Алгоритм аутентификации и авторизации для клиент-серверных веб-приложений с использованием многофакторного контроля доступа

В. А. Микулёнок
[1] Белорусский государственный университет информатики и радиоэлектроники, Минск, Республика Беларусь

Представлен алгоритм аутентификации и авторизации с использованием многофакторного контроля доступа для клиент-серверных веб-приложений.

Ключевые слова: Алгоритм, аутентификация, защита, безопасность, контроль, доступ.

Во всех сферах, таких как банки, государственные учреждения, фармацевтический сектор, военные организации, учебные заведения и т. д., вопросы безопасности становятся все более актуальными. Государственные учреждения устанавливают правила, принимают нормативные акты и заставляют организации и агентства соответствовать этим стандартам. В этих разнообразных отраслях, общим слабым звеном которых являются пароли, существует множество проблем, когда речь заходит о безопасности. Для проверки личности пользователя большинство приложений сегодня полагаются на статические пароли, однако они сопряжены с серьезными проблемами безопасности для администраторов. Пользователи предпочитают использовать легко угадываемые пароли, использовать разные учетные записи с одинаковыми паролями, записывать или сохранять их на своих компьютерах в незашифрованном виде. Использование одного и то же имени пользователя и пароля на нескольких сайтах, при утечке данных с одного сайта может привести к цепной реакции, поскольку злоумышленники получают доступ к другим учетным записям с теми же данными. Более того, хотя специальные системы, называемые менеджерами паролей, могут обеспечить безопасное хранение и поиск паролей, лишь небольшая часть пользователей использует их. Кроме того, у хакеров есть возможность использовать множество методов кражи паролей. Для преодоления этой проблемы была предложена многофакторная аутентификация (2FA) с использованием таких устройств, как жетоны и банкоматные карты, которые, как было показано, трудно взломать.

Многофакторная аутентификация обеспечивает надежную защиту против компрометации учетных записей. Даже если злоумышленник крадет или угадывает пароль пользователя, ему необходимо скомпрометировать телефон пользователя или украсть физический токен, чтобы получить доступ к учетной записи. Таким образом, злоумышленнику значительно сложнее скомпрометировать учетную запись защищенную вторым фактором аутентификации.

В рамках данного проекта будут проанализированы существующие способы аутентификации пользователей, а также разработан алгоритм аутентификации и авторизации для клиент-серверных веб-приложений с использованием многофакторного контроля доступа.

[1] **S. A. Zhang, S. Pearman, L. Bauer, and N. Christin** Why people (don't) use password managers effectively / S. A. Zhang, S. Pearman, L. Bauer, and N. Christin — 2019.

[2] **Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang** The Tangled Web of Password Reuse. In Network and Distributed System Security (NDSS) / Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang — 2014.

[3] **Juan Lang, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas** Security Keys: Practical Cryptographic Second Factors for the Modern Web / Juan Lang, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas — 2016.

The authentication and authorization algorithm for client-server web applications using multi-factor access control

V. A. Mikulenok

[1] Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

An authentication and authorization algorithm using multi-factor access control for client-server web applications is presented.

Keywords: Algorithm, authentication, protection, security, control, access.