УДК: 004.056.52
Максимів Т.Б., аспірант
Тернопільський національний технічний університет ім. І.Пулюя, Україна

БІОМЕТРИЧНА СХЕМА ПЕРЕВІРКИ АУТЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ БІОХЕШ ФУНКЦІЇ

Taras Maksymiv, postgraduate

BIOMETRIC AUTHENTICATION SCHEME USING BIO-HASH FUNCTION

Розподілена, мережева система дозволяє користувачам ефективно отримувати доступ до ресурсів. Веб-сервіси, такі як Інтернет-магазини та Інтернет-банкінг, стали поширеними в сьогоднішньому технологічному світі, що викликало серйозний попит на процеси віддаленої автентифікації, що забезпечує безпеку операцій між користувачами та серверами. У різних серверних середовищах схеми автентифікації користувачів вимагають впровадження підвищених рівнів володіння. Перша схема аутентифікації з застосуванням пароля була введена компанією Lamport в 1981 році, і з тих пір були проведені різні дослідження щодо безпеки, ефективності та вартості схем аутентифікації. Існуючі схеми віддаленої автентифікації в основному реалізуються за допомогою системи відкритих ключів, і в більшості випадків їх можна розділити на традиційні схеми автентифікації на основі сертифікатів та схеми автентифікації на основі ідентичності.

Для забезпечення безпечної, ефективної та практичної автентифікації були запропоновані різні схеми, основані на ідентичності. Один клас заснований на операції порівняння, який є практичним, але неефективним, оскільки для здійснення операції порівняння потрібна висока обчислювальна вартість. Другий грунтується на певній хеш-функції, через яку ідентифікаційна інформація відображається до точки на еліптичній кривій, в результаті чого виникає дуже складна структура. Третій – пряма схема на основі ідентифікатора, яка використовує загальну криптографічну хеш-функцію з структурою, яка є більш простішою, ніж у другому класі. Через простоту цієї структури автентифікацію можна виконати лише за допомогою тристороннього рукостискання. Проте, зловмисник все ще легко може вигадати яку-небудь атаку на таку систему. Коли враховуються всі проблеми згаданих вище трьох категорій, безпечні прямі схеми автентифікації на основі ідентичності забезпечують оптимальний дизайн для користувачів мобільних пристроїв та програм у реальному часі.

Останнім часом схеми автентифікації на основі ідентичності з хеш-функцією були розділені на три категорії відповідно до методів, використовуваних у процедурі автентифікації: (1) схема, основана на знаннях, (2) об'єктна схема та (3) біометрична схема. Проте кожен тип має свої характеристики та обмеження:

1. Аутентифікація, основана на знаннях, проста, зручна та ефективна, але вона є слабкою для витоку інформації зловмисникам;
2. Об'єктна автентифікація, заснована на фізичному володінні пристроєм, таким як смарт-карта, і дозволяє зловмиснику видати себе за законних користувачів у ситуації, коли втрачається смарт-картка,
3. Аутентифікація на основі біометрії показує кращі результати, ніж два типи, описаних вище. Біометричні ключі, такі як відбитки пальців або особові риси, не можуть бути втрачені та забуті. Проте біометричні зразки, такі як обличчя, можуть бути захоплені в різних системних базах даних, тому біометричні ключі можуть залишатися незахищеними.

Багатофункціональна біометрична автентифікація поєднує в собі використання пароля, біометрії та захисту від смарт-карт, щоб підвищити безпеку та запобігати

різним типам атак, і це не впливає на вищезгадані дефекти. Такі схеми останнім часом стали координаційним центром дослідження, головним чином відображеними в роботі, яку висували різні дослідники. Розглянуто біометричну аутентифікацію на основі схеми Cao і Ge. Така схема є вразливою до біометричної помилки розпізнавання, повільного неправильного визначення пароля, офлайн атаки на паролі, атаки на відображення користувача, вгадування ідентифікатора користувача, DoS атаки, а також відсутність узгодження ключів сеансу.

Огляд схеми автентифікації Cao і Ge.

Процес схеми автентифікації Cao і Ge розглядається перед проведенням аналізу безпеки. Їх схема включає в себе три фази: етап реєстрації, фаза зміни пароля та фаза логіну та аутентифікації. Етап реєстрації – цей етап є першим, який потрібно виконати, коли користувач хоче зареєструвати себе на сервері. Етап зміни паролю – виконується, коли користувач хоче змінити пароль або коли смарт-картка втрачена. Етап логіну або аутентифікації – користувач хоче підключитися і увійти у систему віддалено.

Біо-хеш-функція.

Хеш-функція стосується функції односторонньої трансформації. Функція хеша виконує довільний вхід і повертає рядок з фіксованим розміром, який називається хеш-значенням.

Через особливість та здатність біометрії диференціювати конкретну особу від інших, різні системи прийняли методи вирішення проблем аутентифікації та перевірки. Однак невелика зміна біометричних даних (втрата невеликої інформації, шум або зміна порядку введення даних) може призвести до суттєвої зміни хеш-значення через невизначеність, притаманну пошуку біометричних особливостей. Іншими словами, загальні хеш-функції призводять до великих відмінностей через незначні відмінності вхідних даних, а помилки розпізнавання є результатом легких біометричних змін. Для вирішення цієї проблеми пропонується і вивчається біометрична функція. У різних дослідженнях, присвячених системам біохешуванню, функція біо-хешу має дотримуватися наступних властивостей:

- подібна біометрична інформація повинна мати подібні хеш-значення,
- різна біометрична інформація не повинна мати подібних хешей,
- обертання та переклад оригінального шаблону не повинно суттєво впливати на хеш-значення,
- часткова біометрична інформація повинна бути сумісна, якщо є достатньо докладних питань.

Певний клас хеш-функції може бути сформований так, щоб бути вічним у тому порядку, в якому вхідний шаблон представляється хеш-функції, і такі хеш-функції називаються функцією біо-хешу або симетричним хешем. Отже, функція біо-хешу може вирішити помилку розпізнавання загальної хеш-функції і може автентифікувати законного користувача, навіть якщо біометрична інформація користувача трохи зміниться.

Список використаної літератури

1. Fundamentals of Information Systems Security/Access Control Systems [Електронний ресурс]/wikibooks. – Режим доступу: URL: https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems.

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