February 20, 2019

A METHOD OF DETECTING TEMPERING ON COMPUTING DEVICES BY MONITORING ELECTRO-MAGNETIC PATTERN

HP INC

A Method of Detecting Tempering on Computing Devices by Monitoring Electro-Magnetic Pattern

Abstract

- When hardware is tampered with additional 'spying' components, local Electro-magnetic (EM) pattern will be disturbed/changed, and show a different pattern.
- The need for the detection of hardware tampering could be monitored and detected by this method outlined, through the comparison to 'ground state' of local EM field and pattern recognition, then notify administrator and/or end user.

Problems Solved

- The concern and risk of tampering on computing devices is on the rise, including servers, personal systems, and mobile devices.
- Tempered devices could be used for information theft against corporates and personnel and be harmful.
- When hardware is tampered with additional 'spying' components, local EMI pattern will be disturbed, and show different pattern.
- The need for the detection of hardware tampering could be monitored and detected by this method outlined, then notify administrator and/or end user.

Product Details

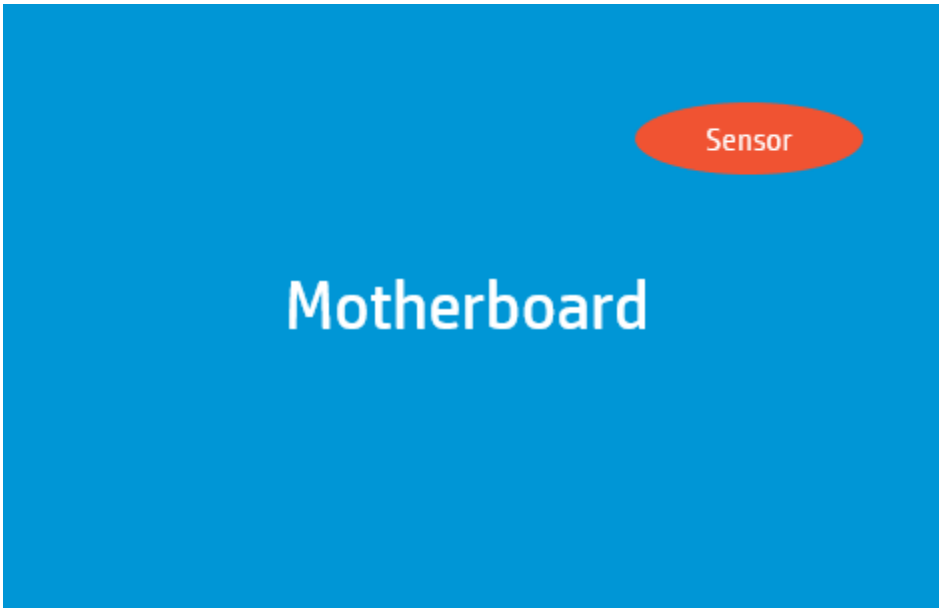
An electric device is defined to have a 'ground state' for calibration, with the exact set of software running and functions enabled, others are disabled and killed.

When the electric device is manufactured in factory, EMI pattern of a given location will be recorded, and show different pattern. of is accurately measured and calibrated to this 'ground state', with the value and 'signature pattern' written into BIOS.

At predefined interval, the system will self run into the 'ground state' and execute EM test, and generate pattern, and compare with 'signature pattern'.

When significant difference is detected through pattern recognition, system will send notification or alert to system administrator.

This can be enabled by a discrete chip embedded on the motherboard with hardware level security.



Advantage

- When hardware is tampered with additional ‘spying’ components, local EM pattern will be disturbed, and show different pattern.
- The need for the detection of hardware tampering could be monitored and detected by this method outlined, through the comparison to ‘ground state’ of local EM field and pattern recognition, then notify administrator and/or end user.

Disclosed by Hui He / Hang Yan Yuen/ Paul Mazurkiewicz, HP Inc.