Linux Invention

Contact Information

Mr Rich Maggiani; rich.maggiani@solari.net

Solari Communication
137 Lost Nation, Suite 14
Essex, Vermont 05452
United States of America
802.879.9330

Title of the Invention

A Single Login Process for External, Internet-based Online Services

Description of the Invention

Many computer services are available online through the Internet, requiring various levels of security and login information. This invention describes how Linux provides for a single login process by tracking this login information to external services and saving it. A user need only securely log in to their personal computer. Once a secure login occurs, Linux uses the saved login information to automatically log the user into Internet sites.

Problem or Opportunity

Many computer services are available online through the Internet, requiring various levels of security. Some online computer services (such as banking, investment, and financial services) require high levels of security. Others (such as online news or informational services) require simply an acknowledgement of the user's identify. Nonetheless, all of these services require login information: usually only a user ID and password; some, however, do require a more detailed level of security before allowing a user to access the service.

Since creating, maintaining, and—especially—remembering all these disparate user IDs and passwords is just too cumbersome, users fall back on using the same user ID and password for every site. While some online services force a specific format for their user IDs and passwords, users tend to respond to this attempt at increased security by simply modifying their familiar user ID and password as little as possible. In the end, almost all users fail miserably at maintaining a unique and difficult-to-crack set of user IDs and passwords. All of this, of course, makes an easy task for an identity thief to access this myriad of information about their victim.

Detailed Description of the Invention

To combat this problem, Linux creates and maintains a locally located, password protected login database that contains all of this disparate login information. When a user must log in to a particular online service, Linux gets involved. Linux sees what the online service is, finds the record for that service in its login database, then simply populates the login fields with that stored information. The user need only click the appropriate button or press the Enter key to gain access to the online service.

To ensure the security of this system, a user must enable the login process for their personal computer (which can also include a biometric sensor to increase security), thus informing Linux that this computer session is secure. Once a user knows that Linux will take care of remembering all user IDs and passwords, the user can then create unique user IDs and strong, difficult-to-crack passwords for each online service.

The Linux online database for this stored login information is text-based. Users can also gain access to their Linux login database to review the user IDs and passwords already created, and to edit them if necessary.

This method does require some user diligence to ensure a high-degree of security. A user must never leave their computer unattended, and always log out of their computer whenever they physically leave it or during any other times when a security breach might be a possibility.

Figure 1 depicts a high-level version of this invention.

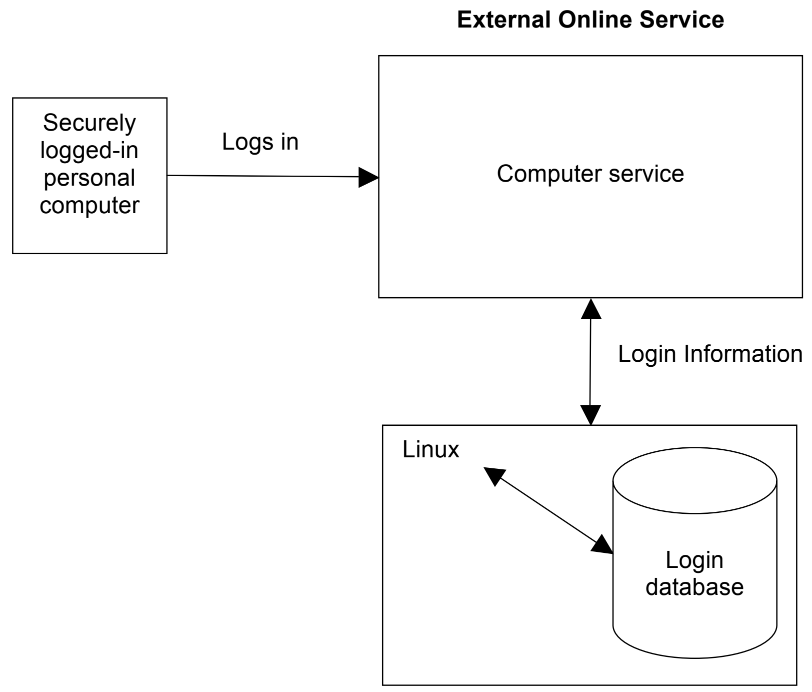

Figure 1. *Process for an automatic login to external computer services*

This process starts with Linux maintaining a login database.

In step 1, Linux collects a list of users and associated login information with accounts on the personal computer on which it is operating. Linux then stores this information in its login database for external computer services.

In step 2, a user securely logs in to the personal computer using their main login information. This login information can also contain a method of physically identifying the user (such as sensing biometric information) as well as the basic user identifier and password.

In decision step 3, Linux attempts to authenticate the user by referencing its login database (who has not set their login options to automatically log them in). If the user's information is found, the method proceeds to step 4; if no, the method returns to step 2 to await the user to securely log in to this personal computer. If the user automatically logs in, then Linux does not process any login attempts to external services.

In step 4, the user accesses an external computer service that requires unique login information.

In decision step 5, Linux determines if this user has been authenticated in step 3. If yes, the method proceeds to step 6; if no, the method returns to step 2 to await the user to securely log in to this computer.

In decision step 6, Linux determines if this user has already created login information for this external computer service. (In other words, has this user ever accessed this computer service before.) If yes, the method proceeds to step 8; if no, the method continues with step 7.

In step 7, Linux stores in its login database (in the form of a cookie), the login information this user enters for the external computer service. The method ends.

In step 8, Linux completes the login information for this computer service, populating the login fields with information from its login database, automatically logging in the user. This step happens so quickly that it is essentially invisible to the user.

The method ends.

Figure 2 depicts a flowchart of how Linux provides for a single login process by automatically logging in a user to multiple online computer services without compromising security.

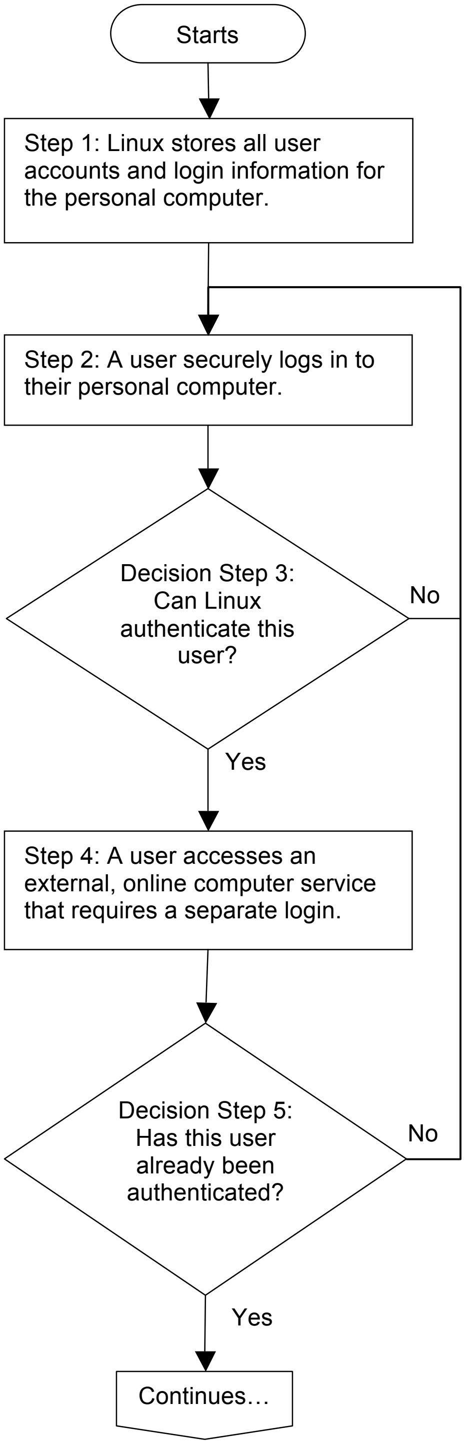
Starts
Step 1: Linux stores all user accounts and login information for the personal computer.
Step 2: A user securely logs in to their personal computer.
Decision Step 3: Can Linux authenticate this user?
No
Yes
Step 4: A user accesses an external, online computer service that requires a separate login.
Decision Step 5: Has this user already been authenticated?
No
Yes
Continues…

Figure 2. *Flowchart of single external login process (part 1 of 2)*

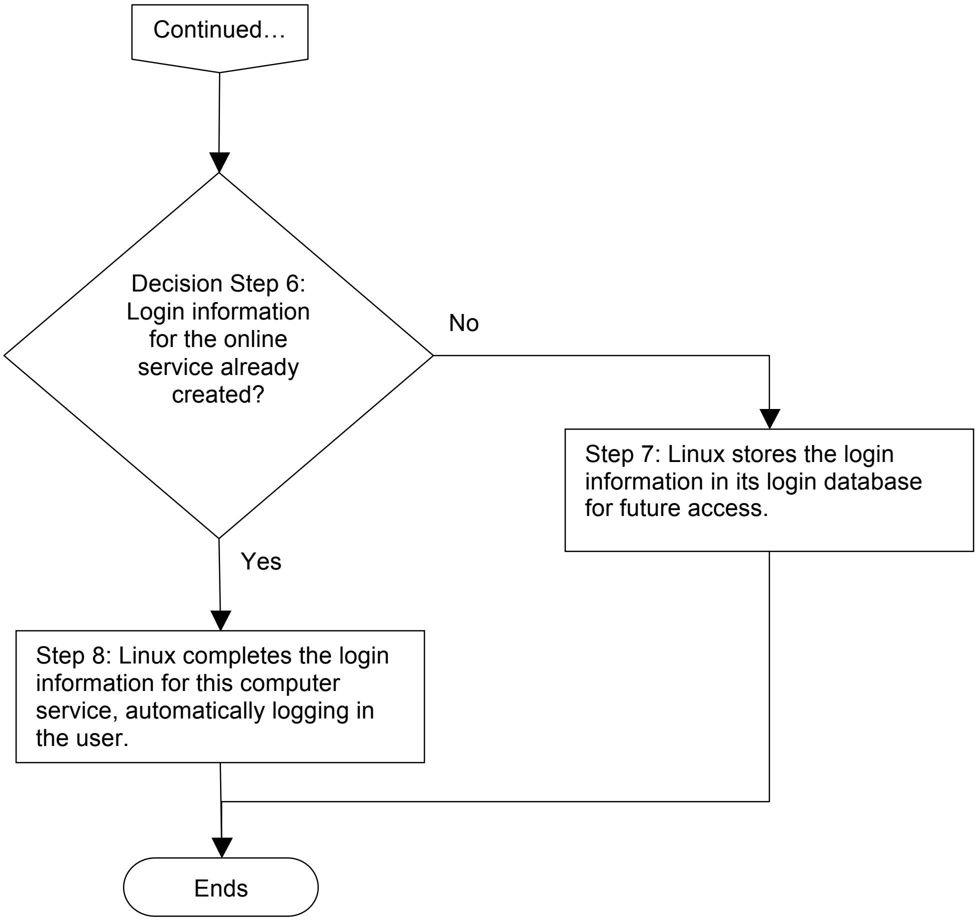
Continued…
Decision Step 6: Login information for the online service already created?
No
Step 7: Linux stores the login information in its login database for future access.
Yes
Step 8: Linux completes the login information for this computer service, automatically logging in the user.
Ends

Figure 2. *Flowchart of single external login process (part 2 of 2)*