СЕКЦИЯ 4. КОНЦЕПЦИЯ И МЕТОДЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

УДК 004

Ахметов У.Р.
Российский государственный университет нефти и газа
(национальный исследовательский университет)
им. И.М. Губкина, Москва

Научный руководитель:
Корнилова А.А.
Уфимский университет науки и технологий, Уфа

ПОДДЕРЖКА ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ (2ФА) В ИНФРАСТРУКТУРЕ SAMBA AD

Аннотация. В данной статье рассматривается настройка двухфакторной аутентификации на основе инфраструктуры Samba AD. Осуществляется внедрение аппаратных решений в инфраструктуре Samba AD, где за основу взята российская разработка – Рутокен.

Ключевые слова: Samba AD, двухфакторная аутентификация, безопасность, аутентификация, Рутокен, Active Directory, Alt Linux.

В эпоху постоянных информационных угроз рассматривается вопрос повышения безопасности с доступом к корпоративным сетям. Чтобы решить данную проблему сегодня все чаще используют средства двухфакторной аутентификации (2ФА). Данный метод в современном мире является одним из наиболее эффективных способов защиты от несанкционированного доступа (НСД).

В данной работе рассматривается внедрение двухфакторной аутентификации в инфраструктуру Samba AD с использованием Рутокена.

Суть 2ФА заключается в проверки подлинности, который использует два различных фактора для подтверждения личности пользователя, что безусловно повышает уровень безопасности.

Выделяют три фактора аутентификации [1], используемые в различных комбинациях: на основе знания чего-либо, обладания чем-либо, на основе биометрических характеристик (табл. 1)

Таблица 1

Факторы аутентификации [2]

Фактор аутентификации	Классификация типов факторов аутентификации NCSC-TG-017	Примеры
На основе знания чего-либо (1-й)	Type 1: Authentication by Knowledge	Пароль или парольная фраза; PIN-код
На основе обладания чего-либо (2-й)	Type 2: Authentication by Ownership	Физический ключ; Карта с магнитной полоской; OTP-токен, генерирующий одноразовый пароль
На основе биометрических характеристик (3-й)	Type 3: Authentication by Characteristic	Отпечаток пальцев; Рисунок сетчатки; Голос

Принцип работы двухфакторной аутентификации состоит из двух взаимосвязанных компонентов:

1. Пароль, который требуется при доступе к ресурсу и хранится у пользователя.

2. Сгенерированный тип данных, который может храниться на физическом устройстве или в зависимости от времени пересоздаваться.

Только при наличии этих компонентов у пользователя имеется доступ к данным.

Для реализации данной технологии существуют различные инструменты двухфакторной аутентификации (табл. 2).

Таблица 2

Инструменты двухфакторной аутентификации

Категория	Название	Описание	Linux пакеты
1	*2*	*3*	*4*
Аутентификационные приложения (Authenticator Apps)	Google Authenticator	Наиболее востреебованные приложение среди аналогов, позволяющее генерировать временные, одноразовые пароли	libpam-google-authenticator
	Microsoft Authenticator	Аналог Google Authenticator, с дополнительными функциями	authenticator
	Authy	Аналог с мультиустройственной синхронизацией, так же поддерживает защиту удаленных акаунтов	Perl-WWW-Authy

Окончание табл. 2

1	*2*	*3*	*4*
Аппаратные токены (Hardware Tokens)	Рутокен	Российская разработка для аппаратной аутентификации и ЭЦП (электронной цифровой подписи)	pcsc-lite-ccid, libpcsclite, pcsc-tools, opensc
SMS и Голосовая аутентификация	SMS	Отправка одноразового кода через SMS или звонок на телефон (последнии цифры номера)	Платформа OpenUDS Server: *openuds-server-nginx*
	Голосовые вызовы	Отправка кодов с помощью голосового вызова	Платформа OpenUDS Server: *openuds-server-nginx*
Биометрическая аутентификация	Распознавание голоса	Встроенное устройство, для сканирования отпечатка пальца (широко распространено)	Платформа VoiceKey.PLATFORM: vk-monitoringcomponent vk-routercomponent vk-securitycomponent vkchroniclercomponent vk-databasecomponent vk-licensingcomponent vk-mediahubcomponent vk-voicegridprocessor
	Распознавание лица	Встроенное устройство для распознавания биометрии лица. Технология, используемая в Apple Face ID и других	howdy
Программные решения для интеграции 2ФА	Duo Security	Поддерживает широкий спектр решений для аутентификации	duo_unix
	Okta Verify	Облачный сервис, который позволяет управлять удостоверениями и доступом	Okta (через API)

В нашем случае для примера реализации 2ФА был выбран Рутокен ЭЦП 3.0. Это активный ключевой носитель, являющийся представителем новой линейки USB-токенов и смарт-карт для подписания документов электронной подписью и строгой 2ФА на настольных и мобильных устройствах. Продукты линейки являются полнофункциональными аппаратными СКЗИ [3].

В смарт-картах и USB-токенах аппаратно-реализованы: ГОСТ Р 34.10–2012.3 [4] с длиной ключа 256/512 бит и ГОСТ Р 34.11–2012.4 [5], а также симметричные шифры Магма и Кузнечик и международные алгоритмы электронной подписи RSA и ECDSA. Криптографические операции выполняются без копирования ключа в память компьютера.

Часть моделей линейки, помимо традиционного контактного интерфейса, оснащена бесконтактным интерфейсом (NFC). При этом функции устройств доступны через оба интерфейса. Это позволяет подписывать документы на смартфонах и планшетах так же легко, как расплачиваться бесконтактной банковской картой, при наличии поддержки в используемом мобильном приложении.

Настройка Samba AD на базе ОС ALT Linux и интеграция с Рутокеном реализована по следующему алгоритму:

Шаг 1: Подготовка программного обеспечения. Обновляем репозитории и устанавливаем необходимые компоненты:

Шаг 2: Подключение устройства и генерация ключевой пары.

Шаг 3: Создание сертификата.

Шаг 4: Настройка локальной аутентификации с использованием Рутокена.

Шаг 5: Финальное тестирование.

Таким образом в данной работе реализована поддержка двухфакторной аутентификации в инфраструктуре SAMBA AD.

Список использованных источников:

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; под ред. А.А. Шелупанова, С.Л. Грузаева, Ю.С. Нахаева. М.: 2009. 552 с.

2. NCSC-TG-017 – документ «A Guide to Understanding Identification and Authentication in Trusted Systems», опубликованный U.S. National Computer Security Center. Руководство содержит комплект рекомендуемых инструкций по процедурам идентифицкации и аутентификации.

3. Уймин, А.Г. Разработка методики тестирования системы безопасности автоматизированных систем управления технологическими процессами на основе корпоративного стандарта // Автоматизация и информатизация ТЭК. 2024. Т. 610. № 5. С. 59–65.

4. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электр-

онной цифровой подписи» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. № 215-ст).

5. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. № 216-ст).

Akhmetov U.R.
Gubkin Russian State University of Oil and Gas (National Research University), Moscow

Scientific supervisor:
Kornilova A.A.
Ufa University of Science and Technology, Ufa

SUPPORT FOR TWO-FACTOR AUTHENTICATION (2FA) IN SAMBA AD INFRASTRUCTURE

Abstract. This article discusses setting up two-factor authentication based on the Samba AD infrastructure. The implementation of hardware solutions in the Samba AD infrastructure is carried out, where the Russian development - Rutoken - is taken as a basis.

Keywords: Samba AD, two-factor authentication, security, authentication, Rutoken, Active Directory, Alt Linux.