

5

solely for access by particular applications. In this embodiment, the kind of allowed access may vary for each area of protected storage, and may include, read, write, read once, write once, etc. In one embodiment, the information may be designated as read once, auto-erase, so that the data retrieved is then immediately erased from the protected storage. This adds another dimension of security to the protected storage. The Pre-OS application may check that the message placed by an OS-Present application into the protected storage and retrieved by the Pre-OS application was authentic, unaltered, and subsequently "trusted." Based on the information retrieved, the Pre-OS application may take any requested or appropriate actions.

The kind of information written to and retrieved from the protected storage will vary based on the purpose and use of the information, and the writer and recipient of the information. The type of information that needs to go into the special protected storage "cell/slot" is determined by the applications that will consume it. But there will be common pieces of information that may be required. Information that may be stored in the protected storage or may be made available by the protected storage include, for example: a requested action data specifying what action is being requested; an identity data identifying the user or application program that is requesting an action; an identity credential data which may attest to the identity of the user or application program; a policy data reporting the policy from the requestor's perspective; a policy credential data that validates the requestor's policy; a completed action data stating what action(s) has/have been accomplished; a miscellaneous-opaque data that may be use specific and may allow for extensibility and customization; and an integrity data that may be used to ensure that a message has not been altered. In addition, various other kinds and forms of data may be accessed via the protected storage depending on the use and purpose of the data and the purpose and goal of the particular application program.

By adding protected storage to a personal computing device with Pre-OS and OS-Present application programs may access protected storage, messages may be sent from one operation space to the other. This can be very powerful as explicit security can be built into these communications that ultimately develop more trust in who is making requests and actions that are being done by proxy. In one embodiment, if a protected storage implementation does not provide sufficient protection to ensure that only authorized entities can access a given storage location, additional fields may be added for use of digital signature or encryption techniques. In this embodiment, the entire contents of a given storage location, such as a set of cells or slots, may be "wrapped" with a digital signature, encryption or both. Any well known digital signature or encryption techniques may be employed.

In the foregoing specification, the invention has been described with reference to specific embodiments thereof. It will, however, be evident that various modifications and changes can be made thereto without departing from the broader spirit and scope of the invention as set forth in the appended claims. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

What is claimed is:

1. A computing device comprising:

- a host processor coupled to a bus to execute a pre-operating system software program and an operating system present software program;
- a non-volatile memory coupled to the host processor, the non-volatile memory to store the pre-operating system software program;

6

a disk memory coupled to the bus, the disk memory to store the operating system present software program and an operating system; and

a protected storage medium coupled to the host processor, the protected storage medium to enable secure exchange of a protected message between the pre-operating system software program and the operating system present software program via the protected storage medium.

2. The computing device of claim 1 further comprising: a first interface to provide the pre-operating system software program access to the protected storage medium; and

a second interface to provide the operating system present software program access to the protected storage medium.

3. The computing device of claim 1 wherein the protected storage medium is a non-volatile re-writable memory device.

4. The computing device of claim 1 wherein the protected message is exchanged during boot-up of the computing device.

5. The computing device of claim 1 wherein the protected message includes user authentication information.

6. The computing device of claim 1 wherein the protected storage medium is further configured to enable the operating system present software program to securely store the protected message for the pre-operating system software program subsequent to boot-up of the computing device.

7. The computing device of claim 6 wherein the protected message is retrieved by the pre-operating system software program during reboot of the computing device.

8. A method comprising:

accessing, by a host processor executed pre-operating system software program, a protected storage medium;

performing, by the pre-operating system software program a boot-up procedure according to a protected message stored within the protected, storage medium by an operating system present software program; and

storing, by the pre-operating system software program, boot-up information within the protected storage medium for the operating system present software program according to the protected message.

9. The method of claim 8 wherein the storing comprises: formatting user authentication information obtained during the boot-up procedure according to the protected message; and

securely storing the formatted user authentication information within the protected storage medium.

10. The method of claim 8 wherein accessing comprises: detecting the protected message within protected storage medium;

performing, by the pre-operating system software program, an authentication procedure of the protected message from the protected storage medium; and discarding the protected message if the authentication procedure fails.

11. The method of claim 8 wherein the storing the boot-up information comprises:

encrypting the boot-up information; and wrapping the encrypted boot-up information within a digital signature of the preoperating system program.

12. The method of claim 8 further comprising: enabling the operating system present software program to perform secure storage of a protected request for the