Alternative Strategies When Multi-Factor Tokens Are Not Available

Alternative Strategies When Multi-Factor Tokens Are Not Available

Multi-factor authentication greatly increases the security of authentication events. It can mitigate the risk of phishing and password cracking attacks, significantly reducing the probability of identity theft, unauthorized transactions, and illegitimate release of sensitive institutional information. A requirement for multi-factor authentication, however, also carries the risk of preventing completely valid transactions when people do not have access to their second-factor tokens.

The causes of this vary. Tokens may be lost, stolen, forgotten elsewhere, or broken. While we often focus on the threat of stolen tokens, anecdotal information indicates that broken tokens (dead batteries, run through the washing machine, *etc*.) are the most common cause.

The impact of this risk may be small ("I can't read my mail until I get home, because I forgot my cell phone") or large ("Professor Smyth's $10M grant proposal for a special-purpose supercomputer to study climate change arrived late, and was rejected, because her grant administrator left his PKI token at the gym"), but the risk to business continuity should always be considered when deploying multi-factor authentication. This document presents potential strategies for mitigating this risk.

Issues

Multi-factor authentication is typically deployed for one or both of the following reasons:

1. It is provided on an opt-in basis to users for their benefit, enabling them to increase their protection against impersonation by someone else. An increasing number of online service providers like Google and LastPass provide this option for their users. Google and LastPass do not have an overriding concern that their services will be used by people utilizing weaker authentication, but they want their users to have that added security if they want it.
2. It is required by a service provider to access their service to mitigate the risk that their users are impersonated. The requirement may either cover all access to the service, or only to certain sensitive functions. For example, a student may be able to add and drop their own courses in the student information system using only a password, but instructors may be required to use multi-factor authentication in order to enter grades. In this case, the service provider definitely does have an interest in users utilizing strong authentication; their users do not have a choice.

Of course, multi-factor authentication may be deployed for a combination of both reasons, particularly when it is part of a single sign-on system used by multiple services with varying requirements for authentication strength.

When multi-factor authentication is deployed on an opt-in basis, alternative strategies must meet user expectations for security and convenience. Service providers do not need to know when alternative strategies are invoked; they don't even necessarily need to know that those strategies exist or any details about how they they can be used.

When multi-factor authentication is deployed to mitigate a service provider's risk of impersonated users, alternative strategies must balance the risk of impersonation with the risk to business continuity (as well as the convenience and security of the service provider's users).

A special case of service provider required multi-factor authentication occurs in identity federations. In federations, identity providers do not typically adjust their practices to address the risk profiles of individual service providers; it just doesn't scale. Instead, the federation defines common, canonical risk profiles for service providers and establishes formal and/or informal assurance profiles for identity providers to mitigate those risk profiles. In this case, alternative strategies become part of the assurance profiles, and service providers select assurance profiles that meet their needs.

Example Strategies

Opt-In Multi-Factor Authentication

As described above, alternative strategies for opt-in multi-factor authentication need meet only the expectations of end-users for security and convenience. The following are examples of such strategies:

- **Pre-Registered Proxies.** At the time a person opts to require multi-factor authentication for their access to services, he provides a list of other people (proxies) who are authorized to remove that requirement. If the user's token is later lost, stolen, or simply left elsewhere, he can contact one of his proxies to remove the multi-factor requirement.
- **Single-Use Passwords.** At the time a person opts to require multi-factor authentication, she is given a list of single-use passwords that can be used to override her multi-factor requirement for a single session.

Service Provider Required Multi-Factor Authentication

In this case, mitigation strategies must balance the risk of user impersonation with the risk to business continuity. The following are potential strategies:

- **Restricted but Not Denied Access.** The service provider allows the use of weaker authentication, but does not enable all capabilities for the user. This preserves security for more sensitive transactions but does not address business continuity when the more sensitive transactions are required.
- **Emergency Access for Limited Time.** Requirements for strong authentication can be relaxed in times of emergency. Assuming there is a mechanism for declaring an emergency, this can preserve business continuity at critical times, while limiting the duration of a security threat due to weak authentication.
- **Authorized Third Parties for Authentication.** The authentication process is structured to require the approval of an authorized third party, such as a departmental administrator, who can approve authentication for a single session without the token.

Note that the strategies for federation required multi-factor authentication can also be used here.

Federation Required Multi-Factor Authentication

In this case, alternative strategies are mutually agreed upon among the federation's identity providers and service providers.

- **Re-Registration.** Some or all of the original registration process is applied for users who will be issued replacement tokens. The re-registration process may also leverage information that is collected during the original registration process for this purpose.
- **Authorized Third Parties for Re-Registration.** A trusted third party can be used to validate a person's identity as part of a re-registration process. These trusted third parties might be contracted companies or people in the workplace, such as departmental administrators, who have been authorized to perform this function.

Note that the strategies for service provider required multi-factor authentication may also be used here.