

УДК: 004.056:621.398.2

Кайдик О.Л., канд. техн. наук, доцент
Терлецький Т.В., канд. техн. наук, доцент
Назарчук А.О., здобувач вищої освіти

Луцький національний технічний університет, o.kaidyk@lntu.edu.ua

Угрин Д.І., докт. техн. наук, професор

Шкідіна К.С., магістрант

Чернівецький національний університет імені Юрія Федьковича d.ugryn@chnu.edu.ua

ПРО ОДНОРАЗОВІ ПАРОЛІ, ЯК МЕХАНІЗМ ПІДВИЩЕННЯ БЕЗПЕКИ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

На сьогодні системи контролю та управління доступом (СКУД) відіграють ключову роль у забезпеченні фізичної безпеки об'єктів на яких здійснюється контроль входу/виходу суб'єктів доступу. Традиційні методи автентифікації в СКУД є зручними у використанні, проте мають певні вразливі місця (копіювання карт, передача PIN-кодів або їх підбір тощо). Враховуючи ці недоліки, можна зробити висновок про те, що інтеграція одноразових паролів (One-Time Password – OTP) в СКУД є перспективним підходом для значного підвищення рівня безпеки та надійності ідентифікації суб'єктів доступу.

На практиці, OTP являє собою динамічно згенеровану послідовність символів, яка є обмеженою певним періодом часу або дійсна протягом однієї сесії автентифікації.

Технологія генерування одноразових паролів базується на використанні криптографічних алгоритмів, які дозволяють скомбінувати секретний ключ до складу якого входить певний змінний параметр. В залежності від застосованого алгоритму, у якості змінного параметра виступає:

1. Час (Time-based OTP – TOTP). Такий алгоритм визначається стандартом RFC 6238 та використовує поточний час у якості змінного параметра.

$$\text{OTP}=\text{Hash}(\text{SecretKey}||\text{CurrentTime}/\text{TimeInterval})$$

де: OTP – згенерований одноразовий пароль;

Hash – криптографічна хеш-функція (SHA-1, SHA-256 тощо);

SecretKey – спільний секретний ключ;

CurrentTime – поточний час у форматі «Unix epoch»;

TimeInterval – тривалість часового вікна (30 або 60 секунд);

|| – операція конкатенації.

2. Подія (Event-based OTP – HOTP). Цей алгоритм підпорядкований стандарту RFC 4226 та використовує лічильник подій як змінний параметр.

$$\text{OTP}=\text{Hash}(\text{SecretKey}||\text{Counter})$$

де: Counter – лічильник подій.

Аналіз основних характеристик паролів (табл. 1) підтверджує й те, що одноразовий пароль дозволяє підвищити безпеку автентифікації суб'єкта доступу завдяки своїй стійкості до поширених атак, а враховуючи те, що кожен із OTP дійсний лише один раз, то ще й ефективно протидіє атакам повторного відтворення. Щодо безпеки OTP, то вона залежить, перш за все, від надійності захисту секретного ключа на обох сторонах та безпеки самого каналу доставки (особливо гостро це питання стоїть для SMS/Email OTP). Неправильна реалізація системи OTP або її конфігурація є ще одним її слабким місцем.

Із викладеного вище бачимо, що OTP є своєрідним криптографічним інструментом, який покликаний підтвердити ідентичність суб'єкта доступу шляхом генерації та верифікації тимчасового секретного значення.

Таблиця 1 – Порівняльна характеристика паролів

Характеристика	Пароль	
	статичний	одноразовий
Термін дії	тривалий	короткий
Повторне використання	так	ні
Стійкість до перехоплення	висока	низька
Стійкість до атак повторного відтворення	низька	висока
Необхідність запам'ятовування	висока	низька

Інтеграція одноразових паролів в СКУД здійснюється на базі наступних технологій:

- двофакторна автентифікація (2FA);
- автентифікація за запитом (Challenge-Response);
- OTP для тимчасового доступу;
- мобільна ідентифікація з використанням OTP.

Як бачимо, одноразові паролі залишаються невід'ємною частиною двофакторної автентифікації, яка вимагає від суб'єкта доступу надання ним двох різних засобів автентифікації для підтвердження своєї особи.

Реалізація OTP базується на загальноприйнятій стандартах RFC 4226 (HOTP: An HMAC-Based One-Time Password Algorithm), RFC 6238 (TOTP: Time-Based One-Time Password Algorithm) й рекомендаціях, які, в кінцевому випадку, дозволяють забезпечити сумісність та надійність різних систем.

З метою досягнення універсальності підходу, а також побудови, на його основі, системи, вимоги до технологій транспортування ідентифікаційної інформації не висувають, оскільки далеко не всі відомі рішення забезпечують безпеку переданих даних. Усе це спонукає до розроблення такого підходу, який дав би змогу застосувати механізм посиленої автентифікації, що дозволить захистити передані дані від можливої крадіжки паролів зловмисником. За умови використання технології OTP, за основу секретного ключа, рекомендується застосовувати такі компоненти:

- числове значення графічного пароля для запуску програми;
- пара ключів (масив вихідних параметрів пристрою, які будуть опитуватись під час кожної генерації тимчасового пароля);
- випадковий набір «біт», який зберігається в прихованій області пам'яті пристрою.

З цих компонентів обчислюється хеш-функція, а з отриманого значення, відповідно до обраного алгоритму шифрування, формується секретний ключ.

Реалізація схеми генерування секретного ключа та алгоритмів автентифікації на основі таких технологій передавання даних, як QR-коди та NFC-мітки також вважаються перспективними підходами до побудови безпечних та зручних систем автентифікації. Проте, безпека цих схем критично залежить від надійності генерування та захисту секретного ключа як на етапі його створення/зберігання, так і захищеності самого процесу передачі даних через QR-код або NFC-мітку від можливого перехоплення або підміни.

Використання ж OTP значно знижує ризик несанкціонованого доступу. Цей підхід базується на криптографічних алгоритмах та спільному секретному ключі й забезпечує високий рівень безпеки при відносно невеликих обчислювальних витратах.

Впровадження у СКУД схем автентифікації на основі OTP є важливим кроком у забезпеченні конфіденційності та цілісності інформації, особливо в умовах зростання кіберзагроз. Подальший розвиток та стандартизація технологій OTP сприятиме їх широкому застосуванню в різноманітних системах та сервісах.