6.170 Laboratory in Software Engineering
Fall 2005
Final Project Amendment: RSS Client
Due: See **UPDATED SCHEDULE**

Note: There has been a change in schedule. **We have moved the final deadline to 9:00 AM, December 12th**. Please use this time to ensure that your design is thoroughly tested, and to make sure that your interface is as clean and usable as imaginable.

Contents:

Content Censorship

The Internet can be a source of incalculable amounts of information covering every imaginable subject, and, in essence, an RSS client bundles that information like a newspaper and delivers it at your door. For parents, the ease with which children can access this information can be a worrisome matter. Individual families often make far different choices than various news sources when deciding what content should be viewed by young children. Because of this, many Internet applications (such as web browsers) give users the *option* of specifying content that cannot be viewed unless a password is entered into the application.

The RSS Client you have designed so far allows absolutely any feed to be added and read as long as the feed's reference URL contains a legal RSS1, RSS2, or Atom file. We would like you to add a feature that allows a user to specify types of feeds and articles that cannot be subscribed to or viewed without a password.

Access Control

The basic requirement of this feature is to allow the user to define a single profile that contains a **banned domain** list as well as a **banned keyword** list that is used to censor content. The following RSS client operations must be password protected by a single master password:

- Adding a feed with a URL from the banned domains list.
- Viewing an article from the banned domains list or one which contains any of the banned keywords in its title, summary, or article text.
- Resetting the master password.

You should allow the censorship option to be turned off and on easily, however to turn off censorship, the master password must be entered. Once censorship has been turned off, all of the previously blocked articles and feeds should be viewable again. Further, the

master password must persist between executions of the application, and upon startup the application must begin with censorship turned on (possibly asking for a password).

Different access control mechanisms are acceptable, as long as they provide roughly the same level of parameterization (or more) for what will be censored. Please read about More Advanced Content Censorship Mechanisms for more information.

User Interface Considerations

A number of considerations should be taken into account when implementing a user interface that allows such censorship. Below is a list of key points to keep mind.

- If a banned keyword is located in either the title, the summary, or the full article text, then all three of these items (title/summary/article) must be masked in your display somehow. That is, it is unacceptable to mask only the single keyword. (The idea here is that we don't want any of the associated content to leak out.)
- Requiring the user to enter their password with every click is unacceptably irritating, however, allowing the password to persist for the entire lifetime of the application can be an equally unacceptable security concern. Find a happy medium that maintains some security guarantees, but is not overly bothersome to the user.
- While censorship is enabled, you may not want to display channels, feeds, or articles that cannot be viewed. Alternatively, you may want to make this fact readily apparent to the user.
- Similarly, while censorship is enabled, you may not want searches to return matches that cannot be viewed. Think about different ways of integrating password protection with search and choose what you think is best.

Security

To ensure the functionality of this protection scheme, the master password must be securely stored to some configuration file on disk. To accomplish this please use a standard, cryptographically secure method to store the "hidden" password on disk and to compare user input with the "hidden" password during verification.

More Advanced Content Censorship Mechanisms

There are certainly more advanced methods of content censorship than simply "blacklisting" keywords and domains as we've described above. If your group would like to implement a more sophisticated method of filtering content, or would like to add the functionality for multiple profiles you are welcome to. Your method need not exactly implement a list of banned keywords and a list of banned domains, but must provide a similar or better level of parameterization for what will be censored. **If you want to try something different, you must talk with your TA to see if it is acceptable.**

As a final note, the censorship method described above is still not sufficient since there is no requirement to mask or hide inappropriate article data stored on disk in the cache. Someone who does not know the password could easily read out the data in the cache themselves and find all of the censored information. Further, an attacker might be able to simply rewrite the value of the "hidden" password wherever it is stored on disk. A more secure application would encrypt banned articles (and possibly any other critical user

state such as the list of subscribed feeds, etc.) whenever information is stored to disk. However, this would require a considerable amount of work and is therefore not required.

Clarifications and Errata

No clarifications or errata have been provided.