімкненні ПК. Окрім задання параметрів автоповтору, контролер здійснює вибір однієї з трьох таблиць скан-кодів, управління світлодіодними індикаторами (Num Lock, Caps Lock, Scroll Lock), виконує діагностичний тест.

На програмному рівні програмування параметрів клавіатури і керування її взаємодії з ПК здійснює контролер 8042. Його вбудоване програмне забезпечення забезпечує вироблення запиту переривання для прийому скан-коду від клавіатури й оброблення керуючих команд від центрального процесора. Контролер розміщений в просторі вводу/виводу за адресом 60h.

Виконавши аналіз, можемо зробити висновок, що для функціонування клавіатури залучається ряд компонентів, які можуть створювати технічні канали витоку інформації. Зокрема це: проводові

лінії, які розташовані поруч, послідовний режим передавання даних, наявність світлодіодів, вузький спектр частот, нескладні мікросхеми обробки попередніх даних тощо.

Технічні канали витоку інформації, які виникають в результаті функціонування клавіатури. Як відомо, утворенню технічних каналів витоку інформації сприяють певні обставини та причини технічного характеру (рис. 1). Щодо клавіатур, стосовно таких причин, як недосконалість елементної бази і схемних рішень, то виробники і не приховують, що з метою економії ресурсів і скорочення часу виготовлення вони не ставлять мети виготовлення "безпечних" клавіатур для широкого загалу, хоча на замовлення урядових і військових організацій за вищу ціну вони виготовляють захищені клавіатури. Експлуатаційне зношення властиве переважно всім технічним пристроям, тим більше електротехнічним. Зловмисні дії можуть походити як від сторонніх осіб, так і з боку працівників, які мають вільний доступ до обладнання.

Згідно з [9] під технічним каналом витоку інформації слід розуміти сукупність носія інформації, середовища його поширення та засобу технічної розвідки. Вважатимемо, що носієм інформації є сигнали з шини Data і Clock, і наявні засоби технічної розвідки.

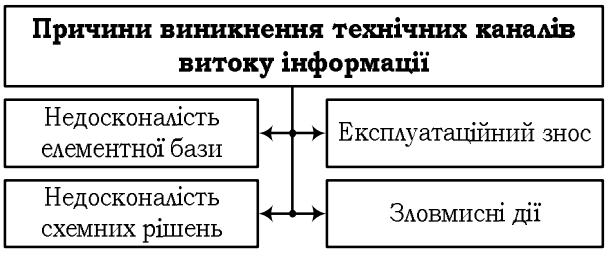

Рис. 1. Причини виникнення технічних каналів витоку інформації

Здійснивши огляд роботи інтерфейсу клавіатури, проаналізувавши публікації у відкритих джерелах [2–6] і беручи до уваги особливості технічних каналів витоку інформації [8], можна виділити щонайменше дев'ять вразливостей, які, у разі реалізації відповідних сценаріїв, можуть забезпечити успішну атаку на клавіатуру з метою забезпечення витоку інформації.

1. Оскільки параметрами роботи і процесом зчитування скан-кодів клавіатури можна керувати програмно, це дає змогу створювати програмні продукти для перехоплення значень натиснених клавіш, які отримали назву "програмні кейлогери". Для того щоб розглянути вразливі місця програмного забезпечення, узагальнимо процедуру клавіатурного введення. Отже, алгоритм проходження сигналу від натискання користувачем клавіш на клавіатурі до появи символів на екрані можна подати так. Спочатку операційна система під час старту створює в системний процес csrss.exe потік необробленого введення і системну чергу апаратного введення. Потім потік необробленого введення в циклі посилає запити читання драйверу класу клавіатури, які залишаються в стані очікування до появи подій від клавіатури. Коли користувач натискає або відпускає клавішу на клавіатурі, мікроконтролер клавіатури фіксує натискання/відпускання клавіші і посилає в центральний комп'ютер скан-код натиснутої клавіші і запит на переривання. Системний контролер клавіатури отримує скан-код, здійснює перетворення скан-коду, робить його доступним на порту вводу-виводу 60h і генерує апаратне переривання центрального процесора. Контролер переривань викликає процедуру обробки переривання IRQ 1, – ISR, зареєстровану в системі функціональним драйвером клавіатури i8042prt. Процедура ISR зчитує з внутрішньої черги контролера клавіатури дані, що з'явилися, переводить скан-коди в коди віртуальних клавіш (незалежні значення, визначені системою) і ставить у чергу виклик відкладеної процедури I8042KeyboardIsrDpc. Як тільки це стає можливим, система викликає DPC, яка, своєю чергою, викликає процедуру зворотного виклику KeyboardClassServiceCallback, зареєстровану драйвером класу клавіатури Kbdclass. Процедура KeyboardClassServiceCallback витягує зі своєї черги запит, який очікує завершення, від потоку необробленого вводу і повертає в ньому інформацію про натиснуту клавішу. Потік необробленого вводу зберігає отриману інформацію в системній черзі

апаратного введення і формує на її основі базові клавіатурні повідомлення Windows WM_KEYDOWN, WM_KEYUP, які ставляться в кінець черги віртуального введення VIQ активного потоку. Цикл обробки повідомлень потоку видаляє повідомлення з черги і передає його відповідній віконній процедурі для обробки. При цьому може бути викликана системна функція TranslateMessage, яка на основі базових клавіатурних повідомлень створює додаткові “символьні” повідомлення WM_CHAR, WM_SYSCHAR, WM_DEADCHAR і WM_SYSDEADCHAR. Практично на кожному з розглянутих кроків алгоритму обробки клавіатурного вводу є вразливі місця, тобто шпигунські програми можуть бути встановлені в будь-якому місці послідовності обробки, перехоплюючи дані про натиснуті клавіші, що передаються однією підсистемою обробки наступної підсистеми в ланцюжку обробників.

2. Апаратні кейлогери є мініатюрними пристроями, які можуть бути прикріплені між клавіатурою та комп'ютером або вбудовані в саму клавіатуру. Вони реєструють всі натиснення клавіш на клавіатурі. Процес реєстрації абсолютно невидимий для кінцевого користувача. Апаратні кейлогери не вимагають встановлення якої-небудь програми на комп'ютері, щоб успішно перехоплювати всі натиснення клавіш. Коли задіюється апаратний кейлогер, абсолютно не має значення, в якому стані перебуває комп'ютер – увімкнений він чи вимкнений. Час його роботи не обмежений, тому що він не вимагає для своєї роботи додаткового джерела живлення. Обсяги внутрішньої незалежної пам'яті даних пристроїв дають змогу записувати до 20 мільйонів натискань клавіш, причому з підтримкою Unicode.

3. З’єднувальний шнур між системним блоком і пристроєм клавіатури відіграє роль антени, що створює і електромагнітний, і паразитний канал витоку інформації. Для зчитування даних з кабелю безконтактним методом може використовуватись безконтактний сенсор. Його будова значно складніша, ніж у випадку безпосереднього під’єднання. За зовнішнім виглядом цей пристрій може виглядати як знімний фільтр перешкод, що вдягається на кабель.

4. Індикаторні світлодіоди створюють оптичний канал витоку інформації. Оскільки вони володіють інерційністю, для людського ока непомітна зміна значення інтенсивності світла. Впливати на цей параметр можуть як паразитні наведення, так і програмні методи доступу для керування процесом ввімкнення/вимкнення.

5. Аналіз акустичних сигналів, наприклад, через телефонну трубку, за даними фахівців, дає змогу відтворити від 60 до 96 % символів, оскільки кожна клавіша має унікальне звучання під час натиснення. Отже, виникає акустичний канал витоку інформації.

6. Кожне натиснення клавіші супроводжується унікальним вібраційним відбитком, що створює вібраційний канал витоку інформації. Залежно від місця розташування клавіатури, вібрація може передаватись на “випадкові антени”, і, використовуючи вібросенсори за принципом аналізу акустичних сигналів, можна реалізувати атаку, описану в 5 пункті.

7. Якщо опромінюють лазерним променем вібруючі поверхні, описані в пункті 6, виникає оптико-електронний канал витоку інформації. Тобто в межах прямої видимості джерелом інформаційного сигналу може бути не лише корпус самої клавіатура але й будь-які об’єкти, розташовані поруч, на які передається вібрація від натискань клавіш.

8. Оскільки поряд з інформаційною шиною даних Data проходить шина заземлення Ground, утворюється електричний канал витоку інформації, інформаційні сигнали проникають в лінії заземлення. Тобто зловмисник, отримавши доступ до лінії заземлення, наприклад, в сусідній кімнаті, вимірюючи паразитні струми, може відтворити сигнали скан-кодів, які передаються по лінії Data. Як зазначено в [6], цю атаку можна реалізувати на відстань до 50 метрів, і на відміну від радіоканалу, паразитний сигнал має кращі характеристики.

9. Як відомо, під час проходження струму в провіднику виникає електромагнітне поле, яке створює електромагнітний канал витоку. В клавіатурі паразитні електромагнітні хвилі можуть виникати як в проводових лініях, як зазначено в пункті 3, так і в матриці клавіатури, оскільки доріжки між клавішами відіграють роль антени.

10. І, звичайно, натиснення клавіші можна просто підгледіти, і, щоб уникнути ризику бути поміченим, використовують або відеокамеру (web-камеру), або складніші технології отримання

відбитого відображення від дзеркальних поверхонь. Відповідно виникає оптичний канал витоку інформації. На основі аналізу отриманого зображення з певною ймовірністю можна одержати відомості про положення пальців рук на клавіатурі і як аналітичний матеріал використати, наприклад, для покращання відсотка розпізнання, яке реалізується іншими методами.

Виконавши аналіз, можна навести класифікацію технічних каналів витоку інформації, які виникають при функціонуванні клавіатур, що використовують протокол PS/2 (рис. 2). Класифікації для клавіатур, що використовують інші протоколи, будуть дещо відрізнятись, оскільки в них закладені інші принципи функціонування як на програмному, так і на апаратному рівнях.

В наведену класифікацію не потрапили програмні й апаратні кейлогери, оскільки їх не можна зарахувати до технічних каналів. Відповідно до згаданого стандарту [9] апаратний кейлогер зараховуватимемо до програмної закладки, тобто потай впровадженої програми, яка створює загрозу для інформації, що міститься у комп'ютері, хоча слово “міститься” доцільніше замінити на “циркулює”. А апаратний кейлогер розуміти як закладний пристрій, тобто потай встановлюваний технічний засіб, який створює загрозу для інформації.

Рис. 2. Класифікація технічних каналів витоку інформації в клавіатурах, що використовують протокол PS/2

Висновки. Як бачимо, роль такого пристрою введення інформації, як клавіатура, в системі пристроїв аутентифікації, оброблення і зберігання конфіденційної інформації є досить важливою. Витік інформації про натиснення клавіш може спростити зловмиснику процедуру викрадення і розшифрування конфіденційної інформації, а в деяких випадках забезпечити йому доступ до всіх ресурсів для тривалого використання.

Для протидії виникненню розглянутих вище каналів варто використовувати і організаційні заходи, і технічні засоби. Організаційно можна обмежити перебування сторонніх осіб, візуальну перевірку засобів обчислювальної техніки на предмет присутності сторонніх предметів, розмежування доступу користувачів тощо. Це прийнятно для невеликих підприємств і організацій, крім того, деколи саме такі заходи можуть бути найефективнішими. Щодо технічних заходів, то потрібно використовувати всі відомі заходи для протидій витоку інформації по наведених технічних каналах. Зокрема це: повне екранування клавіатури і його інтерфейсів; екранування приміщення, в якому розташовані засоби обчислювальної техніки; використання генераторів електромагнітного шуму (ліквідація паразитного й електромагнітного каналу); використання жалюзі чи штор (ліквідація оптичного й оптико-електронного каналу); використання гальванічної розв’язки за допомогою мережевих фільтрів (ліквідація електричного каналу); використання віброгенераторів (ліквідація вібраційного каналу). Також одним із методів боротьби з технічними каналами витоку від клавіатури є введення “критичних” даних за допомогою екранної клавіатури, який спеціалісти із захисту інформації рекомендують використовувати для введення паролів.

1. NATIONAL SECURITY AGENCY. TEMPEST: A Signal Problem, 2007. 2. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards (M.Vuagnoux, S.Pasini). 3. Information

Leakage from Optical Emanations (J. Loughry, D.A. Umphress). 4. Keyboard Acoustic Emanations (D.Asonov, R.Agrawal). 5. ClearShot Eavesdropping on Keyboard Input from Video (Davide Balzarotti, Marco Cova, and Giovanni Vigna). 6. Side Channel Attacks Using Optical Sampling Of Mechanical Energy And Power Line Leakage (A.Barisani, D.Bianco) 7. The PS/2 Keyboard Interface. 8. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО "Издательство Машиностроение", 2009. – 508 с. 9. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97.

УДК 621.384.3

В.І. Боженко
Національний університет "Львівська політехніка",
кафедра радіоелектронних пристроїв та систем

ДОСЛІДЖЕННЯ СПОСОБІВ РІЗНИЦЕВОЇ ОБРОБКИ ЗОБРАЖЕНЬ У ТЕПЛОВІЗІЙНІЙ КАМЕРІ НА ОСНОВІ ПІРОВІДИКОНА

Розглянуто варіанти структури відеопроцесора тепловізійної камери на основі піровідикона. Показано, що аналого-цифрова обробка зображення забезпечує зменшення еквівалентної шуму різниці температур і зменшену розрядність порівняно із цифровою обробкою.

In the article structure variants of pyrovidicon-based thermovision camera video processing unit are considered. Is shown that analog-digital image processing provides decreasing of the noise equivalent temperature difference and reduced number of digits in comparison with the digital processing.

Вступ. Одним із різновидів сенсорів, що використовуються у тепловізійних камерах (ТК), є піроелектричні сенсори. Ці сенсори не потребують охолодження, що дає змогу виготовляти надійні портативні ТК, і мають таку корисну особливість, як чутливість лише до змінного інфрачервоного (ІЧ) випромінення. Ця особливість дає змогу істотно зменшити т.зв. геометричний (просторовий) шум, спричинений відмінностями чутливості елементарних приймачів структурованого сенсора чи зон суцільного сенсора порівняно із іншими різновидами сенсорів (наприклад, із мікроболометричними) [1].

Серед ТК камери на основі піроелектричних відиконів (ПЕВ) широко використовують для загальних призначень завдяки їх низькій вартості і доволі високим показникам. Однак такі ТК мають особливості функціонування, що спричинюють необхідність додаткової попередньої обробки відеосигналу [2].

По-перше, у зв'язку із необхідністю отримання змінного випромінення, ПЕВ та інші піроелектричні сенсори звичайно використовують модуляцію потоку ІЧ випромінення, яка здійснюється механічним обтюратором. Для забезпечення коректного режиму роботи модуляція повинна бути синхронізована з вертикальною розгорткою, звичайно у такий спосіб, щоб кожна фаза обтюратора відповідала одному полю розгортки. В такому режимі мішень ПЕВ поперемінно нагрівається і охолоджується, а накопичений заряд і відеосигнал мають різну полярність в полях розгортки, які відповідають відкритому та закритому станам обтюратора.