УКРАЇНА

(19) UA (11) 116653 (13) U

(51) МПК (2017.01)
G06F 21/31 (2013.01)
G06F 7/00

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2016 13392**

(22) Дата подання заявки: **26.12.2016**

(24) Дата, з якої є чинними права на корисну модель: **25.05.2017**

(46) Публікація відомостей про видачу патенту: **25.05.2017, Бюл.№ 10**

(72) Винахідник(и):
Баришев Юрій Володимирович (UA),
Неуйміна Крістіна Володимирівна (UA)

(73) Власник(и):
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ,
Хмельницьке шосе, 95, м. Вінниця, 21021 (UA)

(54) СПОСІБ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

(57) Реферат:

Спосіб автентифікації користувачів полягає в тому, що генерують дані доступу користувача, системою обчислюють результат гешування, геш-значення присвоюють обліковому запису користувача у системі, для доступу користувачі запитують перехід у захищений режим передачі даних. Користувач і система встановлюють захищений режим, порівнюють обчислений результат зі значенням, збереженим та привласненим обліковому запису поточного користувача системи, системою дозволяють або не дозволяють доступ. Геш-значення на стороні користувача обчислюють на основі пароля користувача та параметрів робочих станцій, які отримують за допомогою пристрою введення автентифікаційних даних користувача та пристрою отримання параметрів робочої станції відповідно. Геш-значення на стороні системи отримують, використовуючи збережене геш-значення пароля користувача як ключові дані для гешування параметрів робочих станцій, з якими користувачеві дозволено працювати.

UA 116653 U

Корисна модель належить до області інформаційних систем і може бути використана при організації системи безпеки в інформаційних електронних системах.

Відомий спосіб автентифікації потоків даних [патент України № 104483 від 06.08.2010., МПК G06F 21/30, бюл. № 7, 2012 р.], який полягає в тому, що включає етапи, на яких генерують криптографічну величину для кількості N послідовних кадрів даних і інформації про конфігурацію з використанням криптографічної хеш-функції, в подальшому геш-функції, де інформація про конфігурацію включає інформацію для рендерингу потоку даних; здійснюють вставку криптографічної величини в кадр потоку даних, що слідує за N послідовними кадрами даних; здійснюють ітеративне генерування проміжної криптографічної величини для кожного з N послідовних кадрів з використанням вихідного стану, де вихідний стан являє собою проміжну криптографічну величину попередньої ітерації і де вихідний стан першої ітерації являє собою проміжну криптографічну величину для інформації про конфігурацію.

Недоліком цього способу є те, що він не може бути використаним для автентифікації користувачів.

Найбільш близьким до способу, що пропонується, є спосіб захисту даних доступу користувача системи [патент України № 9534 від 05.11.2004 р., МПК G06F 7/00, бюл. № 10, 2005 р.], який полягає в тому, що системою генерують дані доступу користувача до системи, системою передають ідентифікатори користувачу додатком до генеральної угоди, ідентифікатори поодинці пропускають через функцію хешування, в подальшому гешування, вихідні значення ідентифікаторів складають, складене вихідне значення пропускають через інший (або той же) алгоритм функції гешування, системою обчислюють результат, значення (в подальшому геш-значення) присвоюють обліковому запису користувача у системі, видаляють початкові ідентифікатори, не зберігаючи їх у системі, для доступу до системи користувачі запитують перехід у захищений режим передачі даних, користувач і система встановлюють захищений режим, користувач передає ідентифікатори до системи, ідентифікатори поодинці пропускають через функцію гешування, вихідні значення ідентифікаторів складають, складене вихідне значення пропускають через інший алгоритм функції гешування, системою порівнюють обчислений результат зі значенням, збереженим та привласненим обліковому запису поточного користувача системи, системою дозволяють або не дозволяють доступ.

Недоліком прототипу є недостатня стійкість до атак з використанням шпигунських апаратних та програмних засобів, які можуть бути встановлені на робочій станції.

В основу корисної моделі поставлена задача створення способу автентифікації користувачів, в якому за рахунок нових операцій та їх послідовності стає можливим покращення віддаленої автентифікації користувачів, що призводить до підвищення стійкості.

Поставлена задача вирішується за рахунок того, що генерують дані доступу користувача, системою обчислюють результат гешування, геш-значення присвоюють обліковому запису користувача у системі, для доступу користувачі запитують перехід у захищений режим передачі даних, користувач і система встановлюють захищений режим, порівнюють обчислений результат зі значенням, збереженим та привласненим обліковому запису поточного користувача системи, системою дозволяють або не дозволяють доступ, крім того геш-значення на стороні користувача обчислюють на основі пароля користувача та параметрів робочих станцій, які отримують за допомогою пристрою введення автентифікаційних даних користувача та пристрою отримання параметрів робочої станції відповідно, геш-значення на стороні системи отримують, використовуючи збережене геш-значення пароля користувача як ключові дані для гешування параметрів робочих станцій, з якими користувачеві дозволено працювати.

На кресленні наведена схема пристрою, що реалізує спосіб автентифікації користувачів.

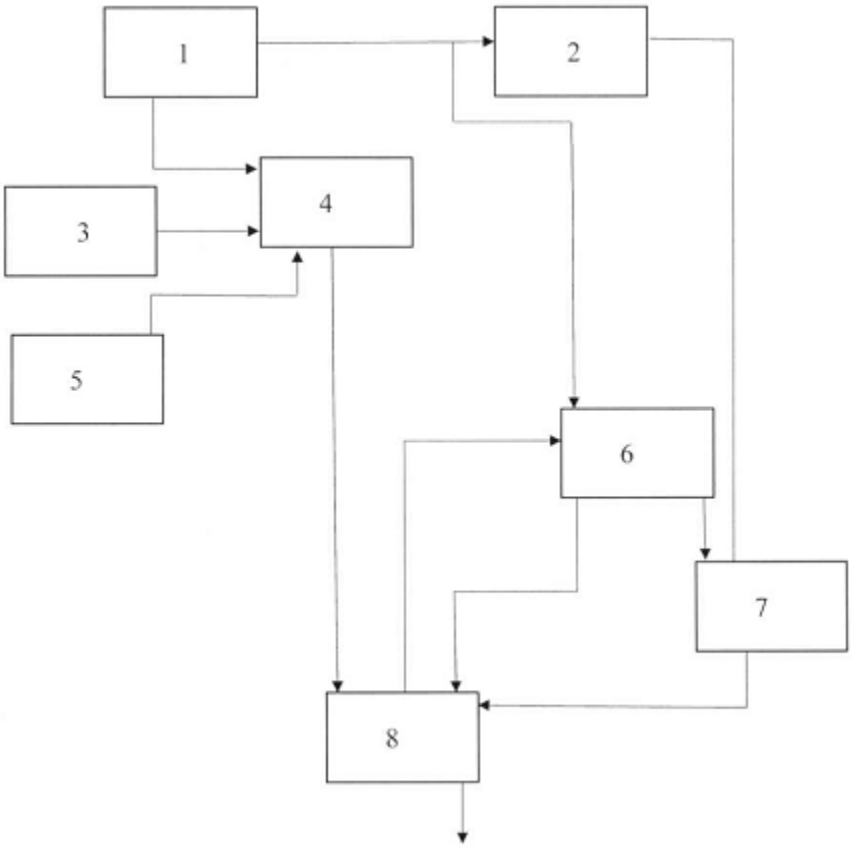
Схема містить пристрій введення автентифікаційних даних користувача 1, перший вихід якого є входом до пристрою зберігання геш-значень паролів 2 та першим входом пристрою зберігання параметрів робочих станцій 6. Другий вихід пристрою введення автентифікаційних даних користувача 1 є першим входом першого пристрою гешування 4. Вихід пристрою зберігання геш-значень паролів 2 є другим входом другого пристрою гешування 7. Другим входом першого пристрою гешування 4 є вихід з регістра зберігання ключа 3, а третім входом є вихід з пристрою отримання параметрів робочої станції 5. Перший вихід пристрою зберігання параметрів робочих станцій 6 є другим входом пристрою порівняння 8, а другий вихід є першим входом другого пристрою гешування 7. Другий вхід пристрою зберігання параметрів робочих станцій 6 є першим виходом пристрою порівняння 8. Першим входом пристрою порівняння 8 є вихід першого пристрою гешування 4, третім входом є вихід другого пристрою гешування 7. Другий вихід пристрою порівняння 8 є виходом всього пристрою.

Спосіб автентифікації користувачів виконується на пристрої таким чином. З пристрою введення автентифікаційних даних користувача 1 до пристрою зберігання геш-значень паролів

2 відправляють ідентифікатор користувача, а до першого пристрою гешування 4 - пароль. За допомогою першого пристрою гешування 4 отримують геш-значення від результату конкатенації пароля та параметрів робочої станції та надсилають його до пристрою порівняння 8. Одночасно ідентифікатор користувача, який передають від пристрою введення автентифікаційних даних користувача 1 до пристрою зберігання геш-значень паролів 2, надсилають до пристрою зберігання параметрів робочої станції 6. Починають ітеративний процес. За допомогою другого пристрою гешування 7 гешують параметри робочої станції, з якою користувачеві дозволено працювати, отримані з пристрою зберігання параметрів робочої станції 6, використовуючи геш-значення пароля користувача, отримане з пристрою зберігання геш-значень паролів 2, як ключ гешування. За допомогою пристрою порівняння 8 порівнюють геш-значення, отримані від першого пристрою гешування 4 та від другого пристрою гешування 7. Якщо геш-значення збігаються, автентифікацію вважають успішною, надсилають сигнал дозволу доступу на другий вихід пристрою порівняння 8, який є виходом всього пристрою, і завершують виконання способу автентифікації користувачів. Якщо геш-значення не збігаються з першого виходу пристрою порівняння 8 надсилають запит на отримання параметрів наступної робочої станції, з якою користувачеві дозволено працювати, і починають нову ітерацію. У випадку, коли з пристрою зберігання параметрів робочої станції 6 до другого пристрою гешування 7 було надіслано всі параметри робочих станцій, з якими користувачеві дозволено працювати, з пристрою зберігання параметрів робочої станції 6 надсилають до пристрою порівняння 8 сигнал про відсутність робочих станцій, на основі якого в пристрої порівняння 8 формують сигнал заборони доступу, який надсилають на другий вихід пристрою порівняння 8, який є виходом всього пристрою, і завершують виконання способу автентифікації користувачів.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб автентифікації користувачів, який полягає в тому, що генерують дані доступу користувача, системою обчислюють результат гешування, геш-значення присвоюють обліковому запису користувача у системі, для доступу користувачі запитують перехід у захищений режим передачі даних, користувач і система встановлюють захищений режим, порівнюють обчислений результат зі значенням, збереженим та привласненим обліковому запису поточного користувача системи, системою дозволяють або не дозволяють доступ, який **відрізняється** тим, що геш-значення на стороні користувача обчислюють на основі пароля користувача та параметрів робочих станцій, які отримують за допомогою пристрою введення автентифікаційних даних користувача та пристрою отримання параметрів робочої станції відповідно, геш-значення на стороні системи отримують, використовуючи збережене геш-значення пароля користувача як ключові дані для гешування параметрів робочих станцій, з якими користувачеві дозволено працювати.



Комп'ютерна верстка А. Крулевський

Міністерство економічного розвитку і торгівлі України, вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601