Home About Center for Secure Design Events Resources

Press

Authorize after you authenticate

While it is extremely important to assess a user's identity prior to allowing them to use some systems or conduct certain actions, knowing the user's identity may not be sufficient before deciding to allow or disallow the user to perform certain actions. For instance, once an automatic teller machine (ATM) authenticates a user via something they have (a debit card), and something they know (a PIN), that does not necessarily mean that user is allowed to withdraw an arbitrary amount of cash from their account. Most users may be authorized to withdraw up to a certain limit per day, or to conduct certain actions (view balance) but not others (transfer funds outside the bank) from the ATM.

Authorization should be conducted as an explicit check, and as necessary even after an initial authentication has been completed. Authorization depends not only on the privileges associated with an authenticated user, but also on the context of the request. The time of the request and the location of the requesting user may both need to be taken into account.

Sometimes a user's authorization for a system or service needs to be revoked, for example, when an employee leaves a company. If the authorization mechanism fails to allow for such revocation, the system is vulnerable to abuse by authenticated users exercising out-of-date authorizations.

For particularly sensitive operations, authorization may need to invoke authentication. Although authorization begins only after authentication has occurred, this requirement is not circular. Authentication is not binary — users may be required to present minimal (e.g. password) or more substantial (e.g. biometric or token-based) evidence of their identity, and authentication in most systems is not continuous — a user may authenticate, but walk away from the device or hand it to someone else. Hence authorization of a specially sensitive operation (for example, transferring a sum of money larger than a designated threshhold) may require a re-authentication or a

Always consider the users

Understand how integrating external components changes your attack surface

Be flexible when considering future changes to objects and actors

Get Involved

higher level of authentication. Some policies require two people to authorize critical transactions ("two-person rule"). In such cases, it is important to assure that the two individuals are indeed distinct; authentication by password is insufficient for this purpose.

Finally, just as a common infrastructure (e.g., system library or back end) should be responsible for authenticating users, so too should common infrastructure be re-used for conducting authorization checks.

Home | Sitemap | Contact Cyber Security | Accessibility | Privacy & Opting Out of Cookies | Terms & Conditions | Nondiscrimination Policy