FIGURE 6-3. Authorizing access to the Facebook Platform API

However, some applications do not easily lend themselves to this second "redirect" step. "Desktop"-style applications or applications based on a device such as a mobile phone or built into a browser can be quite useful as well. In this case, we employ a slightly different scheme using a secondary authorization token. A token is requested by an application through the API, passed to Facebook on the first login, and then exchanged by the application for a session key and a per-session secret after on-site user authentication.

Creating a Social Data Query Service

We have expanded our internal libraries to the outside world by creating a web service with a user-controlled authentication handshake. With this simple change, Facebook's social data now drives any other application stack its users choose to authorize, creating new relations within that application's data through a universally interesting social context.

As seamless as this data exchange becomes in the mind of the user, the developer consuming these platform APIs knows the data sets are very distinct. The pattern the developer uses to access his own data is quite different than the one used to get Facebook's. For one, Facebook's data lives on the other side of an HTTP request, and making these method calls across many