УДК: 004.056.52

Т.Б. Максимів
Тернопільський національний технічний університет імені Івана Пулюя, Україна

АНАЛІЗ СПОСОБІВ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

T.B. Maksymiv

ANALYSIS OF WAYS TO UNAUTHORIZED ACCESS TO INFORMATION IN COMPUTER SYSTEMS

Розмежування доступу до елементів полягає в тому, щоб кожному зареєстрованому користувачу надати можливості безперешкодного доступу до інформації в межах його повноважень і виключити можливості перевищення своїх повноважень. Розмежування доступу користувачів систем може здійснюватися за декількома параметрами: виглядом, характером, призначенням, ступенем важливості і секретності інформації.

При проектуванні систем діагностичного центру потрібно розробити і реалізувати функціональність щодо контролю доступу до апаратури та інформації, як в рамках інформаційної системи в цілому, так і до окремих інформаційних частин.

Першим етапом розмежування доступу стає автентифікація, яка являє собою процедуру перевірки дійсності ідентифікаторів. Спочатку здійснюється ідентифікація – перевіряється приналежність пред'явленого ідентифікатора, безлічі зареєстрованих у системі. У випадку коректності ідентифікатора, виконується автентифікації по перевірці паролю, щоб переконатися, що користувач є саме тим, за кого себе видає. Допуск претендента в систему дозволяється тільки у випадку успішного завершення процедури автентифікації.

Під загрозою безпеки інформаційним ресурсам розуміють дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів програмної системи, а також програмних і апаратних засобів.

Усі можливі способи несанкціонованого доступу до інформації в комп'ютерних системах, можна класифікувати за наступними ознаками:

1. За принципом несанкціонованого доступу:

- фізичне подолання рубежів територіального захисту і доступ до незахищених інформаційних ресурсів; розкрадання документів і носіїв інформації; візуальне перехоплення інформації, виведеної на екрани моніторів і принтери, а також підслуховування; перехоплення електромагнітних випромінювань.
- логічне подолання системи захисту ресурсів активної комп'ютерної мережі.

2. По положенню джерела несанкціонованого доступу:

- внутрішнє розташування джерела. Атака проводиться безпосередньо з будь-якої точки локальної мережі; ініціатором атаки найчастіше виступає санкціонований користувач.
- зовнішнє розташування джерела взлому. Зазвичай несанкціоновані дії в закриту мережу (захищену) відбуваються із відкритої; атака на окремі мережі, орієнтовані на обробку конфіденційної інформації зовсім різного рівня чи секретності різних категорій.

3. По режиму виконання несанкціонованого доступу:

- атаки, причиною яких є людина;
- атаки, причиною яких є спеціально розроблена програма без особистої участі людини. При такому виді несанкціонованого доступу використовуються спеціально розроблені програми, в основу функціонування яких покладена вірусна технологія.

4. За типом використаних уразливих місць систем:

- атаки, основані на недоліках встановленої політики безпеки. При такому виді несанкціонованого доступу політика безпеки не відображує реальні аспекти обробки інформації.
- атаки, основані на помилках управління та адміністрування комп'ютерною мережею. При такому виді несанкціонованого доступу мається на увазі некоректна організаційна реалізація чи недостатня адміністративна підтримка прийнятої в комп'ютерній мережі політики безпеки (через неуважність адміністратора певний каталог доступний усім користувачам).
- непродумані алгоритми захисту, реалізовані у засобах інформаційно-комп'ютерної безпеки;
- неякісна реалізація засобів системи захисту інформації.

5. По шляху несанкціонованого доступу:

- атаки, орієнтовані на використання прямого стандартного шляху доступу до комп'ютерних ресурсів. При такому виді несанкціонованого доступу мається на увазі недоліки політики безпеки; недоліки процесу адміністративного управління комп'ютерною мережею.
- атаки, орієнтовані на використання схованого нестандартного шляху доступу до комп'ютерних ресурсів. При такому виді доступ здійснюються шляхом використання недокументованих особливостей системи інформаційно-комп'ютерної безпеки.

6. По поточному місцю розташуванню кінцевого об'єкта атаки:

- атаки на інформацію, яка зберігається в основній пам'яті комп'ютера
- атаки на інформацію, що зберігається на зовнішніх запам'ятовуючих пристроях;
- атаки на інформацію, яка передається по лініях зв'язку.

7. По безпосередньому об'єкту атаки:

- атаки на політику безпеки і процес адміністративного управління;
- атаки на саму систему захисту та її компоненти;
- атаки на змінні елементи системи безпеки;
- напади на функціональні особливості комп'ютерної системи;
- напади на протоколи взаємодії між користувачами чи компонентами.

Щоб пройти автентифікації можуть використовуватися різні принципи, такі як знання користувачем секретного паролю; пред’явлення користувачем певних статичних характеристик (наприклад, біометрія); встановлення дійсності користувача третьою стороною. Часто для надійності використовуються різні комбінації цих принципів.

Література

1. Разграничение доступа [Електронний ресурс]/Sernam. – Режим доступу: URL: http://sernam.ru/ss_24.php.

2. Проблеми захисту інформації в комп`ютерних мережах [Електронний ресурс]/ Ua-Referat. – Режим доступу: URL: http://ua-referat.com/