Single Sign-On

This presentation is part of the Authentication Overview Self-Study Course.

Transcript

Being one of the key features of identity management systems, Single Sign-On (or SSO) is often used interchangeably with EIM. Single Sign-On frameworks provide two advantages:

1. Access protection for any enterprise application
2. Ease of logging in once and having access to most enterprise application without being challenged again. SSO frameworks come with the infrastructure necessary to secure Web, J2EE and legacy based applications.

Web Access Management solutions (a.k.a. Web-SSO) typically use a web server plug-in to intercept access to web resources. The first time a user accesses a protected resource, they challenge the user to enter their SSO login credentials. Once the user has been authenticated, credentials are stored in session cookies. Protected applications read the credentials from the respective cookie.

Enterprise single sign-on (or E-SSO) – also called legacy single sign-on – occurs after primary user authentication and intercepts login prompts presented by mainframe applications automatically filling in fields such as a login ID or password. Enterprise single sign-on systems allow for interoperability with applications that are unable to externalize user authentication, essentially through "screen scraping" technology.