УДК 004.771

Панов Н.С.
Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск

Научный руководитель:
Холодилов С.С.
Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ VPN-СЕРВЕРА С ПОМОЩЬЮ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Аннотация. В статье проводится комплексный анализ криптографических и архитектурных основ двухфакторной аутентификации в VPN-сетях. Исследуются механизмы реализации временных одноразовых паролей, HMAC-аутентификации и протоколов расширенной аутентификации, проводится сравнительный анализ эффективности различных методов двухфакторной проверки подлинности против современных киберугроз. Особое внимание уделяется криптографической стойкости временных одноразовых паролей и их интеграции с существующими VPN-решениями.

Ключевые слова: VPN, двухфакторная аутентификация, TOTP, криптографические протоколы, информационная безопасность.

Современные угрозы информационной безопасности, включая фишинг, брутфорс-атаки и перехват сессий, требуют пересмотра традиционных методов аутентификации в VPN-сетях. Согласно последним исследованиям самыми распространенными видами атак становятся социальная инженерия (фишинг) и использование вредоносного программного обеспечения (ПО) [1].

В основе временных одноразовых паролей (TOTP) лежит алгоритм HMAC-SHA1, обеспечивающий генерацию 160-битного хеша. Работа этого механизма основана на 30-секундных временных интервалах, вычисляемых как Unix Time, деленное на 30, и секретном ключе длиной не менее 80 бит. Криптостойкость системы обеспечивается тремя основными факторами: необратимостью хеш-функции SHA-1, динамической природой генерируемых кодов и ограниченным временем жизни каждого пароля, которое обычно составляет от 30 до 60 секунд.

Среди протоколов аутентификации особого внимания заслуживают EAP-TTLS/PAP, обеспечивающий инкапсуляцию пароля в TLS-туннель, и PEAP-MSCHAPv2, который сочетает сертификаты сервера с парольной аутентификацией. Альтернативным решением является протокол OATH-HOTP, основанный на событиях и описанный в RFC 4226. Каждый из этих протоколов имеет свои преимущества и ограничения в контексте использования с VPN-технологиями.

При сравнении различных методов двухфакторной аутентификации выявляются существенные различия в их характеристиках. SMS-коды, несмотря на их широкое распространение и удобство использования, демонстрируют низкую стойкость к атакам типа SIM-swap и высокую уязвимость к перехвату. Временные одноразовые пароли (TOTP) [2], такие как реализованные в Google Authenticator, предлагают более высокий уровень защиты от брутфорс-атак, но остаются уязвимыми к фишингу. Наиболее безопасным решением являются U2F-токены, например YubiKey, которые обеспечивают максимальную стойкость к брутфорсу и практически нулевую уязвимость к атакам типа «человек посередине», хотя и уступают другим методам по удобству использования.

Модель RADIUS-сервера представляет собой трехуровневую архитектуру, где VPN-клиент взаимодействует с сервером RADIUS (например, FreeRADIUS с модулем pam_google_authenticator), который в свою очередь аутентифицирует пользователя через LDAP или Active Directory. Такая архитектура обеспечивает централизованное управление аутентификацией и поддерживает множество протоколов, включая PAP, CHAP и MS-CHAPv2.

Альтернативным подходом является использование PAM-модулей для OpenVPN [3]. В этом случае аутентификация осуществляется через

pam_exec с последующей верификацией с помощью специализированных скриптов на bash или Python, которые могут интегрироваться с генераторами TOTP. Этот метод обеспечивает гибкость в настройке и может быть адаптирован под конкретные требования системы безопасности.

Среди основных угроз для систем двухфакторной аутентификации в VPN следует отметить перехват временных паролей через фишинг, атаки на синхронизацию времени через подделку NTP-серверов и компрометацию seed-ключей.

Для противодействия этим угрозам рекомендуется использовать FIDO2/U2F вместо TOTP, внедрять квантово-устойчивые алгоритмы, такие как CRYSTALS-Kyber, и реализовывать жесткую привязку устройств через технологию device fingerprinting. Эти меры позволяют значительно повысить уровень безопасности VPN-соединений.

Проведенный анализ демонстрирует, что современные реализации двухфакторной аутентификации для VPN должны сочетать криптографически стойкие протоколы (например, TOTP с SHA-256), аппаратную верификацию через U2F-токены и защиту от асинхронизации времени через аутентифицированные NTP-серверы. Перспективным направлением развития является разработка квантово-устойчивых методов двухфакторной аутентификации, основанных на решетчатых криптосистемах, которые смогут обеспечить защиту даже в условиях появления квантовых компьютеров.

Список использованных источников:

1. Актуальные киберугрозы в странах СНГ 2023-2024 // АО «Позитив Текнолоджиз». URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/.

2. TOTP (Time-based one-time Password algorithm) // Habr. URL: https://habr.com/ru/articles/534064/.

3. OpenVPN, о котором вы так мало знали // Habr. URL: https://habr.com/ru/articles/435802/.

Panov N.S.
Nosov Magnitogorsk State Technical University, Magnitogorsk

Scientific supervisor:
Kholodilov S.S.
Nosov Magnitogorsk State Technical University, Magnitogorsk

ENHANCE YOUR VPN SERVER SECURITY WITH TWO-FACTOR AUTHENTICATION

Abstract. The article provides a comprehensive analysis of the cryptographic and architectural foundations of two-factor authentication in VPN

networks. The mechanisms for implementing temporary one-time passwords, HMAC authentication and extended authentication protocols are studied, and a comparative analysis of the effectiveness of various two-factor authentication methods against modern cyber threats is carried out. Particular attention is paid to the cryptographic strength of temporary one-time passwords and their integration with existing VPN solutions.

Keywords: VPN, two-factor authentication, TOTP, cryptographic protocols, information security.