УДК 621. 391:519.2:519.7

МЕТОД ПРОТИДІЇ ПЕРЕБОРУ ПАРОЛІВ, ЩО НЕ СТВОРЮЄ ВРАЗЛИВОСТІ ПОРУШЕННЯ ДОСТУПНОСТІ

А.О. БОЙКО

Запропоновано метод протидії перебору паролів. Запропонований метод не створює вразливості для атак порушення доступності системи, що основані на блокуванні системи після кількох невдалих спроб автентифікації.

Ключові слова: пароль, перебір паролів, підбір паролів, доступність, плече атаки.

ВСТУП

Метод автентифікації по паролях використовується у багатьох програмних та апаратних засобах. У зв'зку з тим, що ентропія паролів є низькою, актуальним питанням є захист від атак перебору паролів.

Найбільш поширеним методом протидії перебору є блокування можливості введення паролів на певний час після заданої кількості неправильно введених паролів. Однак такий метод створює іншу вразливість — можливість порушення доступності інформації, яка захищається паролем, з боку неавтентифікованого користувача. У деяких системах та засобах ситуація погіршується тим, що блокування після перевищення порогу кількості неправильно введених паролів є безстроковим — або потребується втручання адміністратора, або інформація знищується.

Прикладом є смарт-картки, у яких після трьох разів неправильно введеного PIN відбувається знищення ключів. Водночас використовувати смарт-картки без такого механізму захисту використовувати небезпечно через те, що PIN має довжину 4–7 цифр (кількість варіантів $10^4 - 10^7$), що може бути легко підібрано.

1. АКТУАЛЬНІСТЬ

При рекомендованих компанією Microsoft налаштуваннях операційної системи Windows XP SP2 [1] визначено, що можливість автентифікації має блокуватися на 30 хв. після п'яти спроб введення неправильних паролів підряд. Якщо припустити, що на введення пустого пароля потрібно не більше 5 с, то лише за $5*5=25$ с порушник може заблокувати робочу станцію на 30 хв., що у окремих випадках може бути небезпечно. Прикладом можуть бути автоматизовані системи керування технологічними процесами.

Під час проведення державної експертизи у сфері технічного захисту інофрмації операційної системи Windows XP SP2 цю небезпеку було відзначено [2] і рекомндовано блокувати можливість автентифікації після 50 спроб введення неправильних паролів підряд. Таким чином, на блокування доступу до робочої станції порушник повинен буде витратити 250 с, що все одно є практично можливим.

2. МЕТОД ПРОТИДІЇ АТАКАМ НА ДОСТУПНІСТЬ

У даній роботі запропоновано метод протидії перебору паролів, що не створює вразливості порушення доступності.

Основним показником атак, спрямованих на порушення доступності, є плече атаки. Плечем атаки називається відношення кількості ресурсів, які стають недоступними внаслідок атаки, до кількості ресурсів, які порушник повинен витратити на атаку. Чим менший цей показник, тим більш стійкою до атаки є система або засіб. У даному випадку ресурсом є час, і плече атаки при рекомендованих компанією Microsoft налаштуваннях операційної системи Windows XP SP2 складає $N = \frac{30*60}{5*5} = 72$.

Для смарт-карток плече атаки взагалі є нескінченним, оскільки при перевищенні кількості неправильно введених підряд PIN вони переходять у стан, з якого не можуть бути повернуті.

Для протидії таким атакам запропоновано динамічно збільшувати час між спробами введення пароля, а саме подвоювати час очікування наступної спроби після кожного неправильно введеного пароля. Щодо часу, який порушник повинен витратити на введення пароля, то можна зробити припущення на користь порушника і знехтувати цим часом.

Нехай після першої спроби система дозволить наступну спробу автентифікації після проміжку часу t . Тоді після другої спроби система дозволить наступну спробу автентифікації після проміжку часу $2t$. Після n спроб система дозволить наступну спробу автентифікації після проміжку часу $2^{n-1}t$. Саме цей час є часом, на який порушник може заблокувати систему, тобто $t_{dos} = 2^{n-1}t$. Водночас сам порушник повинен витратити час

$$t_{spent} = \begin{cases} 0, & n=1 \\ \sum_{i=0}^{n-2} 2^i, & n>1 \end{cases}.$$

Плече атаки складає

$$N = \frac{t_{dos}}{t_{spent}} = \frac{2^{n-1}t}{\sum_{i=0}^{n-2} 2^i t} = \frac{2^{n-1}}{\sum_{i=0}^{n-2} 2^i} = \frac{2^{n-1}}{2^{n-1}-1}.$$

Зі зростанням кількості спроб плече атаки наближається до одиниці.

$$\lim_{n\to\infty} N = 1 .$$

Фактично, порушник для порушення доступності системи або засобу на заданий час повинен витратити такий же час на атаку, що є неефективним з точки зору порушника.

Реалізація даного методу не є складною і потребує лише двох змінних у програмі (регістрів у апаратурі) до 32 біт кожен і тактового генератора (годинника) з періодом $t = 1c$. Реалізація регістрів у енергонезалежній пам'яті дозволить створити смарт-картки, які не потрібно буде блокувати при спробах перебору PIN, оскільки вимкнення і повторне увімкнення живлення не скидатиме лічильники, отже не дозволить порушнику перебирати PIN занадто швидко. Водночас метод не створює незручностей звичайним користувачам, які вводять неправильний пароль або PIN 1–2 рази помилково.

ВИСНОВКИ

Запропонований метод дозволяє ефективно протистояти перебору паролів, оскільки час, який витрачає порушник, експоненційно зростає.

Запропонований метод не створює вразливості порушення доступності системи або засобу через блокування, викликане перевищенням кількості неправильно введених паролів.

Запропонований метод не створює незручностей звичайним користувачам, які вводять неправильний пароль помилково.

Запропонований метод є простим для програмної та апаратної реалізації.

Література

1. Windows XP Professional SP2 Security Guide – Режим доступу: http://www.microsoft.com/en-us/download/confirmation.aspx?id=962
2. Державна експертиза з технічного захисту інформації операційної системи Windows XP Professional SP2. Інсталяція об'єкта експертизи та конфігурування параметрів безпеки – Режим доступу: http://msdb.com.ua/Downloads/Ukraine/Security/Expert/Conf_WXP_ver27_10_06.doc

Надійшла до редколегії 19.06.2014

Бойко Артем Олександрович, кандидат технічних наук. Наукові інтереси: принципи побудування геш-функцій та використання їх у засобах захисту інформації.

УДК 621. 391:519.2:519.7

Метод противодействия перебору паролей, который не создает уязвимостей нарушения доступности / А.А. Бойко // Прикладная радиоэлектроника: научн.-техн. журнал. — 2014. — Том 13. — № 3. — С. 296–297.

Предложен метод противодействия перебору паролів. Предложенный метод не создает уязвимости к атакам нарушения доступности системы, основанным на блокировании системы после нескольких неудачных попыток аутентификации.

Ключевые слова: пароль, перебор паролей, подбор паролей, доступность, плечо атаки.

Библиогр.: 2 назв.

UDC 621. 391:519.2:519.7

Method of preventing password bruteforcing which does not create vulnerability to accessibility violation / A.O. Boiko // Applied Radio Electronics: Sci. Journ. — 2014. — Vol. 13. — № 3. — P. 296–297.

The method of preventing password bruteforcing is proposed. The proposed method does not create vulnerability to attacks of violating system accessibility which are based on blocking the system after a few failed authentication attempts.

Keywords: password, bruteforcing, selection of paroles, accessibility, attack ratio.

Ref.: 2 items.