APPENDIX E

Specific Recommendations to Vendors

This chapter is a an explicit list of recommendations for vendors of computer operating systems and webmail services.

E.1 Recommendations for Desktop Software

The operating system:

- Make Windows `FORMAT.EXE`, the Apple Disk Utility, and the Unix `newfs` commands actually overwrite every block of the media when an initialization is performed. Provide a "quick" option which only writes down the file system structures for people who are in a rush but do not make this the default. Make it clear that using the "quick" feature means that data will not be overwritten. People who are not in a rush deserve to have their media properly sanitized when they format it.
- Implement a `sanitize(fd)` system call that works with the file system to overwrite the contents of an opened file, even on a journaling file system.
- Implement COMPLETE DELETE for the unlink() or DeleteFile() system calls along the lines discussed in Chapter 3.
- For password fields: if the password that's typed doesn't match the password on file, the software should try swapping the case and seeing if it works. If it works, then the user had the **Caps Lock** key on.

  Don't display an annoying pop-up that says "Do you have the Caps Lock key on?" Of course the user has the caps lock key on. Of course the user doesn't realize it. Accept the password and reset the Caps Lock flag; standard PC hardware lets the operating system perform this function.

Some password fields have been modified to indicate the status of the **Caps Lock** key. This is a useful indicator that should be encouraged.

- Provide easy-to-understand and standardized tools for viewing certificates.

Web Browsers:

- Unify the web browser cache, history, and cookies as discussed in Chapter 4.1. When the last reference to a web page from the history or bookmarks is deleted, delete the pages in the cache and any saved cookies that correspond to the site.
- Provide an easy-to-find "reset browser" feature that sets a timer, then performs a Reset to Installation.

Mail clients:

- Provide a standard mechanism whereby "sent" email is actually queued for delivery, during which time it may be edited or moved to a "draft" folder rather than having it being sent.
- Do not allow users to check boxes such as "Sign" if there is no S/MIME private key on file.
- Change the handling of sealed S/MIME mail so that mail that is downloaded by POP is automatically unsealed before it is stored. This reduces the penality for losing one's key. Users who wish to have their mail kept sealed can use a cryptographic file system to protect all of their mail.
- For mail on IMAP servers, mail clients should have the capability to automatically re-seal mail with new keys to allow for key migration.
- Develop a one-click support for mail clients so that they can automatically obtain email-only certificates from CAs that wish to offer them for free.
- Increase the salience of icons that indicate if a message was signed or sealed. Decrease the prominence of warnings that say signatures did not verify, since message signatures are frequently using today's email systems.
- (For Microsoft:) Correct the bug in Microsoft's S/MIME library which prevents Outlook and Outlook Express from opening S/MIME-signed messages that consist of a non-text attachment but no body.
- (For Microsoft:) Correct the handling of the "sign all messages" option in Outlook and Outlook Express. Currently both programs have an option to sign or not sign all outgoing mail, but this default isn't honored under some circumstances.

E.2 Recommendations for Organizations that Send Bulk Email

- Sign all outgoing email that is automatically generated and not designed to be replied to. This includes all newsletters, bulletins, and other email announcements originating from email addresses such as `noreply@adc.apple.com` and `do_not_reply@microsoft.com`.

E.3 Recommendations for Webmail Providers

- Verify the signatures of S/MIME-signed mail so that these messages are validated and shown in a distinctive manner.
- If this is too complicated, simply suppress the display of S/MIME attachments.
- Give users a simple option that will cause the webmail system to obtain a Digital IDs and use them to automatically sign all outgoing mail.