

Доповідь на тему «Захист інформації в портативному ПК»

Виконав студент групи 41-ЕК

Івашко Дмитро

„Захист заради спокою„

Саме так можна оцінити позицію користувача, що побажав убезпечити свій ноутбук на сто відсотків.

В останні роки в наше життя ввійшов термін «мобільність», а з ним змінився й ритм життя. Змінилося поняття про робочий час. Безумовно мисляча людина при рішенні якої-небудь робочої проблеми не може не обмірковувати її в неробочий час. І якщо відповідь знайдена, то в інтересах компанії забезпечити співробітникові інструмент для реалізації, перевірки або просто запису результатів. Одним з таких інструментів у сучасному світі є ноутбук. І ми вже не говоримо про випадок, коли власник малого чи великого бізнесу просто зобов'язаний завжди бути в курсі подій і мати під рукою вірного і надійного друга й помічника - мобільний комп'ютер.

Тому немає нічого дивного в тім, що продажі комп'ютерів такого типу останнім часом значно зросли. І зараз рідко можна зустріти ділову людину, яка б не була власником ноутбука. Тенденція сама по собі, звичайно, непогана, але описана ситуація створює свої проблеми. На жорсткому диску мобільного комп'ютера частенько зберігаються корпоративні документи, втрата яких може мати серйозні наслідки для компанії. Із усього наведеного вище можна зробити висновок, що у всіх розглянутих ситуаціях переносний комп'ютер є сховищем корисної інформації. Але, як це не дивно, багато користувачів згадують про це тільки тоді, коли ноутбук уже украдений, або з нього вилучили конфіденційну інформацію. За доступ до неї певна категорія громадян готова викласти чималі суми, а, як відомо, попит народжує пропозицію. Та і без того прибуткового кримінального бізнесу перепродажу

крадених ноутбуків, як просто дорогої речі, додалися крадіжки з метою одержання доступу до важливої інформації.

Відповідно до дослідження Інституту комп'ютерної безпеки США й ФБР («CSI/FBI Computer Crime and Security Survey 2005»), торік інформаційні втрати від крадіжок ноутбуків у США склали \$ 4 107 300.

Тому на цей час проблема захисту даних й обмеження доступу до інформації, що зберігається на жорсткому диску мобільного комп'ютера, постала досить серйозно.

Виробники ноутбуків швидко усвідомили наявність попиту на захищені вироби й негайно цим скористалися. Сьогодні на ринку співіснують моделі з різними вбудованими системами обмеження доступу до інформації, що в них зберігається. Крім того, існують програмні продукти, призначені для рішення цієї ж проблеми.

Умовно всі небезпеки, що загрожують ноутбуку, мають фізичну або інформаційну природу. Але вони дуже тісно взаємозалежні між собою, тому важливо використати комплексний підхід у забезпеченні безпеки, оскільки саме він забезпечує найвищий рівень збереження як власне мобільного ПК, так й інформації в ньому. Розглянемо існуючі способи й методи захисту.

Програмне забезпечення

Отже, ноутбук дійсно має потребу в захисті. Більшість користувачів використовують для цього стандартні засоби. Деякі встановлюють пароль на завантаження комп'ютера в BIOS. На жаль, застосування одного цього рішення великої користі не принесе. Досить розібрати комп'ютер і на якийсь час вийняти батарею, що живить мікросхему BIOS, щоб скасувати всі встановлені користувачем налаштування, включаючи й пароль. Однак деякі моделі ноутбуків, наприклад фірми IBM Thinkpad, в BIOS зберігають паролі доступу до жорсткого диска, тому при скиданні живлення з мікросхеми буде загублений доступ не тільки до ваших даних, а до жорсткого диска взагалі.

Ще один спосіб захисту, до якого часто вдаються користувачі, - це установка пароля на вхід в Windows. Однак сьогодні існує величезна кількість способів одержати інформацію з такого комп'ютера. Можна, наприклад, завантажитися з дискети або з компакт-диску й прямо або за допомогою спеціальної утиліти одержати вільний доступ до всіх даних. Або ще простіше: зняти жорсткий диск із ноутбука й підключити його до іншого комп'ютера. Але все ж таки не слід нехтувати цим захистом.

Іншим, набагато більш надійним способом захисту інформації в ноутбуці є різні програми, що шифрують важливі дані. Це дійсно прекрасний вихід з положення. Зловмисник, що одержав доступ до портативного комп'ютера, не зможе прочитати інформацію, не знаючи заданого власником пароля. Це таке ПЗ як StrongDisk (Росія), Secret Net 5.0 й ін.

Принцип захисту таких продуктів гранично простий: програма створює захищені диски, які надалі сприймаються операційною системою як звичайні логічні диски. Відмінність полягає в тому, що при запису на такий диск інформація відразу ж шифрується, а при читанні - дешифрується. Фактично ж захищений диск являє собою файл, що може розташовуватися в будь-якому місці й мати довільне ім'я й розширення. Щоб одержати доступ до інформації, захищений диск необхідно підключити.

При підключенні диска потрібно ввести пароль або підключити зовнішні ключі. Як зовнішній ключ може виступати електронний ключ, смарт-карта або файл-ключ. На зовнішній ключ записується код, що необхідний для дешифрування інформації на захищеному диску. Цей код генерується випадковим чином і має значну довжину, що виключає можливість швидкого його підбору.

Подібних програм дійсно дуже багато, і вони надають різний рівень безпеки, тому кожний користувач може вибрати що-небудь своє залежно від важливості вмісту жорсткого диску.

Якщо використовувати шифрування, то потрібно мати на увазі, що як ключ звичайно використовується пароль входу в систему, тому його потрібно вибрати максимально ретельно.

Однак на думку багатьох експертів система шифрування EFS, не забезпечує гідного рівня захисту, провиною всьому є широка поширеність ОС Windows, що породило масу способів злому цієї системи.

Альтернативний варіант крипто-системи, на яку варто звернути увагу - це PGP (Pretty Good Privacy), що дозволяє шифрувати окремі файли, створювати захищені розділи. До того ж вона дозволяє дуже ефективно шифрувати поштовий обмін, оскільки наявність двох асиметричних ключів (один у відправника, інший в одержувача) гарантує високу криптостійкість.

Настійно рекомендується включити всі опції безпеки в BIOS. Наприклад, варто поставити пароль на BIOS, заборонити завантаження з USB-драйву, CD-приводу або дискети.

Системи аутентифікації

Загальновідомо, що парольний захист вважається таким, що не відповідає сучасним вимогам інформаційної безпеки. І самою слабкою ланкою тут є користувач, що іноді вибирає занадто прості паролі, однакові для всіх сервісів.

Позбутися від цього недоліку дозволяють спеціальні пристрої - персональні ідентифікатори або токени. Вони представляють собою пристрої призначені для зберігання ключів шифрування, паролів й іншої конфіденційної чи секретної інформації. Для того щоб одержати доступ до всіх цим даних, користувачеві потрібно запам'ятати всього лише пін-код. Причому за його безпеку теж можна не боятися - токени захищені від підбора пароля.

Смарт-карти

По своєму зовнішньому вигляді вони нічим, не відрізняються від звичайних банківських карт. Ці пристрої мають гарні характеристики надійності. У них є власний вбудований мікропроцесор, що дозволяє реалізувати різні алгоритми захисту.

Залежно від виробника захищеність карт міняється. У маленький шматок пластику із чипом можуть вбудовуватися різні датчики призначення яких заборона функціонування мікропроцесора при спробі пошкодження пластику. Це можуть бути температурні датчики або датчики, чутливі до механічних впливів - наприклад, до зрізання пластикового впакування для прямого доступу до електроніки. Вся інформація, що зберігається в чипі, шифрується, щоб фахівцю, що знайде лазівку до вмісту мікросхеми не вдалося її прочитати, принаймні відразу. Є також захист від підбору пароля аж до знищення всіх даних, що знаходяться в чипі.

Призначені смарт-карти для зберігання особистої інформації, паролів доступу й даних для аутентифікації. Гарні вони тим, що, будучи досить компактними, мають такі якості, як довговічність і великий об'єм даних, що можуть зберігати. Для успішної аутентифікації потрібно вставити смарт-карту в зчитувальний пристрій і ввести пароль (PIN-код).

Загалом, смарт-карти - дуже серйозний бар'єр на шляху зломисника. Це зручний і недорогий засіб для захисту інформації. Однак вони мають серйозний недолік - низьку мобільність, оскільки для роботи з ними потрібен зчитувальний пристрій - рідер.

І якщо на настільні комп'ютери встановлення додаткового обладнання особливих ускладнень не викликає, то для ноутбуків це вже досить серйозна проблема. Але, у принципі, вихід є, і не один. Так, у продажі є рідер, виконаний у форм-факторі флопі-дисководу та спілкується з ноутбуком через його ж інтерфейс. А останнім часом розроблювачі ноутбуків стали вбудовувати в нові моделі пристрої для читання смарт-карт. Природно, що й самі картки йдуть у комплекті. Яскравим прикладом може служити ноутбук від компанії Acer-Travel Mate 800.

На відміну від простих USB-to-кенів, смарт-карти забезпечують значно більшу безпеку зберігання ключів і профілів користувача. Смарт-карти оптимальні для використання в інфраструктурі відкритих ключів (PKI), тому, що здійснюють зберігання ключового матеріалу й сертифікатів користувачів у самому пристрої, а секретний ключ користувача не попадає у вороже зовнішнє середовище.

Для кожного адаптера можуть бути задані списки дозволених і заборонених смарт-карт. Відповідно, при підключенні заборонених смарт-карт адаптер блокує роботу ЕОМ, а при підключенні дозволених смарт-карт - працює в нормальному режимі. Для адаптера також може бути визначений фіксований набір адміністративних смарт-карт (мастер-карт). Зміна налаштувань і конфігурація адаптера можлива тільки з використанням мастер-карти. Для того, щоб змінити фіксовані налаштування адаптера (листи доступу

користувачів, режими авторизації і т.д.), адміністратор повинен підключити до адаптера мастер-карту і ввести адміністративний пароль, який запитає програма конфігурації адаптера.

USB-токени

Що стосується USB-токенів, то найчастіше використовуються пристрої eToken Pro, розроблені й випущені компанією Aladdin Knowledge Systems. Зовні цей пристрій представляє собою звичайну флешку, але по своїм виконуваним функціям він багато в чому відповідає смарт-карті. Користуватися цими пристроями дуже зручно, оскільки немає необхідності запам'ятовувати безліч паролів і кодів доступу, вся інформація зберігається в USB-токені. Крім того на носії можуть бути цифрові підписи, сертифікати й інша інформація, яку небезпечно зберігати на жорсткому диску ноутбука.

Процес двохфакторної аутентифікації з використанням USB-токенів проходить у два етапи: користувач підключає цей невеликий пристрій в USB-порт комп'ютера й вводить PIN-код. Перевагою даного типу засобів аутентифікації є висока мобільність, тому що USB-порти є на кожній робочій станції й на будь-якому ноутбуці.

При цьому застосування окремого фізичного пристрою, що здатен забезпечити безпечне зберігання конфіденційних даних (ключів шифрування, цифрових сертифікатів тощо), дозволяє реалізувати безпечний локальний або віддалений вхід в обчислювальну мережу, шифрування файлів на ноутбуках, робочих станціях і серверах, керування правами користувача й здійснення безпечних транзакцій.

Крім того, USB-токени більше практичні, ніж смарт-карти: їх можна причіпляти замість брелока до звичайних ключів, що зводить ризик втрати до мінімуму. Недоліком же цих токенів є ціна. У середньому смарт-карта коштує у два рази дешевше USB-ключа.

ОТР-токени

У eToken NG-ОТР реалізований алгоритм одноразових паролів (One-Time Password - ОТР).

Алгоритм генерації одноразових паролів заснований на алгоритмі HMAC і використовує як вхідні значення секретний ключ і поточне значення лічильника генерацій. Секретний ключ відомий тільки даному токени еToken NG-ОТР і серверу аутентифікації.

Основний функціональний блок алгоритму HOTP спочатку обчислює значення HMAC-SHA-1, а потім виконує операцію усікання (виділення) з набутого 160-бітового значення 6-ти цифр, що є одноразовим паролем:

$$\text{HOTP}(K, N) = \text{Truncate}(\text{HMAC-SHA-1}(K, N))$$

де K =секретний ключ, N =счетчик генерацій.

Лічильник генерацій і секретний ключ генеруються еToken NG-ОТР під час реєстрації користувача в системі централізованого управління TMS і в коннекторі ОТР.

Під час занесення профілю ОТР на еToken NG параметри ОТР (лічильник генерацій і секретний ключ) генеруються в еToken NG-ОТР і зберігаються у вигляді віртуального токена в об'єкті користувача Active Directory.

Цей пароль порівнюється зі значенням, згенерованим на сервері аутентифікації, після чого виносяться рішення про надання доступу. Перевагою такого підходу є те, що користувачеві не потрібно з'єднувати токен з комп'ютером. Недоліком ОТР-токенів є обмежений час життя цих пристроїв (три-чотири роки), тому що автономність роботи припускає використання батарейки.

Програмні токени

У цьому випадку роль токена грає програмне забезпечення, що генерує одноразові паролі, застосовувані поряд зі звичайними паролями для багатфакторної аутентифікації. На підставі секретного ключа программа-токен генерує одноразовий пароль, що відображається на екрані комп'ютера або мобільного пристрою й повинен бути використаний для аутентифікації. Але оскільки токеном є програма, записана на робочій станції, мобільному комп'ютері або стільниковому телефоні, то ні про яке безпечне зберігання ключової інформації мови не йде. Таким чином, даний спосіб безпечніший в порівнянні зі звичайними паролями, але набагато слабкіший ніж застосування апаратних ідентифікаторів.

Біометричні сканери

Додатковий носій - це предмет, що може бути загублений або украдений, і із цієї причини значне поширення в сучасних ноутбуках одержали біометричні сканери. Звичайно в ролі «біометричного предмета» використовується відбиток пальця користувача, його неможливо украсти й дуже складно підробити. Система настроюється на відбиток пальця власника й при наступному доступі порівнює відскановане зображення з оригіналом, що зберігається. Використання біометричного сканера відбитка пальців дуже просто й у той же час досить надійно. Кращий пароль для входу в систему або ж спосіб шифрування інформації й придумати неможливо.

На сьогоднішній день це самий надійний метод входу в систему. Однак варто знати, що одна наявність сканера не гарантує високого ступеня безпеки вашої інформації. Для ефективного захисту даних біометрична система повинна бути інтегрована в криптосистему.

Виробники портативних ПК і тут виявилися на висоті. Звичайно, ноутбуків, оснащених біометричними сканерами, менше, ніж тих, у яких є вбудовані рідери смарт-карт. Проте, придбати таку модель не проблема - вони вільно продаються в усіх світі.

Комп'ютери зі сканерами відбитка пальця вже випустили такі відомі фірми, як Hewlett-Packard, Acer, Samsung тощо. Так, наприклад, у ноутбуках IBM лінійки ThinkPad використовується сканер відбитків пальців із системою запису Client Security Solution (відмінна риса - облікові записи відбитків пальців зберігаються в спеціальному чипі сканера). Але в більшості дешевих моделей IBM можна зустріти й більше просту систему запису Ominpass, що зберігає ці дані на жорсткому диску.

Крім відбитка пальця, є й інші біометричні системи. Так, на сьогоднішній день доступний пристрій для сканування райдужної оболонки ока, причому досить компактний. Варто зазначити, що райдужна оболонка ока має високий рівень індивідуальності, а це значить, що не можна зустріти людини з таким же малюнком. Отже, у даного способу дуже високий рівень захисту, значно вищий, ніж при скануванні відбитка пальця. Але досить висока ціна - у кілька сотень доларів - поки не дозволяє розроблювачам вбудовувати подібні сканери в ноутбуки - і без того не дешеві пристрої.

Нові розробки систем захисту

Компанії, що займаються випуском портативних комп'ютерів, не зупиняються на досягнутому. Вони активно ведуть роботи в області розробки засобів захисту інформації, що будуть вмонтовуватися в ноутбук.

Останнім часом у деяких ноутбуках використовуються TPM-модулі (Trusted Platform Module). Фактично такий модуль представляє собою спеціальну мікросхему, установлену на материнську плату ноутбука, і може зберігати паролі, цифрові сертифікати, з її допомогою можна шифрувати файли й папки. Однак існує думка, що ця система не так вже безпечна, як це підноситься, адже звертання до TPM-модуля й робота з ним здійснюються програмним шляхом.

Є в потенційних власників ноутбуків і ще одна надія на майбутнє. Мова йде про технології захисту інформації на рівні центрального процесора, які розробляють відразу кілька великих компаній (наприклад, Intel). Уже

зараз відомо, що в лінійці захищених «каменів» будуть і мобільні моделі, призначені для установки в портативні комп'ютери. Таким чином, сучасні технології цілком дозволяють використовувати ноутбуки й при цьому надійно захищати дані, розміщені на їхніх жорстких дисках.

Компанія A-Data вирішила піти на новий щабель захисту, вмонтувавши FBI USB двигун, в USB flash диск. Це дало змогу створити сканер відбитків пальця безпосередньо в пристрої USB flash. За допомогою ПЗ перевіряється ваш відбиток пальця при першому використанні та вимагаються подібні методи аутентифікації для наступного доступу до даних, що знаходяться на диску. Якщо відбитки пальця недоступні, або якщо ви хочете комусь надати ваш US B flash диск, то завжди можна використати резервну систему пароля.

Особливо цікаві спроби створення спеціалізованих не комп'ютерних технологій. Це використання так званої технології Zero-Interaction Authentication system (ZIA - система аутентифікації нульової взаємодії), розробленої американським ученим Брайаном Ноублом (Brian Noble) з Мічиганського університету.

Вся інформація на ноутбуці кодується в режимі реального часу. При цьому ключ шифрування зберігається в спеціальному пристрої, який користувач повинен мати завжди при собі. Принцип роботи захисту полягає в тому, що цей токен є мініатюрним радіопередавачем, що регулярно відправляє в ефір спеціальні сигнали. Вони вловлюються приймачем у ноутбуці й перевіряються. При цьому визначається, чи дійсно передавач, що згенерував ці сигнали, «прив'язаний» до цього комп'ютера. У випадку позитивного результату інформація декодується. Як тільки передавач відійде від ноутбука на певну відстань (визначається по потужності сигналу), відразу спрацьовує захист, що закриває дані.

Для роботи використовується кеш в 32 МБ, що дозволяє значно підвищити швидкість процесу кодування-де-кодування, що у цьому випадку займає всього п'ять-шість секунд. Таким чином, весь процес відбувається

практично непомітно для користувача й не вимагає з його боку абсолютно ніяких зусиль.

Взагалі, принцип цієї технології дуже схожий на метод роботи USB-ключів або смарт-карт. Єдина відмінність полягає в тім, що користувач урятований від необхідності постійного підключення й відключення токенів, а також введення PIN-коду. Крім того, і це важливо, зовні ноутбук виглядає абсолютно незахищеним. Так що зловмисник довідається про те, що інформація зашифрована, тільки після його крадіжки, коли зробити щонебудь уже буде неможливо.

Фірмою Wheels of Zeus («Колеса Зевса», у короткому написанні - wOz) розроблено продукт за назвою wOz Location-Based Encryption (шифрування на основі місця розташування), що готується до виходу на ринок.

Якщо характеризувати продукт коротко, то це орієнтований на корпоративний ринок мережевий додаток, в якому система визначення географічного місця розташування GPS інтегрована в бездротову мережу для участі в шифруванні конфіденційної інформації.

Підсумки :

Ідеального захисту немає, і бути не може -це прекрасно розуміють всі. Але все-таки зазначимо, що, скориставшись перерахованими вище способами, можна досягти дуже високого ступеня захищеності. Зламати можна все що завгодно, але, як відомо, ціль повинна виправдувати засоби, і злом багатьох систем безпеки реальний тільки в тому випадку, якщо інформація, що зберігається в ноутбуці, має величезну цінність. Тому користувачі повинні вибирати такий рівень захисту який би відповідав цінності інформації.