технології 3D Secure, протоколу KERBEROS та багатофакторної системи автентифікації дає можливість виокремити їхні недоліки та на основі цього запропонувати комбінований механізм автентифікації під час здійснення транзакції в інтернет-платіжній системі.

Мета роботи полягає у аналізі методів автентифікація міжнародних платіжних систем VISA і MasterCard, протоколу автентифікації KERBEROS, який застосовується при розрахунках в інтернет-платіжних системах, та багатофакторної автентифікації. Основні завдання дослідження: проаналізувати механізми дії технології 3D Secure, протоколу KERBEROS та багатофакторної автентифікації;виокремити основні недоліки описаних методів; запропонувати шляхи вдосконалення існуючих методів автентифікація в інтернет-платіжних системах.

Високоефективними розробками у галузі безпеки електронних платежів є технології 3D Secure (Verified by VISA і MasterCard Secure Code), які дозволяють значно знизити ризики при мережевих розрахунках. Суть технології 3-D Secure полягає у попередній перевірці особистості власника карти. Звірку даних виконує банк-емітент платіжної картки, який володіє необхідною інформацією про клієнта. Таким чином, банк-емітент автентифікує користувача картки у момент здійснення платежу та повідомляє віртуальний магазин у режимі реального часу про те, чи дійсно покупець є користувачем даної картки [1]. Іншим методом автентифікації, який, на нашу думку вартий уваги,є протокол Kerberos. Основним недоліком даного протоколу є безпосередня передача реквізитів картки від покупця до продавця. Враховуючи це, можна запропонувати удосконалену систему автентифікації на основі Kerberos. Ця система передбачає відсутність ключа між сервером продавця та покупця, а також присутні нові зв'язки між сервером продавця та PGS

Очевидною перевагою запропонованого нами удосконаленого варіанту протоколу Kerberos є відсутність безпосередньої передачі реквізитів картки від покупця до продавця під час інтернет-платежу. У такий спосіб можна зменшити кількість шахрайств, пов'язаних із перехопленням реквізитів картки. У запропонованій схемі протоколу продавцю передаються маркери платежу замість інформації по картці. І, таким чином, ні продавець, ні зловмисник, який зламує базу даних, не мають можливості нелегально отримати реквізити картки. Варто також зазначити, що маркер криптографічно безпечний і дійсний лише для конкретного продавця, тож отримання його через прослуховування каналів нічого не дає зловмиснику. Наше удосконалення може бути застосоване до існуючого протоколу шляхом модифікації потоку даних, тобто замість надсилання реквізитів картки безпосередньо продавцю , до платіжного сервера надходить маркер [2, 3].

На нашу думку, найефективніший механізм автентифікації в інтернет-платіжних системах передбачає:

1) Використання спеціального коду, який генерує банк покупця, що дає можливість не передавати реквізитів картки через Інтернет безпосередньо продавцеві.

2) Цей код можна змінювати щоразу для нової трансакції, що передбачає значні затрати для банківської установи та створення окремого підрозділу для постійного супроводження та генерування кодів, необхідність для клієнта щоразу звертатися до свого банку за новим кодом. Проте цей код можна не змінювати щоразу для кожної нової трансакції шляхом його хешування у процесі передачі. При цьому, додатковим заходом безпеки може бути смс-підтвердження.

Список літератури

1. MasterCard представляет новое решение MasterCard TM Secure CodeTM, способствующее укреплению безопасности электронной коммерции [Електронний ресурс]. – Режим доступу: http://www.finances.kiev.ua/news/Ynternet_bankyn1/07-05-2008/MasterCard_pred.html

2. A secure on-line credit card transaction method based on Kerberos Authentication protocol [Електронний ресурс] / Jung Eun Kim . – Режим доступу http://digitalcommons.library.unlv.edu/cgi/viewcontent.cgi?article=1005&context=thesesdissertations&sei-redir=1#search=%22new+methods+of+authentication+in+internet+ payment+system%22

3. Why is Kerberos a credible security solution? [Електронний ресурс]. – Режим доступу http://www.kerberos.org/software/whykerberos.pdf

---

УДК 519.711.3:343

В.Г. Іванов, *inform@nulau.edu.ua*
Н.А. Кошева
Н.І. Мазниченко
Національний університет «Юридична академія України ім. Я. Мудрого», Харків, Україна

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ В ЗАДАЧАХ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ КОМП'ЮТЕРНИХ СИСТЕМ

Одним з основних і невід'ємних елементів комплексної системи безпеки інформаційних комп'ютерних систем є підсистема управління доступом до інформаційних ресурсів. Доступ користувачів до різних класів інформації повинен визначатися ідентифікацією, тобто процесом розпізнавання параметрів, що визначають користувача. В даний час існують три основні підходи до ідентифікації користувачів: парольна ідентифікація; апаратна ідентифікація (використання різноманітних токен, скреч-карт і т. д.); біометрична ідентифікація.

Найбільш поширені в даний час методи ідентифікації засновані на використанні паролів. Але пароль може бути скомпрометований безліччю способів. Методи, що відносяться до другого підходу, також

достатньо поширені. Фізичні об'єкти (носії інформації) можуть бути втрачені, вкрадені, передані іншій особі, дубльовані. Методи, що використовують для ідентифікації унікальні характеристики користувача (біометричні), вільні від перерахованих недоліків, тому є найбільш перспективними.

Біометрична ідентифікація – це спосіб ідентифікації особи по окремих специфічних біометричних ознаках, властивих конкретній людині. Сучасний рівень розвитку комп'ютерних технологій дозволив використовувати подібні ознаки як основу для ідентифікації людини.

Серед біометричних механізмів ідентифікації можна виділити такі: по статичних ознаках – те, що практично не міняється з часом, починаючи з народження людини (фізіологічні характеристики); по динамічних ознаках – поведінкові характеристики, тобто ті, які побудовані на особливостях, характерних для підсвідомих рухів в процесі відтворення якої-небудь дії.

Серед статичних методів в задачах ідентифікації користувачів комп'ютерних систем використовують наступні: ідентифікація по відбитку пальця, по розташуванню вен на долоні, по сітківці ока, по веселковій оболонці ока, за формою грона руки, за формою обличчя. Серед динамічних методів можна назвати наступні: ідентифікація по голосу, по почерку, по клавіатурному почерку.

При всьому теоретичному різноманітті біометричних методів тих, що застосовуються на практиці серед них небагато. Основних найпоширеніших методів три – розпізнавання по відбитку пальця, по зображенню особи (двомірному або тривимірному) і по веселковій оболонці ока.

Незважаючи на активну діяльність у напрямку розробки та вдосконалення методів ідентифікації користувачів з метою управління доступом до ресурсів інформаційних систем, надійність та стійкість існуючих систем недостатня для потреб сьогоднішнього дня. Тому актуальною бачиться проблема розробки і дослідження комплексних систем, що використовують для прийняття рішення доступу до інформаційних систем декілька біометричних характеристик користувача (наприклад, особливості клавіатурного почерку, мови, динаміки роботи користувача з маніпулятором «миша» і т.д.) або які об'єднують використання біометричних характеристик разом з класичними способами ідентифікації користувачів (наприклад, парольний захист, PIN-код, використання різноманітних карт і т.д.)

Список літератури

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. Под ред. В.Ф. Шаньгина. – М.: Радио и связь, 2001. – 376 с.

2. Голубев Г.А., Габриелян Б.А., Современное состояние и перспективы развития биометрических технологий // Нейрокомпьютеры: разработка, применение. 2004, № 10. с. 39-46.

3. Кухарев Г.А. Биометрические системы: Методы и средства идентификации личности человека. – СПб.: Политехника, 2001. – 240 с.

УДК 681.14:004.681.3

В.Д. Козюра
И.В. Пискун
В.А. Хорошко
Государственный университет информационно-коммуникационных технологий, Киев, Украина

АРХИТЕКТУРА И МЕТОД СИНТЕЗА СТРУКТУРЫ ЗАЩИЩЕННЫХ СЕТЕЙ

Региональные защищенные информационно-вычислительные сети предназначены для оперативного управления деятельностью организации, расположенных в пределах территориального управления. В настоящее время широко ведутся работы по созданию региональных и интегрированных защищенных автоматизированных систем управления деятельностью организации на базе региональной информационно-вычислительной сети. В интегрированной защищенной системы управления должен быть обеспечен доступ к ресурсам региональной информационно-вычислительной системы пользователей расположенных во всех организациях, в том числе, где нет своих вычислительных центров. Экономическая целесообразность создания региональных защищенных информационно-вычислительных сетей заключается в повышении эффективности АСУ за счет коллективного использования каналов связи и сокращения затрат на техническое обслуживание средств вычислительной техники и связи.

Региональная защищенная информационно-вычислительная сеть состоит из абонентских систем и региональной сети передачи данных, которая в свою очередь содержит: коммуникационные системы магистральной сети передачи данных, коммуникационные системы региональной сети передачи данных, терминальные узлы сети, каналы связи региональной сети передачи данных, терминальные сети передачи данных.

Для сравнения различных вариантов физической структуры региональных защищенных систем передачи данных выбран комплексный критерий оценки эффективности, учитывающий приведенные затраты на коммуникационные системы региональной защищенной сети передачи данных и каналов связи, а также потери связанные с отказами каналов связи. Основным ограничением являются предельно допустимое время задержки сообщений в региональной сети передачи данных.

Региональная защищенная сеть передачи данных имеет иерархическую структуру с простым или сложным подчинением. На нижнем ярусе располагаются терминальные узлы сети с подключенными к ним