SYSTEM AND METHOD FOR PROTECTED OPERATING SYSTEM BOOT USING STATE VALIDATION

ABSTRACT OF THE DISCLOSURE

A mechanism for protected operating system boot that prevents rogue components from being loaded with the operating system, and thus prevents divulgence of the system key under inappropriate circumstances. After a portion of the machine startup procedure has occurred, the operating system loader is run, the loader is validated, and a correct machine state is either verified to exist and/or created. Once the loader has been verified to be a legitimate loader, and the machine state under which it is running is verified to be correct, the loader's future behavior is known to protect against the loading of rogue components that could cause divulgence of the system key. With the loader's behavior being known to be safe for the system key, the validator may unseal the system key and provides it to the loader.

Fig. 4