HTTP cookies are a special type of Magic Cookie and are used by server-side web applications to store and retrieve long-term information on the client side.

The security of an authentication cookie generally depends on the security of the site that issues it, on the user's web browser, and depends on whether the cookie is encrypted or not. Security vulnerabilities can allow hackers to read cookie data, which could be used to gain access to user data, or to gain access (with user credentials), to the website to which the cookie belongs. Cookies are commonly used to store users' browsing searches; this sensitive data can be a potential threat to user privacy.

The cookies can be used to monitor internet browsing, which is why they become the subject of discussion regarding the right to privacy. They have also been criticized because they are not always able to identify the user accurately, and also because they can potentially be the subject of cyber attacks.

The cookies stored on the user's computer contain information that allows applications to authenticate the userID, monitor user behavior and customize the contents of a site.

```
[SERVER] <——-> [BROWSER]
               I
               I
          [ATTACKER]
```

A cookie can be stolen from another computer intercepted from the network. The traffic of a network can be captured and read by a computer connected to a different network, compared to that of the sender and recipient (in particular when connected to an unencrypted WI-FI network. This traffic can allow attackers to read communications from other network users.