Tokens

A security token is a physical or digital device that provides two-factor authentication (2FA) for a user to prove their identity in a login process. It is typically used as a form of identification for physical access or as a method of computer system access. The token can be an item or a card that displays or contains security information about a user and can be verified by the system.

Security tokens can be used in place of, or in addition to, traditional passwords. They are most commonly used to access computer networks but also can secure physical access to buildings and act as electronic signatures for documents.

How do security tokens work?

A security token provides authentication for accessing a system through any device that generates a password. This can include a smart card, a Universal Serial Bus key, a mobile device or a radio frequency identification card. The device generates a new password every time it is used, so a security token can be used to log in to a computer or virtual private network by typing the password generated by the token into the prompt.

Security token technology is based on the use of a device that generates a random number, encrypts it and sends it to a server with user authentication information. The server then sends back an encrypted response that can only be decrypted by the device. The device is reused for every authentication, so the server does not have to store any username or password information, with the intent of making the system less vulnerable to hacking.

Types of security tokens

Multiple types of security tokens are used to secure a variety of assets and applications. These include the following:

One-time passwords (OTPs). A form of digital security token, OTPs are valid for only one login session, meaning they are used once and never again. After the initial use, the authentication server is notified that the OTP should not be reused. OTPs are typically generated using a cryptographic algorithm from a shared secret key composed of two unique and random data elements. One element is a random session identifier, and the other is a secret key.

Disconnected tokens. This is a form of digital security token that does not connect physically or logically to a computer. The device may generate an OTP or other credentials. A desktop application that sends a text message to a cellphone, which the user must input in the login, is using a disconnected token.

Connected tokens. A connected token is a physical object that connects directly to a computer or sensor. The device reads the connected token and grants or denies access. YubiKey is an example of a connected token.

Contactless tokens. Contactless tokens form a logical connection with a computer without requiring a physical connection. These tokens connect to the system wirelessly and grant or deny access through that connection. For example, Bluetooth is often used as a method for establishing a connection with a contactless token.

Single sign-on (SSO) software tokens. SSO software tokens store digital information, such as a username or password. They enable people who use multiple computer systems and multiple network services to log in to each system without having to remember multiple usernames and passwords.

Programmable tokens. A programmable security token repeatedly generates a unique code valid for a specified time frame, often 30 seconds, to provide user access. For example, Amazon Web Services Security Token Service is an application that generates 2FA codes required for information technology administrators to access some AWS cloud resources.

Security token advantages

While it's true that passwords and user IDs are still the most widely used form of authentication, security tokens are a more secure option for protecting networks and digital systems. The trouble with passwords and user IDs is that they are not always secure. Threat actors continue to refine methods and tools for password cracking, making passwords vulnerable. Password data may also be accessed or stolen in a data breach. In addition, passwords are often easy to guess, usually because they are based on easily discoverable personal information.

Security tokens, on the other hand, use a physical or digital identifier unique to the user. Most forms are relatively easy to use and convenient.

Security token vulnerabilities

While security tokens offer a variety of advantages to users and organizations, they can introduce disadvantages as well. The main disadvantage of physical security tokens is that they are subject to loss and theft. For example, a security token could be lost while traveling or stolen by an unauthorized party. If a security token is lost or stolen, it must be deactivated and replaced. In the meantime, an unauthorized user in possession of the token may be able to access privileged information and systems.

References

<https://www.techtarget.com/searchsecurity/definition/security-token>