Курсова робота

Апаратні засоби захисту інформації

План

1. Вступ
2. TCG: картель безпеки

а) Контроль: без ліцензії і активації ніяк не можна

б) Принцип роботи NGSCB

в) Чи може користувач ухвалювати рішення? Intel наполягає на примусовому контролі

г) Сховище ключів: чи стане TPM для звичайного користувача «чорним ящиком»?

ґ) NGSCB для користувача: віруси – кращий аргумент.

3. DRM: тотальний контроль

 а) Без ваших даних тут не обійтися

б) Принцип роботи DRM в Microsoft Media Player 9

4. Усюдисущий чіп

а) На футбол з чистою совістю

б) Антиутопія супермаркетів

в) Принцип роботи RFID

5. Зворотній зв'язок

6. Висновок

7. Зміст

Зміст

1. Вступ……………………………………………………………………………2

2.TCG: картель безпеки…………………………………………………………..3

2.а) Контроль: без ліцензії і активації ніяк не можна…………………………..4

2.б) Принцип роботи NGSCB…………………………………………………….5

2.в) Чи може користувач ухвалювати рішення? Intel наполягає на примусовому контролі……………………………………………………………6

2.г) Сховище ключів: чи стане TPM для звичайного користувача «чорним ящиком»? ………………………………………………………………………….7

2.ґ) NGSCB для користувача: віруси – кращий аргумент……………………...8

3.DRM: тотальний контроль………………………………………………….....10

3.а) Без ваших даних тут не обійтися…………………………………………..11

3.б) Принцип роботи DRM в Microsoft Media Player 9………………………..12

4.Усюдисущий чіп……………………………………………………………….14

4.а) На футбол з чистою совістю……………………………………………….14

4.б) Антиутопія супермаркетів…………………………………………………14

4.в)Принцип роботи RFID………………………………………………………14

5.Зворотній зв'язок………………………………………………………………17

6. Висновок………………………………………………………………………20

Великий Брат, що підкрадається на м'яких лапах... В песимістичних прогнозах Оруелла і Хакслі це був образ усюдисущої держави, яка всюди переслідує своїх громадян. Через 20 років після виходу у світ романа-антиутопії Джорджа Оруелла «1984» сценарії тотального контролю і їх дійові особи виглядають інакше: глобальні промислові і торгові концерни винаходять все більш витончені способи, щоб під гаслом «безпека» контролювати своїх клієнтів, каталогізувати їх інтереси і аналізувати їх вчинки. Ніколи ще не було таких можливостей для явного або таємного стеження, як сьогодні, і це не параноя. Узяти хоча б назви нових методів контролю — вони жахливі: Next Generation Secure Computing Base (NGSCB), Digital Rights Management (DRM) або Radio Frequency Identification (RFID). Що все це значить, для кого це все придумано?

Найвідоміший серед «батьків» цих методів — Microsoft. Концерн так майстерно і непомітно вплітав інтернет-функції в свою операційну систему Windows, що користувачі навряд чи вже помічають, коли їх комп'ютери самі виходять на зв'язок з Редмондом (там розташована штаб-квартира компанії Microsoft). Але це тільки початок. Критики нових концепцій безпеки, таких як Trusted Computing («Довірчі обчислення»), бачать в них настання вирішального етапу на шляху до позбавлення користувачів ПК всякої самостійності. Звичайно, нові методи можуть дати більш високий рівень безпеки. Але все таки задамося питанням: кого обрадує думка про те, що інформація про нього і його комп'ютерній системі знаходиться в руках всемогутніх корпорацій?

**TCG: картель безпеки**

Альянс найбільших комп'ютерних фірм світу хоче за допомогою нової апаратури і нового ПО перетворити персональний комп'ютер у фортецю. Для захисту від хакерів, вірусів і піратського копіювання потрібен постійний контроль. Є лише одна проблема: хто контролюватиме контролерів?

Ви можете уявити собі абсолютно безпечний ПК? Наприклад, такий, до якого не мають доступу ні хакери, ні віруси, і вже тим більше той, який буде на корінню присікати всі спроби встановлювати дефектні драйвери. Чудово. Саме цього прагне група Trusted Computing Group (TCG). Більш того, метою TCG є розробка стандартів безпеки для ПК, ноутбуків, КПК, мобільних телефонів і будь-яких різновидів спеціальних комп'ютерів, наприклад банкоматів. В правління групи входять «кити» комп'ютерної галузі: AMD, HP, Intel, Microsoft, Sony і Sun - вони утворюють найвпливовіше коло «засновників» і платять за це задоволення порівняно скромну суму - $50 000 в рік. Одним ступенем нижче перебувають «постійні члени». Витративши трохи менше, всього $15 000 в рік, вони мають право впливати на розробку технічних специфікацій. Такий статус мають фірми ATI, Fujitsu-Siemens, Nokia, NVIDIA, Philips і Samsung. Нижче за всі перебувають «кандидати», такі фірми, як AMI, Gateway і Toshiba, які за $7500 в рік можуть випробовувати розробки групи TCG в бета-версіях своїх програм. Внески, на перший погляд, невеликі, але все таки для приватних кузень програмного забезпечення або невеликих проектів Open-Source навіть $7500 - це солідна сума. Наслідком чого є те, що вони залишаються не біля справ. Ядро концепції TCG - це чіп на материнській платі, так званий Trusted Platform Module (TPM), в побуті -«фріц-чип». Так він названий на ім'я американського сенатора Фріца, який відомий як активний прихильник кодування інформації. Цей чіп починає працювати вже при завантаженні комп'ютера, проте для здійснення всіх його функцій контролю потрібна спеціальна програмна підтримка. І ось Microsoft вже стоїть на старті з своєю Next Generation Secure Computing Base (NGSCB). Захищена комп'ютерна система наступного покоління - це звучить чудово, адже навряд чи знайдуться ті, кому можуть не подобатися безпечні з усіх боків комп'ютери. Особливо такі ПК, які працюватимуть в офісах крупних підприємств. Керівництво ж цих фірм, нарешті, здійснить свою давню мрію по створенню абсолютно «чистої» локальної мережі. Група TCG хоче створити фірмовий знак, логотип, який кожний виробник апаратури, відповідної вимогам TCG, може надрукувати на упаковці свого товару. Чи відповідає продукт цим вимогам, повинні перевіряти нейтральні установи. Вважається, що адміністратори не використовуватимуть програми і устаткування, що не мають сертифікату, виданого такою інстанцією.

🡨 Серце системи: чіп ТРМ постійно

контролює компоненти комп'ютера

**Контроль: без ліцензії і активації ніяк не можна**

|  |
| --- |
|  |

«NGSCB — єдиний технічно виправданий шлях, за допомогою якого можна гарантувати цілісність кожної системи»

Герольд Хюбнер, керівник відділу безпеки Microsoft. Німеччина

Сертифікація на рівні держави вибила б грунт з-під ніг тих критиків, які побоюються, що група TCG перетвориться на інстанцію, вирішуючу абсолютно все. Передбачається, що безпосередній сертифікації піддасться лише фріц-чіп, що є головною частиною нової системи. Працювати ця технологія буде за наступним принципом: користувач включає цей чіп (за замовчуванням він відключений), і він перевіряє в процесі завантаження, які апаратні компоненти ПК встановлені «неправильно». В чіпі наперед збережені необхідні дані про апаратуру різних виробників. За допомогою цих даних ТРМ розпізнає, чи не була змінена BIOS материнської плати. Важлива подробиця: чіп пасивний і не може блокувати залізо або програми. Він лише зберігає коди компонентів, використані в системі ключі або сертифікати безпеки. За твердженням голови відділу концерну Infineon Томаса Ростека (під його керівництвом і розробляється чіп ТРМ), користувач або адміністратор і надалі контролюватимуть всі процеси і ухвалюватимуть критичні рішення. Якщо фріц-чіп під час перевірки визначить, що якийсь компонент апаратури не сертифікований, тобто не гідний довіри, то повідомить про це користувача. Томас Ростек стверджує: якщо користувач упевнений, що компонент «чистий», він зможе продовжити роботу. Тоді ТРМ збереже конфігурацію ПК як «гідну довіри». Фріц-чіп не лише перевіряє конфігурацію системи на предмет небажаних втручань ззовні. В процесі роботи він спостерігає також за тим, чи працюють на ПК несертифіковані програми, наприклад віруси. Для цього потрібна операційна система, яка може використовувати всі «здібності» ТРМ. Тут в гру знов вступає Microsoft: NGSCB буде інтегрований в нову операційну систему Longhorn, поява якої запланована на 2006 рік. Герольд Хюбнер, один з керівників відділу безпеки Microsoft, запевняє, що в стандартній конфігурації NGSCB буде відключена. Більше того, те ж саме гарантують і партнери Microsoft.

Щоб почати роботу з системою, у якій NGSCB активна, користувач повинен реєструватися. Це можна зробити лише за допомогою клавіатури, сумісної з NGSCB, оскільки входи і виходи комп'ютера теж знаходяться під контролем. В колишніх версіях Windows всі без виключення програми і апаратура «спілкувалися» з операційною системою і мали безперешкодний доступ до оперативної пам'яті і жорсткого диска. Інакше йде справа з NGSCB. Комп'ютер розділений на дві області: незахищену, в якій все функціонує як раніше, і захищену, де вся комунікація йде через систему контролю Nexus. При установці будь-якої нової програми чіп ТРМ передає серійний номер програми і ідентифікаційний код ПК спеціальному серверу в Інтернеті. Сервер дає команду на активацію програми і зберігає в Мережі дані комп'ютера. Наслідок: тепер програма жорстко «прив'язана» до комп'ютера, і якщо вона встановлюється як піратська копія на іншому ПК, то це можна відстежити. Вірусам вхід заборонений, адже пройти процедуру активації повинна кожна програма, що працює під NGSCB.

Так працює Next generation secure computing base (NGSCB)

**Модель безпеки Microsoft для окремо взятого ПК**

**Програмне забезпечення:** операційна система Longhorn розділяє систему на дві незалежних один від одного частини: незахищену і захищену. Остання керується NGSCB. В ній можуть працювати тільки програми, сумісні з NGSCB. Ці програми не мають, як раніше, прямого доступу до оперативної пам'яті комп'ютера, але спілкуються з апаратурою виключно через NGSCB. Зв'язок захищений 2048-бітним кодуванням.

**Nexus:** серцем NGSCB є файл NexusMgr.sys. Він служить шлюзом всієї внутрішньої комунікації комп'ютера. В його задачі входить, серед іншого, роздача зарезервованих областей пам'яті окремим програмам. Якщо програмі потрібен доступ до пам'яті, вона

посилає в Nexus закодований запит. Файли-агенти передають необхідні для цього сертифікат і ключ. Nexus порівнює ключ з ТРМ 2048-бітним зразком, що зберігається в чіпі, і виділяє програмі певну область пам'яті.

**Апаратура:** на материнській платі знаходиться чіп ТРМ. Він служить сервером всіх ключів, що використовуються в системі. Навіть периферійні пристрої, миша або монітор, можуть спілкуватися з комп'ютером тільки за допомогою безпечного кодування. Чіпсет і процесор постійно переключаються між NGSCB і «нормальним» режимом. Результат: два комп'ютери в одному корпусі, де незахищена область може працювати також і зі звичними пристроями.

🡨При установці невідомих драйверів Windows XP просто «скаржиться».NGSCB буде все це блокувати

Nexus перевіряє кожний запит: чи гідний він довіри. Необхідні відомості зберігаються у фріц-чіпі — під кодом. Якщо, наприклад, Media Player просить доступ до оперативної пам'яті, Nexus перевіряє, чи і далі цей компонент від Microsoft є «чистим». Для зв'язку між Nexus і встановленими програмами служать файли-посередники, «агенти»; вони переносять ключі і сертифікати, одержані від чіпа ТРМ. На апаратному рівні чіп ТРМ спостерігає, чи гідні довіри монітор, миша, відеокарта або USB-сканер — це можливо лише для тих пристроїв, які розуміють його кодування. Якщо хтось схоче працювати на комп'ютері з NGSCB, йому знадобиться нове залізо, оскільки захисні програми ставлять нові вимоги до апаратури. Концепція Microsoft «Secure I/O» передбачає, що вся інформація від пристроїв введення або інформація від відеокарти до монітора посилається в закодованому вигляді. ТРМ є при цьому сервером ключів, ступінь криптостійкості яких неймовірно великий — 2048 біт.

**Чи може користувач ухвалювати рішення? Intel наполягає на примусовому контролі**

|  |
| --- |
|  «Користувач повинен мати повний контроль над всією інформацією»Бригіта Цюпріс, міністр юстиції Німеччини |

У користувача повинен бути вибір: чи потрібна йому система, захищена фріц-чіпом і NGSCB, або він використовуватиме Longhorn так само, як колишні версії Windows. Ясне одне: якщо програма безпеки від Microsoft залишається деактивованою, то і ТРМ не можна використовувати під Windows. В цьому пункті плани членів групи TCG Intel і Microsoft вступають в суперечність. Виробник чіпів наполягає на тому, щоб NGSCB завжди була активна. Це недивно, адже сталося б таке, Intel змогла б непогано заробити на примусовому технічному переозброєнні власників комп'ютерів. Тому Intel планує в майбутньому вбудовувати в материнські плати свій власний варіант NGSCB з назвою La Grande.

🡨 До найновішої ОС від Microsoft інтегрована система NGSCB – в стандартному стані вона відключена.

І Microsoft форсує розвиток своєї NGSCB не з любові до ближнього: імідж концерну з Редмонда страждає від нових дір, що постійно відкриваються, в захисті Windows; за допомогою NGSCB концерн міг би, нарешті, заявити про перемогу над хакерами, вірусами і небезпечними драйверами. Просто для того, щоб користувач був упевнений: його комп'ютер володіє імунітетом проти будь-яких нападів.

Керівник відділу безпеки Хюбнер характеризує архітектуру захисту як «магічний трикутник», що складається з ідентифікації користувача, чітко визначених прав доступу до вмісту і цілісності окремого комп'ютера. Остання повинна гарантувати, що в систему можуть бути встановлені тільки «чисті» драйвери. Вже зараз ОС Windows XP скаржиться, якщо ваші драйвери не перевірені в Microsoft, проте достатньо одного натиснення миші, щоб таке повідомлення зникло. Скоро буде по-інакшому. Адже окрім безпеки йдеться про улюблені всіма гроші. Це особливо важливо для виробників програмного забезпечення. Вони тріумфують, оскільки використовування піратських копій стане незабаром практично неможливим. NGSCB передбачає, що кожну програму необхідно буде активувати в Мережі за допомогою закодованих ключів — і зломщикам не залишиться жодного шансу. Для незалежних розробників програм ця форма контролю може стати справді убивчою. Щонайменше, з NGSCB їх програми працювати не зможуть. Представник Microsoft Хюбнер говорить, про те що його концерн надасть вільним програмістам безкоштовний пакет для розробки програмного забезпечення, за допомогою якого кожний зможе створювати свій софтвер заздалегідь сумісним з NGSCB. З Hewlett-Packard теж чутні примирливі тони: Дірк Кулман, представник HP, запросив в жовтні минулого року співтовариство Open-Source до участі в розвитку Trusted Computing. Про яке-небудь зниження платні за вхід в групу TCG розміром в $7500, зрозуміло, немає і мови. Вирішенням проблеми, що виникає для програм Open-Source або Freeware, міг би бути той самий поділ системи на дві частини, який NGSCB пропонує користувачу. Такі програми, як Office, працюють в захищеній області Nexus, Freeware — паралель, в незахищеній області. Дуже принадна обіцянка, щоб йому можна було довіряти, чи не так? Припустимо, що воно все-таки правдиве, і програма, розроблена за допомогою безкоштовного пакету від Microsoft, дійсно повністю сумісна з NGSCB. Але не вистачає ще одної дрібниці: вона не має сертифікату. А він знадобиться, коли сертифікований вміст захоче сертифіковане програмне забезпечення. І тоді прощай, Freeware. Тому що сертифікат, цю відпускну грамоту, програміст може одержати у урядовців з BSI тільки за гроші. При цьому в BSI ще самі не знають, як виглядатиме процедура видачі сертифікатів. За словами прес-секретаря Міхаеля Дікопфа: «Все це поки дуже туманно». Ще одна проблема: хто розпоряджатиметься ключами і сертифікатами, інформація про які міститься у фріц-чіпі? Хто дає дозвіл на активацію програми? Її виробник? Сам користувач? Або якась вища інстанція, яка спостерігає за тим, щоб жоден ключ не був використаний двічі, і тому цій інстанції, як і користувачу, повинні бути відомі всі ключі?

**Сховище ключів: чи стане ТРМ для звичного користувача «чорним ящиком»?**

Якась невідома раніше організація, комп'ютерний клуб «Хаос» (Chaos Computer Club – ССС) однозначно вимагає, щоб ключами міг розпоряджатися тільки користувач. Інакше власний комп'ютер перетвориться для нього на «чорний ящик», до якого він не має суверенного доступу. Цій думці вторить федеральний міністр юстиції Німеччини Бригіта Цюпріс: «Користувачі повинні мати повний контроль над всією інформацією, незалежно від того, закодована вона чи ні. Залежність від третіх осіб недопустима». NGSCB буде міцним горішком і для виробників апаратури. Комп'ютеру, оснащеному чіпом ТРМ і NGSCB, потрібні материнська плата і процесор, які можуть постійно переключатися між різними режимами.

🡨 Ноутбук: концерн IBM вже вбудував чіп безпеки TPM в свою модель Thinkpad X30

Приклад: до цих пір адресація пам'яті проводиться операційною системою. Такі платформи, як Linux або Windows XP, вже мають віртуальну адресацію, при якій призначені для користувача програми не знають, яка адреса пам'яті використовується зараз. Але контроль над цим все ще зберігає система, отже, її ще можна зламати. Зовсім інакше при NGSCB: тут управляти адресацією пам'яті повинні процесор і чіпсет. Коли поступає запит з безпечного сектора Nexus, процесор повинен спочатку «запитати» чіп ТРМ. Якщо доступу до пам'яті вимагає яка-небудь програма з незахищеної області, процесор, перш ніж повідомити програмі адресу пам'яті, з міркувань безпеки спочатку очистить свій кеш. Кожне рішення процесора повинне бути схвалено ТРМ. А відповідні для цього чіпсети і процесори з'являться нескоро.

**NGSCB для користувача: віруси — кращий аргумент**

Говорячи про швидке вживання ТРМ в комп'ютерах, група TCG не хоче називати точні терміни. Спочатку попит буде обмежений тільки областю бізнесу, оскільки ця техніка якнайбільше зацікавить адміністраторів комп'ютерних мереж фірм. У них є вагомі причини захищати свої комп'ютери від недозволеного доступу. Незахищена частина системи з NGSCB не має для адміністраторів ніякого сенсу. Приватним користувачам, якщо вони хочуть використовувати безкоштовні програми, навпаки, немає ніякого толку від наявності безпечної області. Від нападів вірусів вони захищатимуться, як і раніше, за допомогою програмного забезпечення. Незахищений режим надалі працюватиме в звичному середовищі зі всіма типовими для неї ризиками. Приватні користувачі дуже рідко мають справу з інформацією настільки секретною, щоб їм був потрібен безпечний Nexus — за виключенням хіба що онлайнових покупок або банківських операцій. Але для банківських операцій цілком достатня існуюча система чіп-карт HBCI. Як її заміна NGSCB була б дуже дорогою іграшкою. Продавцям контенту, навпаки, трапляється цікава нагода: з сертифікованими медіаплеєрами можна зв'язати систему контролю авторських прав (Digital Rigts Menagement) і ТРМ. Наприклад, при покупці в Мережі музики продавець запитає ключ ідентифікації, що бережеться в ТРМ вашого ПК і запише його в проданий файл. Музичний твір можна буде відтворити тільки на одному комп'ютері. Microsoft за допомогою фріц-чіпа теж може ефективно боротися з піратським копіюванням: концерн володіє декількома патентами на взаємодію операційної системи, Digital Rights Management і ТРМ. Наприклад, при установці викачаного з Інтернету оновлення Windows ваш комп'ютер відправить в Редмонд ім'я і адресу користувача.

Trusted Computing обіцяє багато чого — захист від вірусів, піратського копіювання, хакерів. Та чи варто в обмін на це віддавати картелю комп'ютерних гігантів контроль над всіма ПК в світі? Звичайно, ні, та і плани групи TCG ще дуже розпливчаті і непрозорі. Кінець кінцем користувач повинен сам розпоряджатися ключами від своєї системи. Але тоді знову встає проблема безпеки.

**DRM: тотальний контроль**

Музична індустрія стикається з безліччю труднощів при продажу цифрового контенту в Інтернеті. У разі появи піратських копій необхідно з'ясувати, хто і коли купив поширюваний на піратських дисках матеріал. Взнати це допоможе технологія Digital Rights Management.

Кармін Каріді — актор. Звичайно, не особливо відомий, але все таки один з 5803 членів жюрі премії «Оскар». 69-річний артист одного разу знявся в епосі про мафію під назвою «Шеф-2». Методи «поганих хлопців», мабуть, так сильно вплинули на нього, що Каріді вирішив порушити правила Американської кіноакадемії. Одержавши для приватного перегляду номінований на премію «Оскар» кінофільм «Чого хочеться серцю», він передав його своєму знайомому, який негайно зняв з нього копію і помістив її в Інтернеті. Каріді не повезло: фільм на його DVD був оснащений спеціальним цифровим «водяним знаком», який залишився навіть на копії, переведеній у формат DivX. Саме по цьому знаку і вдалося відшукати первинного власника розтиражованого піратами диска.

Подібні «водяні знаки» — найм'якша форма цифрового нагляду за правами. Як правило, їх записують в окремі пікселі зображення або ж в звукові частоти. «Водяний знак» може містити як все, так і лише окремі дані про покупця музичного твору. Вже сьогодні жоден розповсюджувач музики не обходиться без подібного цифрового контролю. Такі формати файлів, як Microsoft WMA або WMV, забезпечують виробників можливістю накладати ще більші обмеження: на кодування, термін придатності матеріалу, кількість його користувачів.

Проте поряд зі всіма методами DRM є один загальний момент, який їх об'єднує: будь-який клієнт розглядається як потенційний злодій. Наприклад, компанія T-Vision, онлайн-відеотека найбільшого провайдера Німеччини T-Online, продає DRM-ліцензії на проглядання відеоконтенту, дія яких закінчується через 24 години.

🡨 T-Vision, онлайнова відеотека T-Online. Всі фільми захищені за допомогою DRM

T-Online використовує для цього технологію Microsoft Windows Media Codec 9. Інтегрований в неї Windows Media Rights Management відповідає саме за те, що термін проглядання фільму закінчиться через 24 години прокату, навіть якщо фільм буде скопійований і збережений. Для прямих трансляцій в Інтернеті в Microsoft також є технологія, яка називається Live DRM. Її перевага для продавця полягає в тому, що передаваний контент не може бути одержаний ніким, окрім зареєстрованого клієнта. Недолік для користувача: можливість відтворювати одержані дані тільки за допомогою Windows Media Player 9 — про альтернативні плеєри можна відразу забути. Інший шлях, ніж обмежувальні методи DRM, вибрав Інститут інтегрованих схем Фраунхофера. Його так званий Light Weight Digital Rights Management (LWDRM) — полегшений варіант DRM — дозволяє використовувати цифровий зміст без яких-небудь обмежень, а інформація про покупця повинна перешкодити лише тому, щоб файл виставлявся на мережних біржах обміну. Отже якщо музичний портал наперед попереджає своїх користувачів, що поширювані їм файли забезпечені DRM, то намагатися виставити дані композиції на біржі обміну буде просто безглуздо.

Програмне забезпечення

**Без ваших даних тут не обійтися**

Все почалося з MS Office і Windows XP, коли Microsoft зажадала обов'язкову активацію програмного забезпечення через Інтернет. Багато виробників пішли цьому прикладу, але деякі з них пішли ще далі: вони примушують своїх покупців до реєстрації з вказівкою повного імені і домашньої адреси.

|  |  |
| --- | --- |
| **Примусова активація** **реалізована в наступних продуктах:** * Microsoft Windows XP;
* Microsoft Office XP;
* Adobe Photoshop CS;
* Cute FTP;
* Digimap для Palm;
* Tomtom Navigator для КПК.
 | **Отримання оновлень для цих програм можливе тільки після реєстрації в Інтернеті:*** Panda Antivirus Platinum;
* Антивірусний пакет G Data;
* Powerquest Partition Magic;
* Powerquest Drive Image;
* Microsoft Office XP.
 |

|  |
| --- |
|  **«**Наші клієнти повинні мати можливість необмеженого користування купленої музики»Івонн Ібс, прес-секретар Universal Music |

Декілька порталів, що пропонують музику для скачування, вже працюють з LWDRM. Наприклад, компанія Popfile. В «водяному знаку», розташованому усередині файлу МРЗ, не вказано ім'я покупця — це не дозволено законом про інформацію, — але зафіксований унікальний номер покупки. «Водяний знак» такий стійкий, що його можна прочитати навіть після того, як пісня буде скопійована на лазерний диск. За заявами самої Popfile, вони не прихильники жорсткої лінії: «Ми як фірма, що випускає диски, повинні захищати інтелектуальну власність наших композиторів. Проте ми також повинні дати можливість нашим клієнтам слухати музику де завгодно і в будь-який слушний для них час», — говорить Івонн Ібс, представник Universal. Інший приклад - - іспанська компанія Weblisten.com. Даний портал пропонує музику у форматах WMA і МРЗ. Файли МРЗ забезпечені «водяним знаком», який містить всі необхідні відомості про покупця. Файли WMA, за твердженням продавця, потрапляють до користувача без яких-небудь «водяних знаків» або DRM. Дивно, що музична індустрія Іспанії спокійно дозволяє собі те, на що в багатьох західних фірм деколи не вистачає сміливості: музичний портал з необмеженими правами на користування скачуваної музики.

🡨 Фільми, трансльовані T-Vision, можна дивитися тільки за допомогою Microsoft Media Player 9

На жаль, композиції, одержані від Weblisten, можна використовувати тільки на території Іспанії. Але деякі інтернет-торговці обходяться з правами користувачів на придбані композиції набагато більш жорстко. Наприклад, портал Musicload проводить достатньо строгу політику: файли WMA ви можете відтворювати на ПК скільки завгодно, але записувати їх на CD не більше трьох разів. Ще один приклад – відома багато чим компанія Apple, яка робить ставку саме на DRM і при цьому не є такою щедрою, як Popfile або Weblisten. Файли формату ААС, що продаються нею, можна копіювати і записувати на аудіодиски, але не більше ніж на чотирьох апаратах — це може бути як iPod, так і будь-які інші комп'ютери. Як вже було сказано, щоб виключити можливість розповсюдження незаконних копій, DRM містить дані про покупця. Крім того, він забезпечує файли спеціальним ключем, який генерується з поєднання серійного номера жорсткого диска, версії BIOS, імені процесора і ідентифікаційного коду встановленої версії Windows. Компанія Apple, здається, знайшла золоту середину в даному питанні: музичні файли просто не вийде скопіювати. При спробі відтворити файл на іншому ПК плеєр iTunes спершу перевірить, чи підходить ключ музичного файлу до встановленої апаратури. Можливості DRM цікаві не тільки для галузі розваг. Охорону прав можна використовувати і в повсякденному житті офісів. Так само, як в музичних або відеофайлах, дані DRM можуть міститися і в електронних листах. Наприклад, діловий лист буде доступним тільки певному кругу читачів і автоматично самоліквідується через 30 секунд. За часів розвитку технології DRM це не жарт, а реальність. Звичайно, власник прав повинен захищати свій товар від піратського копіювання. Незрозуміло, проте, чому будь-який інтернет-покупець наперед підозрюється в намірі зробити піратську копію, чому він може лише обмежено використовувати куплений файл, тоді як покупець лазерного диска може копіювати його скільки завгодно і на якій бажано носій.

Так діє DRM в Microsoft Media Player 9

**Digital Rights Management**

T-Vision продає своїм клієнтам фільми через Інтернет. Щоб уникнути неліцензійного копіювання відеофайли забезпечені Digital Rights Management. Як результат через 24 години фільм більше не придатний для перегляду. Такий же метод можна застосовувати при трансляції фільмів або телепередач в реальному часі.

**Продавець:** Сервер продавця знаходить файл, бажаний клієнтом, забезпечує його інформацією про DRM, терміні придатності і праві на використання, після чого кодує його. Ліцензійний ключ готовий.

**Інтернет:** Файл виставляється на вебсервері продавця для скачування або перегляду в режимі реального часу. Ключ, за допомогою якого файл може бути розшифрований, залишається на віддаленому сервері продавця.

**Користувач:** Media Player завантажує файл або відтворює його прямо з Мережі. DRM повідомляє його, де знайти відповідний ключ. Плеєр з'єднується з сервером, на якому бережуться ліцензії, і одержує необхідний для відкриття файлу ключ. Тепер файл може бути відтворений.

**сюдисущий чіп**

Технологія контролю Radio Frequency Identification (RFID) дозволяє імплантувати пристрої обробки і зберігання інформації в етикетки, одяг або навіть під шкіру, настільки малі чіпи. Але хто має доступ до відомостей, що бережуться в них?

**На футбол з чистою совістю**

«Ви не маєте права входу на стадіон», — так, вже перед вертушкою на вході, можуть раптово закінчитися відвідини матчу футбольного чемпіонату світу 2006 року в Німеччині для потенційно небезпечного фаната. В квитках на матч будуть заховані чіпи RFID. «Таким чином ми хочемо запобігти нелегальній торгівлі квитками і їх підробку», — говорить Герда Грау, прес-секретар організаційного комітету чемпіонату. Що ж, можливо, саме технологія RFID виявиться тим магічним засобом, який допоможе розв'язати вічну проблему нелегальної торгівлі квитками на публічні заходи.

Основним каналом збуту квитків буде, як планується організаторами чемпіонату, Інтернет: оплата тут проводиться за допомогою кредитної карти. Той, хто хоче купити квиток, повинен реєструватися у Федерації футболу Німеччини. Федерація не виключає, що дані покупця можуть бути негайно перевірені по спеціальній картотеці уболівальників-хуліганів. Те, що кожний уболівальник потрапляє під підозру, Герда Грау не розглядає як сценарій чергової технологічної антиутопії, що збувся.

Поки не ясно, яка саме інформація буде записана на чіпі, відомо лише, що його місткість складає сьогодні 1 кбайт. Про інфраструктуру, яка оброблятиме ці дані за кулісами стадіонів, Грау теж нічого поки сказати не може. Вміст чіпів розшифровуватиметься не на стадіонах. Заспокоюючи футбольну громадськість, Грау обіцяє: «Ми переслідуватимемо уболівальників не дуже жорстоко».

🡨 У магазині Future store в Рейнберзі товари оснащені чіпами RFID

**Антиутопія супермаркетів**

Чемпіонат світу — це все-таки справа майбутнього, хоча і не такого віддаленого, а RFID працює вже сьогодні. Торговий концерн Metro застосовує цю техніку з 2003 року в своєму супермаркеті Future Store («Магазин майбутнього») в Рейнберзі, Німеччина. Іскристі ярлики з вказівкою ціни служать в першу чергу для захисту від крадіжки: якщо чіп RFID проходить контрольну рамку, система б'є тривогу.

У випадку з квитками на чемпіонат світу 2006 відстань до прочитуючого пристрою може складати від 10 до 12 сантиметрів, проте вона може бути і більшою. Наскільки простий RFID у вживанні, настільки ж різноманітні і можливості зловживань ним. Похмурі фантазії про «прозорого» клієнта (втім, похмурими вони представляються тільки покупцю, продавці ж просто в захваті від перспективи, що розкривається перед ними) можуть стати реальністю наших днів.

Покидаючи магазин, ви везете візок мимо електронного бар'єру, який посилає імпульс ярликам ваших покупок. Чіпи повідомляють ціну в касу, сума списується з вашого рахунку автоматично. А десь за кулісами, в обчислювальному центрі, вся інформація про ваші покупки обробляється і оцінюється. Складається індивідуальний «портрет покупця», в якому разом з особистими даними враховані всі ваші купівельні звички. «Теоретично це можливо, на практиці — дуже дорого, — така думка прес-секретаря мережі супермаркетів Metro Альбрехта фон Труксеса. — Це стане повсякденною реальністю не раніше ніж через 10 або 15 років». Причини подібних песимістичних оцінок такі: чіпи RFID поки не годяться для масового вживання, оскільки банки овочевих консерв, молочні пакети і заморожені продукти по-різному відображають промінь считуючого пристрою. «Крім того, — додає Труксес, — немає змісту ставити чіп, який коштує 40 центів, на упаковку йогурту за 30 центів». Проте мене такі заяви мало заспокоюють. Насправді, чим більше виготовляється чіпів, тим дешевше вони стають. З цього року RFID використовуватиметься в транспортних упаковках і піддонах постачальників торгової мережі Metro. В супермаркеті Future Store чіпи RFID поки наклеєні лише на товари фірм Kraft, Pantene і Gillette. Фахівці по захисту інформації стежать за цим розвитком уважно. Петер Шаар, федеральний уповноважений по захисту інформації, нагадує, що відомості на ярликах RFID повинні бути закодовані, і у будь-який час повинно бути ясно, хто має доступ до цієї інформації. Крім того, для збору інформації про клієнта необхідна його згода.

Так функціонує RFID

**Хитрі ярлики на упаковці**

**Енергія і інформація за допомогою радіохвиль:** коли RFID потрапляють в зону дії считуючого пристрою, вони передають інформацію (до 64 кбайт) за допомогою радіохвиль (до 5 м). Необхідну енергію RFID одержують від електромагнітного поля считуючого пристрою. Оскільки ці чіпи здатні виходити на зв'язок без батареї, вони так і просяться на ярлики-цінники.

**1. Запит:** зчитуючий пристрій посилає електромагнітний імпульс, який активує зашитий в товарі чіп RFID.

**2. Відповідь:** чіп RFID використовує енергію цього імпульсу, щоб надіслати свою інформацію считуючому пристрою.

**3. Обробка:** зчитуючий пристрій передає одержані дані в комп'ютер. Той, у свою чергу, обробляє їх.

Петер Шаар – уповноважений по захисту інформації уряду Німеччини : «RFID містить багато ризиків відносно захисту інформації. Річ, однак, не про те, щоб перешкоджати вживанню цієї технології, просто необхідне дотримання закону про захист інформації. А це означає, що зацікавлені особи повинні повідомлятись про те, коли і для яких цілей використовується технологія RFID. Покидаючи магазин, покупці повинні мати нагоду деактивувати чіпи і видалити весь їх вміст. І, зрозуміло, повинна бути наявною гарантія (наприклад, кодування), що інформацією цих чіпів не зможуть скористатися ті, у кого немає на це законних прав».Організація захисту інформації Foe-BuD попереджає, що і карти покупця, що дають право на знижки в «Магазині майбутнього», містять чіпи RFID.

 🡨 На футбольному чемпіонаті світу 2006 чіпи RFID будуть заховані у вхідних квитках.

Пан Труксес заявляє: «За допомогою таких чіпів ми вивчаємо вік покупців DVD-дисків». Річ у тому, що в Future Store покупці можуть проглядати ролики з фільмів, що є у продажу. Згідно із заявою Труксеса, їх дані не збираються, і «портрети покупця» не складаються. На карті покупця записаний лише клієнтський номер. Чіпи RFID в Future Store містять ідентифікаційний код продукту і номер серії чіпа, даний його виробником. Спеціальний деактиватор обнуляє код продукту, коли покупець покидає магазин. Наступне покоління пристроїв зможе анулювати і номер серії. Той факт, що вміст чіпа можна змінити у будь-який час, здатний привести до найнегативніших наслідків. Адже, якщо можна «переписати» номер на чіпі, то він може бути замінений іншою інформацією, наприклад іншим ім'ям покупця. Тому доктор Франк Гілерт, керівник відділу технологій ідентифікації концерну Infineon, вважає дискусію про захист інформації необхідною.

🡨 підшкірні імплантанти з чіпами RFID доступні вже в Росії

Гіпотетичну небезпеку того, що за допомогою RFID можуть бути складені «портрети покупців», він оцінює сьогодні як незначну: «Вміст сміттєвого контейнера може дати набагато більше інформацію про звички покупця». З таким аргументуванням можна згодитися.

**Зворотній зв'язок**

Операційна система Windows XP відома не тільки своєю зручністю, надійністю і захищеністю. Окрім цього вона набула і погану славу через свої таємні операції, коли з комп'ютера користувача без його відома на сервер компанії Microsoft відправляється якась особиста інформація.

🡨 Спеціальна програма Antispy перевіряє комп’ютер на наявність програм-шпіонів

Але цінні особисті дані збираються не тільки за спиною громадян, без їх відома і згоди. Хитромудрі системи знижок і різних поблажок привертають покупців до добровільної співпраці, таким чином витягаючи з потенційних клієнтів все, що вимагається про них дізнатися.

«Здрастуйте, пан Петренко!» -вітає книжковий онлайновий магазин. Звідки ж він знає, що до нього зайшов саме пан Петренко, а не пані Сидоренко? Все просто: після того, як покупець зробив перше замовлення, інтернет-магазин зберігає на його комп'ютері cookie-файл. Коли клієнт заходить на стартову сторінку сайту наступного разу, система запрошує cookie і взнає таким чином, з ким має справу.

🡨 Того, хто хоч раз зробив замовлення в інтернет-магазині Amazon.com, при повторному відвідуванні вітатимуть по імені.

Браузер виробництва Microsoft дотепер жодним чином не перешкоджав подібній практиці, а в шосту версію Internet Explorer`а нарешті була вбудована система управління cookie-файлами, за допомогою якої їх зручно сортувати і видаляти. Але браузер передає інформацію в Мережу не тільки за допомогою cookies. В пункті меню «Додатково» користувачу пропонується включити відображення посилань на близькі до тематики сайти. З одного боку, це корисно: таким чином можна одержати більше інформації по темі, що цікавить. Але в цій можливості є і недолік: для того, щоб її включити, потрібен плагін ActiveX фірми Alexa (дочка Amazon.com). Цей плагін не тільки показує вам схожі сайти, але також фіксує і передає в Мережу фірмі Alexa ваші пошукові запити. Що з цією інформацією відбувається далі — залишається тільки здогадуватися.

Але і це ще не все. З часу випуску Windows XP корпорація Microsoft настільки тісно «вплесла» користувача в Мережу, що часто зовсім не відомо, які відомості куди саме посилаються. Адже не дарма Antispy, компонент операційної системи, тепер обов'язково встановлюється на кожному комп'ютері, куди ставиться Windows XP.В арсеналі Windows XP є більше тридцяти різних функцій, які вимагають виходу в Інтернет і зв'язку з сервером Microsoft. В їх числі зовсім нешкідливі і навіть корисні, такі як синхронізація часу на домашньому комп'ютері, але є і вельми обтяжливі, наприклад відсилання розробникам повідомлення про помилку, при якій весь зміст оперативної пам'яті відправляється в Microsoft. Але наймогутнішим «зв'язковим», що відправляє ваші дані без вашого ж відома, є Media Player. Він посилає в Мережу інформацію про те, які музичні композиції і відеофайли були програні, а також які кодеки використовувалися при відтворенні. Програма зв'язується з Редмондом, як тільки в CD-привід вставляється аудіодиск. Не важливо, що ви збираєтеся зробити за допомогою плеєра, він спершу встановить зв'язок з сервером Microsoft. А невтаємниченим так і зовсім може здатися, що програма не працює в офлайн-режимі. Ще один прийом Microsoft для отримання інформації – це Smarttags. Власне кажучи, ці хитрі безкоштовні додатки приносять користь: клікніть правою кнопкою миші на незнайомому місці і одержите пояснення до певного поняття, об'єкту або слова. Проте і тут є свій «гачок»: клацання мишкою веде вас до Encarta — онлайнової енциклопедії від Microsoft, і інформація з вашого комп'ютера знову витікає в Редмонд.

🡨 Будь-який запит до енциклопедії Encarta передається через Інтернет на сервер Microsoft

Хоча і малоймовірно, що корпорація дійсно в змозі обробити відомості про мільйони своїх клієнтів, але, у принципі, така можливість існує, і вам нічого не повідомлять про те, яку саме інформацію одержала від вас Microsoft і як саме вона буде використана. Швидше за все, корпорація не складає досьє на користувачів її продукції, але інтернет-магазини прямо-таки живуть цим, навіть такі гіганти, як Amazon. Безумовно, Amazon не здійснює ніяких протиправних дій. Проте покупець ризикує, залишаючи на сайті яку-небудь інформацію особистого характеру. В жовтні 2003 року відбувся такий випадок. Дівчина з Німеччини поїхала до свого нареченого в США. В аеропорту міста Атланта її затримали. На питання про причину вона одержала несподівану відповідь: прикордонник нібито встановив за допомогою Amazon.com, що дівчина має «підозрілі літературні пристрасті». «Фактично, — пояснює Кристина Хегер, прес-секретар німецького відділення Amazon, — його думка була основана на списку літератури, яку замовляла молода жінка». Уповноважений по захисту інформації уряду Німеччини Петер Шаар теж не бачить в цьому нічого осудного. Врешті-решт, дівчина сама добровільно виставила список своїх вподобань на загальний огляд в Інтернеті. Разом з цим Шаар радить кожному, хто розміщує в Мережі зведення про себе, не тільки не указувати всю правду, але ще і трохи прибріхувати. Торгові мережі, що поширюють так звані карти покупця, також збирають дані про своїх клієнтів, заручаючись їх згодою. Така діяльність мереж навіть принесла цим картам Приз Великого Брата — «Big Brother Award», який присуджує німецька організація по захисту інформації FoeBuD. За її оцінками, за допомогою карт покупця збираються персональні відомості про мільйони клієнтів — в одній тільки Німеччині такими картами володіють близько 25 млн. чоловік. Зібрані відомості використовуються в комерційних цілях, для реклами і вивчення ринку. Згідно закону, основне призначення таких карт — надавати покупцям знижку, а складання досьє на клієнтів, власне, не є основною задачею. Тому згідно із законом відповідальність для тих, хто випускає карти покупця, менш строга, ніж для тих, хто займається збором інформації професіонально. Крім того, через великий об'єм даних про своїх клієнтів фірма, що використовує «карти покупця», сама має в штаті спеціаліста по захисту інформації. Прес-секретар однієї з таких фірм Ніна Пурчер роз'яснює: «Ніякі досьє на клієнтів не ведуться». Власники карт покупця можуть одержувати поштою деяку рекламу, але тільки в тому випадку, якщо вони погоджуються з відповідним пунктом договору, який укладають з компанією, що надає їм карту. В інтернет-магазині, торгуючому програмним забезпеченням, бережеться ваш обліковий запис, який ви самі і зареєстрували. Пригадайте, які дані ви туди вводили: свої ім'я, ім’я по-батькові прізвище, домашня адреса, по якій кур'єр доставить вам коробочні версії програм, телефон для зв'язку і, наприклад, номер пластикової картки, за допомогою якої ви розплачувалися. Чи не так, вже достатньо інформації? Яку, зауважте, ви ввели самі, добровільно.Скільки інформації про вас і вашому способі життя можна взнати, тільки вивчивши платежі, зроблені за допомогою тієї ж пластикової картки! Те ж програмне забезпечення, куплене вами в інтернет-магазині; платні сайти, за доступ до яких ви платили, спрямованість музики, яку ви скачували, книги, годинник, їжа і напої — скрізь ви використовували одну і ту ж пластикову карту. І знову ж таки, інформація, якою в даний момент в кращому випадку володіють ваш банк і всі ті місця, де ви встигли «засвітитися», а у гіршому разі — взагалі невідомо хто, була надана вами без якого б то не було примушення. Якце не жорстоко звучить, але той, хто дає згоду на використання своїх даних третіми особами, винний сам. Проте покупцю повинно бути роз'яснено, хто може скористатися його даними; крім того, покупець повинен мати право відмовитися від надання своєї інформації у будь-який час. В порівнянні з США, де рекламні фірми ведуть досьє на потенційних клієнтів і завалюють їх дзвінками і електронною поштою, ми поки що живемо в цілком заповідному місці.

**Висновок**

Завжди і у всьому є свої плюси та мінуси. Навіть такий гігант комп’ютерної індустрії, як Microsoft стикається з проблемами на шляху розвитку захисту інформації від несанкціонованого копіювання, використання невідомих драйверів та ін.. Але з часом всі ці методи захисту удосконаляться і будуть широко розповсюджені по світу.

Широке використання TPM-чіпів призведе до революції в комп’ютерній індустрії, бо виробникам периферії прийдеться виготовляти свою продукцію сумісну з NGSCB. Тому я думаю, що TPM-чіпи будуть довго приживатися.

Так, DRM не дуже вигідне рішення, для покупця. Бо звичайно, що дешевше придбати піратську копію тієї, чи іншої програми чи фільму. Але це вже є порушенням закону багатьох країн світу…

RFID також не є вигідним рішенням для продавців – це зумовлене порівняно високою ціною самого чіпа. Але з часом ціна на нього знизиться і він себе оправдає. Але є ще одна проблема – проблема безробіття: коли в супермаркетах будуть стояти зчитуючі пристрої, які будуть зчитувати інформацію з RFID чіпів, цим супермаркетам треба буде набагато скоротити кількість персоналу. І так само є певна частка ризику збою роботи зчитуючого пристрою, який може зняти неправильну суму з рахунку покупця. Ця сума може бути і більшою, і меншою тому цей ризик існує і для покупця, і для продавця. Але я надіюсь, що і ця проблема буде вирішена.

На мою думку, нам прийдеться довго чекати до того часу, коли ці всі технології будуть використовуватись всіма і скрізь.