2. Kraus K. Security management process for video surveillance system. Proceedings in Advanced Intelligent Video Surveillance, Proceedings of IFIP Wireless Days, 6th IFIP Network Control Conference; November 2008

УДК 004.056.5

АНАЛІЗ МЕХАНІЗМІВ ЗАХИСТУ СУЧАСНИХ ОПЕРАЦІЙНИХ СИСТЕМ

Койдан Ю. Г., здобувач вищої освіти гр. МКБп-201
Науковий керівник: **Петренко Т. А**, к.т.н., доцент
Національний університет «Чернігівська політехніка»

Вимоги що встановлюються НД ТЗІ 1.1-002-99 - Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу жорстко регламентують схему (або модель) адміністрування механізмів захисту. Це повинна бути централізована схема, єдиним елементом якої виступає виділений суб'єкт, зокрема адміністратор. При цьому кінцевий користувач виключений у принципі зі схеми адміністрування механізмів захисту.

При реалізації концепції побудови системи захисту, регламентованої розглянутими вимогами, користувач не наділяється елементом довіри, оскільки він може вважатися потенційним зловмисником, що і відбувається на практиці.

Розглянемо концепцію, реалізовану в сучасних універсальних ОС. Тут "власником" файлового об'єкта, тобто особою, яка одержує право на завдання атрибутів доступу до файлового об'єкта, є особа, котра створює файловий об'єкт. Оскільки файлові об'єкти створюють кінцеві користувачі, вони й призначають атрибути доступу до створюваних ними файлових об'єктів. Інакше кажучи, в ОС реалізується розподілена схема призначення атрибутів доступу, де елементами схеми адміністрування є власне кінцеві користувачі [2].

У цій схемі користувач повинен наділятися практично такою ж довірою, як і адміністратор безпеки, при цьому нести поряд із ним відповідальність за забезпечення комп'ютерної безпеки.

Зазначимо, що централізована й розподілена схеми адміністрування - це дві діаметрально протилежні точки зору на захист, що вимагають різних підходів до побудови моделей і механізмів захисту. При цьому скільки-небудь гарантований захист інформації можна реалізувати тільки при прийнятті концепції повністю централізованої схеми адміністрування, що підтверджується відомими загрозами ОС.

Можливості моделей, методів і засобів захисту розглядатимемо стосовно реалізації саме концепції централізованого адміністрування, одним із елементів якої є розгляд користувача як потенційного зловмисника, здатного здійснити НСД до інформації, що захищається.

Захист ОС сімейства Unix і Windows у загальному випадку базується на трьох основних механізмах:

- ідентифікація й аутентифікація користувача при вході у систему;
- розмежування прав доступу до файлової системи, в основі якого лежить реалізація дискреційної моделі доступу;
- аудит, тобто реєстрація подій.

Передусім в ОС сімейства Unix, внаслідок реалізованої в ній концепції адміністрування (нецентралізована), неможливо забезпечити замкнутість (або цілісність) програмного середовища. Це пов'язано з неможливістю установки атрибута "виконання" на каталог. Тому при розмежуванні адміністратором доступу користувачів до каталогів користувач як "власник" створюваного ним файла може занести у свій каталог виконуваний файл і установити на файл атрибут "виконання", після чого запустити записану ним програму. Ця проблема безпосередньо пов'язана з реалізованою в ОС концепцією захисту інформації.[4]

Не в повному обсязі реалізується дискреційна модель доступу, зокрема не можуть розмежовуватися права доступу для користувача "root". Відповідно, всі процеси, що запускаються ним, мають необмежений доступ до захищених ресурсів.

Крім того, в ОС сімейства Unix неможливо вбудованими засобами гарантовано видаляти залишкову інформацію. Для цього у системі абсолютно відсутні відповідні механізми.

Що стосується реєстрації, то в ОС сімейства Unix не забезпечуються реєстрація видачі документів на "тверду копію", а також деякі інші вимоги до реєстрації подій.[1]

Вбудованими засобами захисту деяких ОС сімейства Unix керування доступом до вузлів локальної обчислювальної мережі не реалізується.

Тепер коротко зупинимося на основних механізмах захисту, реалізованих в ОС сімейства Windows, і проведемо аналіз захищеності ОС сімейства Windows .

На відміну від сімейства ОС Unix, де всі завдання розмежувальної політики доступу до ресурсів вирішуються засобами управління доступом до об'єктів файлової системи, доступ у даних ОС розмежовується власним механізмом для кожного ресурсу.

Тут явно виділяються (у кращий бік) можливості розмежувань прав доступу до файлових об'єктів (для NTFS) - істотно розширені атрибути доступу, які установлюються на різні ієрархічні об'єкти файлової системи (логічні диски, каталоги, файли). Зокрема, атрибут "виконання" може установлюватися й на каталог, тоді він успадковується відповідними файлами.

При цьому істотно обмежені можливості керування доступом до інших ресурсів, які захищаються, зокрема до пристроїв уведення (неможливо заборонити запуск несанкціонованої програми з дисководів).

У межах концепції реалізації розмежувальної політики доступу до ресурсів (для NTFS) розмежування для файла більш приорітетне, ніж для каталогу, а в загальному випадку - розмежування для файлового об'єкта, який включається, приорітетніше, ніж для того, що включає. Тому користувач, створюючи файл і будучи його "власником", може призначити будь-які атрибути доступу до такого файла (тобто дозволити до нього доступ будь-якому іншому користувачеві). Звернутися до цього файла може користувач незалежно від установлених адміністратором атрибутів доступу на каталог, у якому користувач створює файл. Така проблема безпосередньо пов'язана з реалізованою в ОС Windows концепцією захисту інформації.[3]

Щодо розподілених мережевих ресурсів, то фільтрації піддається тільки вхідний доступ до розподіленого ресурсу, а запит доступу на комп'ютері, з якого він здійснюється, фільтрації не підлягає.

Отже, багато механізмів, необхідних із погляду виконання формалізованих вимог, ОС сімейства Windows реалізовані лише частково ы потребують додаткового налагодження зі сторони адміністраторів.

Крім цього, наявна велика частина загроз ОС, спрямованих на подолання вбудованих в ОС механізмів захисту, що дають змогу змінити налаштування механізмів безпеки, обійти розмежування доступу тощо. Таким чином, статистика фактів несанкціонованого доступу до інформації свідчить, що більшість поширених систем (універсального призначення) досить уразливі із погляду безпеки. І це попри виразну тенденцію до підвищення рівня їх захищеності.

Необхідно зазначити, що на практиці сучасні інформаційні системи, призначені для оброблення конфіденційної інформації, будуються уже з урахуванням додаткових заходів безпеки, що також побічно підтверджує початкову уразливість сучасних ОС.

Список використаних джерел

1. Резников Ф. А. 3 в 1. Операционная система Ubuntu Linux 10.04 (+ DVD-ROM) / Ф. А. Резников, В. Б. Комягин. — М. : Триумф, 2011. — 208 с.

2. Mac OS — операционная система от компа-нии Apple. MACLINKS.RU. [Электронный оесурс] [Цитировано: 24 декабря 2010 г.]. — Режим доступа: http://www.maclinks.ru/index.html.

3. Элсенпитер Р. Windows 10 Professional. Администрирование сетей / Р. Элсенпитер, Т. Дж. Велт. — М. : Эком, 2018. — 560 с.

4. Максимальная безопасность в Linux. — К. : ДиаСофт, 2000. — 400 с. 8. Интернет-магазин ROZETKA. [Электронный ресурс]. — Режим доступа: http://rozetka.com.ua/

УДК 004.056.53

ОСОБЛИВОСТІ ПРОЦЕСУ ВИЯВЛЕННЯ ПРИХОВАНИХ ВІДЕОКАМЕР

Коротка Г. М., здобувач вищої освіти гр. МКБп-201
Науковий керівник: **Петренко Т. А**., к.т.н., доцент
Національний університет «Чернігівська політехніка»

Візуальне спостереження є найдавнішим та досить дієвим методом збору інформації. Приховане спостереження (дистанційна зйомка відеоінформації) завдяки своєї високої інформативності та конспіративності є одним з найперспективніших способів отримання конфіденційної інформації, тому досить велика кількість зусиль була направлена зловмисниками на їх розробку та вдосконалення. Задача своєчасного виявлення оптичного спостереження стає однією з основних при проведенні профілактичних та спеціальних захисних та охоронних заходів. Своєчасне викриття наявності несанкціонованого спостереження дає змогу встановити мету проведення та визначити загрозу, яку несе спостерігач за об'єктом, персоною або групою осіб [1].

Реально протидіяти прихованій відеозйомці вкрай складно, оскільки в більшості випадків встановлення прихованих відеокамер виконують професіонали високого класу, встановлюючи мініатюрні відеокамери не тільки в стіни приміщень, але і вмонтовують їх у побутові предмети: настінні годинники, книги, попільнички, тощо. Виявити таку камеру неозброєним оком, особливо при її камуфлюванні, досить складно.

На сьогодні, відеокамери можна виявити декількома відомими способами:

1) за допомогою індикатора поля (у випадку, коли передача інформації з камери ведеться по радіоканалу);

2) оптичним способом (лазерний промінь, який виходить з оптичного детектора, відображується від об'єктива відеокамери);

3) електромагнітний детектор відеокамер [2].

Найпростішими та найдешевшими детекторами радіовипромінювання закладних пристроїв є індикатори електромагнітного поля, які світовим або звуковим сигналом сигналізують про наявність у точці розташування антени електромагнітного поля з напругою вище порогової. Більш складні з них – частотоміри, які у додаток до того забезпечують вимірювання частоти найбільш «сильного» у точці прийому сигналу. До таких детекторів-приймачів можна віднести, наприклад, трьох-діапазонний індикатор поля «iPROTECT 1216» (рис. 1). iPROTECT 1216 – точний і надійний прилад, що призначений для знаходження різних видів радіочастотних підслуховуючих пристроїв в діапазоні від 50 МГц до 12 ГГц. На відміну від інших RF-детекторів, він має значно вищу чутливість до 3G, Wi-Fi і Bluetooth пристроїв. Тому Wi-Fi, Bluetooth та інші бездротові протоколи, що працюють в діапазонах від 2,4 до 5 ГГц, виявляються на більшій відстані.

Пошук прихованої зйомки оптичними детекторами ґрунтується на зворотному відбитті спрямованого випромінювання оптичною системою об'єктиву камери відеоспостереження. Оскільки всі оптичні прилади спостереження містять світлочутливий елемент (наприклад, ПЗС-матрицю), промінь, спрямований на цей елемент, відіб'ється від нього і повернеться назад до джерела, тобто до детектора. Таким чином, оператор надсилає зондуючий промінь на місце передбачуваного розміщення прихованої відеокамери, і в разі, якщо камера дійсно встановлена, він побачить відблиск, відбитий від світлочутливого елемента. Однак, крім потрібного сигналу в поле зору будуть потрапляти випромінювання від інших елементів, для