October 03, 2018

SMART DISINFECTION MODE

HP INC

Smart Disinfection Mode

Abstract: A technique that allows computers used in healthcare delivery to be disinfected without shutting down the computer or putting it into sleep mode locks the keyboard, touch pad and touch panel of a computer automatically when a user performs disinfection and unlocks them after disinfection is completed.

This disclosure relates to the field of computers.

A technique is disclosed that allows computers used in healthcare delivery to be disinfected without shutting down the computer or putting it into sleep mode.

A key differentiator for computers used in healthcare delivery applications, particularly portable computers such as laptops, notebooks, and tablets, is the ability for clinicians (nurses and physicians) to disinfect the entire notebook. The primary existing form of disinfection is via prepackaged sanitary wipes made specifically for hospitals. Most hospital procedures require clinicians to cleanse the notebook after any patient encounter. Therefore, as nurses/physicians perform their rounds, after each patient visit they need to be able to quickly wipe down the notebook on-the-go as they walk towards the next patient room. However, the data can be undesirably impacted if the keyboard or touch panel still work during disinfection.

To avoid this situation, the computer must be shut down, or at least put into sleep mode, before disinfection is performed, and then awakened or restarted afterwards. The delay is doing this is costly in a healthcare delivery setting.

According to the present disclosure, a Smart Disinfection Mode (SDM) application locks the keyboard, touch pad and touch panel of a computer automatically when nurses or physicians perform disinfection, and unlocks them after disinfection.

In operation, at step 1, a nurse/physician executes the SDM application under control of the operating system. At step 2, the computer waits to detect the disinfection. In one example, this module may be an embedded controller (EC). At step 3, the EC detects disinfection occurring. In one example, the occurrence of disinfection is detected by determining that multiple keys have been pressed within a short time. For example, 10 keys that are pressed in 500ms. In addition, it is determined that these keys are sequentially pressed and released in the same direction relative to the keyboard; for example, from left to right, right to left, top to bottom, or bottom to top of the keyboard.

At step 4, once disinfection is detected, the keyboard, touch pad, and touch panel are locked in order to prevent inadvertent operation of the keyboard and touch pad, and the user is informed by the display of a message on the computer such as “Disinfection Mode”. A timer is also displayed, so that the user knows how much time remains to complete the disinfection operation before the user input features of the computer are re-enabled. When the timer times out, at step 5 the user is notified by another message, and the keyboard, touch pad, and touch panel are unlocked and the computer is once again fully functional.

In an alternative approach, rather than unlock the keyboard, touch pad, and touch panel based on expiration of a timer, detection of a particular combination or sequence of keys being pressed can be used. This adds a step that the user must perform, but can be useful

if the time to disinfect the computer can vary from user to user or from environment to environment.

The disclosed technique advantageously reduces the time and effort for nurses/physicians to perform disinfection of a healthcare computer. It is implemented in software, and thus does not add any hardware cost to the computer.

Disclosed by Yi-Fan Hsia, Pinky Chen, Neil C. Cortez, Vincent Feng, and Patrick Chen, HP Inc.