КОНТРОЛЬ ЗАХИЩЕНОСТІ БЕЗДРОТОВИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Юдін О.М., к.т.н., професор
Полтавський університет споживчої кооперації України

При створенні та експлуатації комп'ютерної мережі неминуче виникає питання її захищеності від погроз на безпеку інформації. Захищеність, в умовах постійного зростання ролі інформаційних ресурсів, є однією з важливих характеристик сучасної комп'ютерної мережі (КМ). Для визначення стану захищеності КМ адміністратором використовуються спеціальні засоби – системи аналізу захищеності (САЗ), які працюють як на рівні мережі (сканери безпеки), так і на рівні вузла (програмні агенти) [1]. Причинами низької ефективності контролю захищеності є його епізодичний, запізнений характер, відсутність у сучасних САЗ можливості врахування динамічного характеру сучасних мереж та адаптації процесу контролю до поточного стану вузлів мережі і лінії зв'язку, а також значний час, що витрачається САЗ на проведення повного контролю. Аналіз дії адміністратора [2], які виконуються при проведенні контролю захище-

ності, показує, що етап перевірки вузлів мережі на наявність уразливостей характеризується великими витратами часу (до 50 % від загального циклу рішення задачі).

Покращення оперативності дії адміністратора і вдосконалення контролю захищеності можливо за рахунок організації і проведення автоматичного адаптивного контролю захищеності КМ на основі експертної інформації [3]. Останнім часом все більш частіше для побудови сегментів КМ використовуються бездротові КМ (БКМ). Організація контролю захищеності у БКМ у порівнянні із кабельними (дротові) КМ визначається особливостями їх архітектури та протоколів функціонування:

– вузли БКМ є мобільними, що обумовлює динамічну топологію мережі, а також можливість попадання вузла у «мертві зони»;

– на якість зв'язку (дальність і швидкість) здійснюють вплив різні перешкоди, зі зростанням відстані від точки доступу швидкість передавання даних і загальна якість зв'язку зменшується;

– обмеженість ресурсів елементів мережі: ємність джерела живлення, обсяг пам'яті, продуктивність процесору тощо.

Таким чином, організація контролю захищеності БКМ залежить від наступних факторів: відстані вузла до точки доступу, відстані вузла до «мертвої зони», часу автономної роботи джерела живлення вузла, активності пересування вузла, кількості запитів, що формує вузол (активність вузла) та кількості запитів, які він обслуговує (важливість вузла). Враховуючі вище зазначені фактори особливість роботи алгоритму організації контролю БКМ полягає у використанні показників для визначення важливості вузла, що відображають динамічний характер БКМ, не вимагають застосування експертної інформації внаслідок чого зменшується час підготовчих операцій на проведення контролю. Критерієм роботи алгоритму, що визначає його особливість, є повнота проведення контролю, тобто охоплення контролем максимально можливої кількості вузлів мережі.

Література

1. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ – Петербург, 2003. – 624 с.: ил.
2. Шохін Б.П., Юдін О.М., Мазулевський О.Є. Вдосконалення контролю за станом захищеності комп'ютерної мережі на основі адаптивного моніторингу // Зб. наук. пр. ВІТІ НТУУ «КПІ». – К.: ВІТІ НТУУ «КПІ» – 2004. – № 4. – С. 208–217.
3. Мазулевский О.Е. Методика организации контроля защищенности компьютерной сети // Радіоелектронні і комп'ютерні системи. – Х.: «ХАІ», 2006. – № 5. – С. 122–127.