April 2023

QuickPass for TSA Security

HP INC

QuickPass for TSA Security

Abstract: Techniques for ensuring that a portable computer has not been tampered with can be adopted by TSA to improve screening point throughput for travelers who do not belong to a safe traveler program.

This disclosure relates to the field of airline travel.

Techniques are disclosed that allow laptop and notebook computer owners who do not have TSA safe traveler status to leave their devices in their carry-on bags when going through a security screening checkpoint at airports.

Travelers can pay and interview for certain “safe traveler” status/services, such as for example TSA Precheck, to expedite their screening at airports. When passing through a TSA checkpoint at the airport, travelers with a safe traveler status are allowed to leave their personal electronic devices in their bags at the security checkpoint. However, travelers without a safe traveler status must remove personal electronic devices larger than a cell phone from their carry-on bags and place them in a bin with nothing placed on or under them for X-ray screening or, in some cases, hand searches. This is inconvenient to the traveler who must remove the computer and then repack their bag after passing through the checkpoint. It also slows down the throughput of travelers at security checkpoints, leading to excessive delays and, in some cases, travelers missing their flights.

According to the present disclosure, a first technique uses RFID signals and electronic tamper lock technology to assure officials that the electronic devices are genuine and free of any dangerous modification. While the computer is on, or on standby, it detects the X-ray at the checkpoint using a dosimeter. The computer then assesses whether it has been tampered with. It then emits an RF signal to a TSA reader indicating whether or not the laptop is free of dangerous modification. During this process, the laptop generates a one-time security token including: (1) a temporary authorization key for the encrypted data; (2) the tamper lock status; and (3) flight and user identification information for government use. The TSA backend then verifies the key and reads the information. Upon receiving the safe signal, the reader then marks the traveler as a subset of the “safe traveler” status process, allowing them to leave their laptop in their bag.

Alternatively, a second technique utilizes a materials-based tamper-aware mechanism built into the chassis of the computer. In one example, the mechanism is a high-density metal wire component with thin ends, in a form of straight wire, or wire forming a certain pattern per design, which will deform or break with excessive force. In another example, the mechanism is a ceramic component with a thin portion that will break if excessive force is applied to it. These parts cannot be restored or replaced by end users. Damage to these components caused by tampering is clearly seen by X-ray even when the computer remains in a carry-on bag. Upon ensuring untampered status of the computer by X-ray, the scanner will then mark the traveler as a subset of the “safe traveler” status process, allowing them to leave their computer in their bag.

These operations are performed before the traveler passes through the security scanner. He or she still needs to remove their belts, shoes, etc. as usual when passing through the checkpoint.

The disclosed techniques advantageously allow users to avoid the hassle of fumbling around at a security checkpoint to find their computer, remove it from their carry-on bag, place it in a separate tray, and resituate it back into their carry-on bag after the x-ray scanning process has been performed. It saves travelers money by not requiring them to join a "safe traveler" program. Standardized use of these techniques would significantly reduce the lines at the TSA checkpoints.

Disclosed by Srinath Balaraman, Jack Hui He, Sean Lin, and Edmond Xue, HP Inc.