УДК 004.056.55

АНАЛИЗ СУЩЕСТВУЮЩЕГО МЕХАНИЗМА ДИНАМИЧЕСКОЙ АУТЕНТИФИКАЦИИ ЛИЧНОСТИ

РАХАТОВА З. Р.

Евразийский национальный университет имени Л. Н. Гумилёва
(г. Астана, Казахстан)

Аннотация. С экономическим развитием глобализации, широким распространением Интернета и непрерывным внедрением национальной информатизации информационная безопасность стала центром внимания системы гарантий национальной безопасности. Аутентификация личности - это первая линия защиты системы сетевой связи и портала сетевой безопасности. Криптография является основным содержанием системы информационной безопасности и широко используется в различных приложениях, таких как сетевая безопасность и защита данных.

Abstract. With the economic development of globalization, the widespread spread of the Internet and the continuous introduction of national informatization, information security has become the focus of the national security guarantee system. Identity authentication is the first line of defense of the network communication system and the network security portal. Cryptography is the main content of an information security system and is widely used in various applications such as network security and data protection.

Введение

Информационная сеть является важной инфраструктурой современного общества и тесно связана с жизнью людей. Развитие сетевых технологий облегчило общение и обмены между людьми и предоставило людям удобные информационные ресурсы. Платформа электронной коммерции, поддерживаемая сетевыми технологиями, предоставляет предприятиям новый тип режима работы. Непрерывный прогресс сетевых технологий привел к развитию ряда новых отраслей промышленности и модернизации традиционных отраслей промышленности и способствовала прогрессу и инновациям в области вычислительной техники и коммуникационных технологий. Технология сетевой безопасности включает в себя множество компонентов. Криптографическая технология является важным инструментом для обеспечения конфиденциальности информации в сети и является основой сетевой безопасности. В практических приложениях люди больше заботятся о подлинности и целостности информации. Чтобы решить эту проблему, люди выдвинули идею цифровая подпись. В настоящее время большинство алгоритмов цифровой подписи основаны на криптографии с открытым ключом, и реализация протоколов сетевой безопасности неотделима от поддержки технологии цифровой подписи. С углублением фундаментальных теоретических исследований постоянно предлагаются новые теоретические инструменты, подходящие для приложений цифровой подписи. Кроме того, непрерывные изменения в среде приложения также требуют от нас постоянного совершенствования существующих алгоритмов подписи. В этой статье мы изучим вышеупомянутые проблемы.

Основная часть

Поскольку алгоритмы асимметричного шифрования требуют, чтобы как ключ шифрования (закрытый ключ), так и ключ дешифрования (открытый ключ) были получены из одного, а другой вычислительно неосуществим, этот тип алгоритма широко используется в области цифровых подписей. Теоретически, раскрытие открытого ключа не будет представлять никакой угрозы для безопасности закрытого ключа, поэтому открытый ключ может быть отправлен нескольким проверяющим по запросу, и безопасность закрытого ключа должна быть гарантирована [1]. В настоящее время цифровые подписи в основном включают цифровые подписи с симметричными системами ключей и цифровые подписи с асимметричными системами ключей. В этой статье схема цифровой подписи, разработанная, использует цифровые подписи с асимметричными системами ключей.

Ключевая проблема использования системы симметричных ключей для цифровой подписи заключается в том, что все доверяют третьей стороне, потому что третья сторона сохраняет все ключи и считывает все подписанные зашифрованные тексты [2]. Но некоторые люди не доверяют третьим лицам. Следовательно, было бы лучше, если бы при подписании документов участвовали только подписывающие стороны, и система асимметричных ключей может соответствовать этому требованию. Следовательно, было бы лучше, если бы при подписании документов участвовали только подписывающие стороны, и асимметричная система ключей могла бы соответствовать это требование.

В этой статье оптимизируется дизайн, основанный на механизме динамического пароля "вызов / ответ", который является асинхронным. Динамический пароль вызова ответа использует алгоритм шифрования или одностороннюю хэш-функцию для создания динамического пароля [3]. При получении запроса пользователя на вход сервер аутентификации генерирует код вызова и отправляет его пользователю. Клиент выполняет операцию хэширования, и входными параметрами операции хэширования являются код вызова и секретный ключ. То операция хэширования генерирует динамический пароль и отправляет его на сервер аутентификации [4]. Таким же образом сервер аутентификации использует ту же одностороннюю хэш-функцию для проверки личности пользователя [5]. Процесс аутентификации включает в себя четыре этапа, а именно:

1. Клиент вводит информацию о пользователе и отправляет запрос на вход на сервер аутентификации.
2. Сервер проверяет информацию пользователя, и если информация пользователя верна, он генерирует код вызова и отправляет его обратно клиенту.
3. Клиент выполняет операцию односторонней хэш-функции с ключом и кодом вызова в качестве входных параметров функции, генерирует случайный код ответа и отправляет его на сервер.
4. Сервер выполняет ту же функцию, что и клиент, генерирует код ответа как показано на рисунке 1. и сравнивает его с кодом ответа, отправленным клиентом, чтобы получить результат проверки и отправить его клиенту [6].

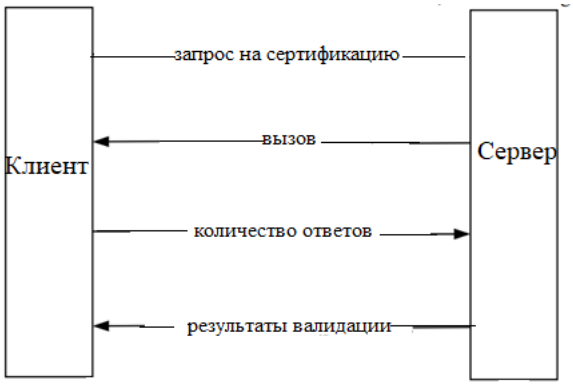

Рис. 1. Механизм динамической аутентификации по паролю

Заключение

В данной статье изучаются различные технологии и методы динамической аутентификации личности, анализируются и сравниваются преимущества и недостатки схем аутентификации, основанных на синхронизации событий, механизмах запроса-ответа и синхронизации времени, а также изучаются технологии шифрования и дешифрования. В нем исследуется существующая технология динамической аутентификации личности, в основном объясняются связанные концепции аутентификации личности, классификация аутентификации личности, идея динамическая аутентификация по паролю, метод генерации и преимущества динамической аутентификации по паролю, а также угрозы, с которыми сталкивается динамическая аутентификация по паролю. Намечены открытые исследовательские проблемы по регистрации пользователя, аутентификации при входе в систему, подробным техническим усовершенствованиям схемы и по применению схемы динамической аутентификации личности на облачной платформе.

Список использованных источников

1. Wang, Y. (2007) Research on Digital Signature Technology and Its Application in Electronic Government Affairs. Chengdu: Southwest Jiaotong University.
2. Xu, C. S., Guo, F. Y. (2020) Research and Design of Dynamic Identity Authentication Mechanism Based on Digital Signature. Computer Knowledge and Technology, 16(11):22-23.
3. Cao, Y. (2018) Key agreement scheme for dynamic identity authentication in multi-server environment. Computer Technology and Development, 28(05):131-134.
4. Zhang, S. T., Xie, Y., Wu, L., et al. (2017) Design of Security Protection Architecture of Electric Power Communication Network Based on SDN. Electronic Design Engineering, 25(19):136- 140.
5. Shi, L., Chen, N., Zhang, J. (2019) Research on access trust technology of big data platform based on dynamic and continuous authentication of identity. Cyberspace Security, 10(07):66-72.
6. Huang, G. B., Ma, J. B., Jia, R. X., et al. (2019) Identity authentication management service based on SMS dynamic password. Electronic Measurement Technology, 42(02):108-111.