



УКРАЇНА

(19) UA (11) 54757 (13) A

(51) 7 H04M1/66, H04Q7/00

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ
НА ВІНАХІДВидається під
відповідальність
власника
патенту

(54) СПОСІБ АУТЕНТИФІКАЦІЇ ТЕРМІНАЛЬНОГО УСТАТКУВАННЯ

1

2

(21) 2002032322

(22) 25 03 2002

(24) 17 03 2003

(46) 17 03 2003, Бюл. № 3, 2003 р.

(72) Владишевський Борис Сергійович, Радзімовський Броніслав Казимирович, Кіреєв Ігор Анатолійович

(73) ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "АЛБРОНА"

(57) Спосіб аутентифікації термінального обладнання, що полягає у використуванні обміну службовою інформацією між термінальним обладнанням і станцією (чи іншим устаткуванням), який відрізняється тим, що у відповідь на сигнал заняття лінії зв'язку терміналом станція передає у бік терміналу випадкову чи псевдовипадкову послідовність, сформовану на станції і яка складається з N бітів, серед яких вибирається n бітів, причому $n < N$, за визначеним правилом, що є бітами запиту

терміналу, а з прийнятої терміналом послідовності з N бітів витягаються по тому ж правилу n бітів запиту, що піддаються нелінійному перетворенню, результат якого у вигляді послідовності з m бітів розміщується за визначеним правилом у випадковій чи псевдовипадковій послідовності з M бітів, сформованої терміналом, причому $m < M$, що передається у бік станції, де з прийнятої послідовності M бітів витягається за відомим станції правилом послідовність з m бітів відповіді терміналу, що порівнюється з результатом нелінійної обробки, процедура якої аналогічна терміналу, послідовності з раніше переданих n бітів, причому якщо порівнювані послідовності збігаються, то це свідчить про істинність підключеного терміналу, при цьому кожен термінал має свій індивідуальний ключ нелінійної обробки і розміщення службових бітів запиту і відповіді

Винахід відноситься до техніки мереж зв'язку і може бути використано, зокрема, як спосіб захисту абонентського термінального обладнання від його несанкціонованої підміни

Є відомий спосіб, що описаний у книзі «Защита информации в компьютерных системах и сетях», Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин, под ред. д-та В. Ф. Шаньгина, М., "Радио и связь", 1999 г. (стр. 141-144), де на початку сеансу роботи абонентський термінал по запиті іншої сторони (станції, сервера чи іншого терміналу) видає пароль у її сторону. З метою приховання замість відкритої форми пароля передається відображення пароля, яке отримується шляхом перетворення відкритого пароля за допомогою деякої спеціальної функції. У цьому випадку підтвердження автентичності абонентського термінального обладнання полягає в порівнянні отриманого по запиті відображення пароля з його попередньо обчисленим і збереженим на станції еквівалентом. Якщо ці відображення рівні, то запитуваний абонентський термінал вважається істинним. Для підвищення стійкості пароля як спеціальна функція перетворення відкритого пароля використовується одні-

чна функція, що вимагає великого обсягу обчислень та складної програмної чи апаратної реалізації

Найближчим прототипом винаходу, що заявляється, є спосіб, що рекомендується для використання керівним нормативним документом КНД 45-092-98 «Система захисту від несанкціонованого доступу до використання телефонних мереж загального користування України», введеного в дію 01.06.1998 р. Відповідно цього документа, перед початком сеансу зв'язку після надходження сигналу ініціалізації з боку термінального обладнання, система захисту (СЗ) повинна передати зі станційної сторони у бік абонентського обладнання сигнал запиту автоматичної видачі коду аутентифікації (пароля). У відповідь абонентський термінал повинний передати у бік станції сигнал пароля. На станції прийнятий від абонентського терміналу пароль порівнюється з паролем, що зберігається в пам'яті станційної частини СЗ і який закріплений за даним абонентським терміналом. Якщо пароли збігаються, то СЗ дозволяє подальшу організацію з'єднання. У протилежному випадку абонентський термінал вважається помилковим і подальше з'єд-

(13) A

(11) 54757

(19) UA

нання не допускається

Документ КНД 45-029-98 обмовляє, що пароль повинний автоматично мінятися, при цьому кількість можливих комбінацій повинне бути не менш 2^{16}

Основним недоліком прототипу є те, що ступінь захищеності його від розкриття використовуваного пароля малий (перебір $2^{16} = 65536$ кодових комбінацій зажадає не більш хвилини для сучасного персонального комп'ютера)

В основу винаходу поставлена задача практично не допустити помилкової аутентифікації абонентського терміналу шляхом її підміни

Технічним результатом винаходу є аутентифікація термінального обладнання шляхом обміну спеціальною інформацією між нею і іншим обладнанням (станцією, сервером чи іншим абонентським терміналом)

Рішення згаданої задачі досягається тим, що при організації з'єднання станція передає убік абонентського терміналу службовий сигнал запиту, що обробляється в терміналі певним чином, а результат обробки передається у вигляді відповіді на станцію. Аналіз цієї відповіді на станції дозволяє зробити висновок про істинність підключеного термінального обладнання. Одержання технічного результату винаходу можливо тільки при тім, що сигнал запиту від станції являє собою випадкову чи псевдовипадкову послідовність біт, що генерується на станції, з яких тільки деяка частина біт призначена для запиту. Ця частина біт обробляється у терміналі неперіодичною процедурою, наприклад, визначається залишок при розподілі по mod D, де D - деяке число. Цей залишок замишується у випадкову чи псевдовипадкову послідовність біт, що генерується терміналом і передається у вигляді відповіді убік станції.

Процедура аутентифікації абонентського терміналу відбувається у такий спосіб

Термінал абонента перед початком сеансу

зв'язку ініціалізується і передає на станцію (чи інше обладнання) сигнал заняття лінії зв'язку між ними. Перш ніж надати терміналу можливість здійснити процедуру подальшого встановлення з'єднання, станція спочатку робить аутентифікацію підключеного терміналу, тобто встановлює його істинність, щоб не допустити підміни. Для цього станція, у відповідь на сигнал заняття лінії зв'язку (наприклад, абонентської лінії), передає убік терміналу запит у вигляді «короткої», з n біт випадкової чи псевдовипадкової послідовності, поміщеної в більш довгу, випадкову чи псевдовипадкову послідовність з N біт, що генерується станцією, причому $n < N$.

З цієї «довгої» послідовності біт термінальне обладнання витягає запитальну послідовність, знаючи місце розташування біт запиту в переданій «довгій» послідовності. Ця запитальна послідовність обробляється з застосуванням неперіодичної процедури, у результаті якої виходить деяке число. Це число у вигляді послідовності з m біт заміняє за визначеним правилом відповідне число біт більш довгої випадкової чи псевдовипадкової послідовності з M біт, що генерується термінальним обладнанням, причому $m < M$, і переданої убік станції. Прийнята станцією відповідь порівнюється з числом, що було отримано на станції в результаті аналогічної термінальному устаткуванню неперіодичної процедури над тією ж «короткою» послідовністю з n біт, що була обрана станцією як запитальна. Якщо результат порівняння позитивний, то даний термінал вважається істинним, у протилежному випадку - помилковим. Індивідуальність кожного терміналу визначається правилом розміщення n m біт «коротких» запитальної і відповідної послідовностей біт у «довгих» випадкових чи псевдовипадкових послідовностях з N і M біт, а також ключем неперіодичного перетворення, наприклад, числом D. Таким чином, забезпечується висока стійкість від підміни.