УДК 681.51:519.876
У. Яциковська
(Тернопільський національний технічний університет імені Івана Пулюя)

МЕТОД АУНТЕНТИФІКАЦІЇ МАРШРУТИЗАТОРА ЗА ДОПОМОГОЮ СХЕМИ СЛОВНИКА

Атаки типу *DoS/DDoS/DRDoS* є одними із найпоширеніших атак на сьогодні і становлять основну небезпеку для комп'ютерних мереж.

Одним з методів аунтентифікації маршрутизатора є схема словника, яка складається з перевіреного джерела та багатьох каталогів. Достовірне джерело створює і підтримує базу даних словника *D* об'єктів, які зберігаються у вигляді пари ключів (*k, o*). Каталоги відповідають на запити ключа для *D* від імені клієнта-користувача. У відповідь на запит клієнт застосовує ключ *k* і надсилає запит в каталог. Якщо існує такий об'єкт в каталозі, то він висилається користувачеві. Якщо ні, то каталог повертає спеціальне значення. У будь-якому випадку каталог перевіряє, в залежності від стандартних криптографічних припущень, чи відповідь, яка б мала прийти від джерела, є актуальною і точною. Крім того, за рахунок розгортання багатьох каталогів, які є в мережі, використовується перевірка автентичності словника, що дає змогу зменшити час очікування відповіді та є ефективним способом проти атаки на відмову в обслуговуванні типу *DoS/DDoS/DRDoS*. Доцільно перевірити достовірність словника для різних схем трасування, забезпечення строгої аутентифікації маршрутизаторів, не вимагаючи від них підпису для будь-якого повідомлення.

Для аутентифікації маршрутизаторів в мережі доцільно визначити послідовність таємних ключів $K_{X,0}, K_{X,1,\dots}$ для кожного маршрутизатора. Тоді, для користувача *V* призначити повідомленням M_X. Маршрутизатор *X* містить у собі *HMAC* з $h(V \| K_{X,t})$, де *h* – є односторонньою криптографічною хеш-функцією, а *t* – квантовий час лічильника. Для того щоб знизити ймовірність повторення атаки, доцільно додати значення *V* в *HMAC*. Тобто, знайти ключ $K_{X,t}$ для маршрутизатора *X* в проміжку часу $t+2$. Для цього потрібно здійснити перевірку автентичності словника для кожної автономної системи (*AS*), джерелом якого є адміністратор *AS*. Доцільно припустити, що цей адміністратор розподіляє таємні ключі для маршрутизаторів. Отже, немає ризику атаки на хеш-функцію *h*, а дані фіксуються для користувача *V* в проміжку часу *t*. Такий підхід додає 32, 48 або 64 біт повідомленню M_X в залежності від аутентифікації маршрутизатора *X*.

Функція *HMAC* з повідомленням ключа експозиції є альтернативною схемою з використанням послідовності таємних ключів $K_{X,0}, K_{X,1,\dots}$, включаючи $K_{X,t-2}$ в повідомлення M_X протягом часу *t*. Таким чином, маршрутизатор *X* розкриває таємний ключ, використаний в *HMAC*. У цьому випадку доцільно створити послідовність ключів, як хеш-послідовність за допомогою односторонньої криптографічної хеш-функції *g*, щоб виконувалась умова $K_{X,i} = g(K_{X,i+1})$. Потім потрібно зберігати тільки $K_{X,0}$ в аутентифікації словника для *X*–го маршрутизатора автономної системи. Для будь-якого $K_{X,t}$ користувач може визначити ключ, використовуючи значення *t* з функції *g*. Таким чином, цей підхід дозволяє зменшити обсяг роботи для адміністратора *AS*. Адміністратор публікує бази хеш-послідовності кожного маршрутизатора. Оскільки ключі визначаються за допомогою хеш-послідовності, то для користувача потрібно виконати *t* хеш-обчислень для кожного маршрутизатора в мережі атаки. Для користувача такий обсяг роботи може бути незначним, якщо кількість маршрутизаторів в дереві атаки *T* не перевищує 1000.