УДК 004.056.53

РАЗРАБОТКА ПОДСИСТЕМ УПРАВЛЕНИЯ ДОСТУПОМ НА ОСНОВЕ ИНТЕГРАЦИИ МОДУЛЯ PAM И KEYCLOAK

Мустецов Д.А. (Военно-космическая академия им. А.Ф.Можайского)
Научный руководитель – кандидат технических наук, Крюков Р.О.
(Военно-космическая академия им. А.Ф.Можайского)

Введение. В условиях роста количества киберугроз и усложнения векторов атак на информационные системы обеспечение надежной аутентификации пользователей является одним из критически важных аспектов информационной безопасности. Существующие решения на основе модуля PAM (Pluggable Authentication Modules) часто не соответствуют современным требованиям безопасности и масштабируемости. Разработка модуля PAM на языке Golang с интеграцией Keycloak представляет собой решение, которое предлагает использование современных протоколов аутентификации, обеспечение централизованного управления доступом и повышение информационной безопасности, путем применения многофакторной аутентификации (MFA) [1].

Основная часть. В отличие от традиционных инструментов централизованного управления доступом (AD, OpenLDAP, FreeIPA), использующих ограниченный набор методов аутентификации, разрабатываемая подсистема управления доступом предоставляет широкий спектр современных механизмов верификации через интеграцию с Keycloak: многофакторную аутентификацию (MFA), аппаратные ключи (WebAuthn/FIDO2), внешние IP (LDAP/Active Directory, SAML), а также поддержку протоколов OAuth2 и OpenID Connect [2].

Важным преимуществом разработанного решения является централизованное управление аутентификацией и создание единого журнала событий с использованием Elasticsearch. Это позволяет осуществлять комплексный мониторинг безопасности и аудит действий пользователей в режиме реального времени, что критически важно для современных информационных систем [3].

Разработка собственного API для модуля PAM на языке Golang обеспечивает ряд критических преимуществ для высоконагруженных и встраиваемых систем [4]. Данный подход позволяет достичь максимальной производительности за счет прямого взаимодействия с системными вызовами и оптимизации использования ресурсов на низком уровне. Особенно важным является обеспечение детального низкоуровневого контроля над процессами аутентификации, что критично для систем с повышенными требованиями к безопасности. В случае применения в страиваемых системах такой подход позволяет учитывать специфические ограничения аппаратных ресурсов и обеспечивать стабильную работу в условиях ограниченной вычислительной мощности.

Выводы. Таким образом разработанная подсистема управления доступом на основе интеграции модуля PAM и Keycloak представляет собой эффективное решение, сочетающее в себе современные технологии аутентификации, что позволит организациям адаптироваться к новым киберугрозам. Благодаря многофакторной аутентификации, гибкости в выборе методов аутентификации и централизованному управлению пользователями, данная подсистема обеспечикает высокий уровень защиты от несанкционированного доступа.

Список использованных источников:

1. Red Hat Developer. Authentication and authorization using the Keycloak REST API. URL: https://developers.redhat.com/blog/authentication-and-authorization-using-the-keycloak-rest-api (дата обращения: 23.11.2024).
2. OpenID Foundation. OpenID Connect Core 1.0 Specification. URL:

https://openid.net/specs/openid-connect-core-1_0.html (дата обращения: 18.12.2024).

3. Search Guard. Kibana Single Sign-On with OpenID and Keycloak. URL: https://search-guard.com/blog/kibana-openid-keycloak/ (дата обращения: 23.10.2024).

4. Li, Y., et al. Performance Analysis of RESTful and gRPC APIs in Microservices Architecture: A Case Study on Keycloak Integration with Golang Applications. International Journal of Computer Applications, 2023. URL: ieeexplore.ieee.org (дата обращения: 23.11.2024).

Автор _____ Мустецов Д.А.

Научный руководитель _____Крюков Р.О.