CLAIMS:

1. A method for verifying system integrity of an electronic device, the method comprising:

verifying, by a verifier module provided within a secure environment in the electronic device, integrity of a scanner module provided within a normal environment in the electronic device;

generating, by the verifier module, a challenge;

transmitting the challenge from the verifier module to the scanner module provided within the normal environment in the electronic device, wherein the challenge instructs the scanner module to execute an integrity verification function in the normal environment to generate a response;

encrypting, by the scanner module, the response and transmitting the encrypted response to the verifier module; and

verifying, by the verifier module, integrity of the scanner module by decrypting the encrypted response and verifying the integrity of the scanner module if the response may be successfully decrypted, and

once the integrity of the scanner module has been verified, determining the system integrity of the electronic device by assessing the validity of the received response and performing a mitigation action if the received response is invalid.

2. The method according to claim 1, wherein the verification function comprises:

scanning a kernel code;

scanning a process list;

scanning a memory page table; or

checking a status and parameter of a kernel protection mechanism.

3. The method according to claims 1 or 2 wherein the assessing the validity of the received response comprises:

matching the response with data contained in a secure database provided in the secure environment, wherein when a match is not found, the response is determined as invalid.

4. The method according to claim 1 wherein the verifying the integrity of the scanner module provided within the normal environment comprises:

generating, by the verifier module, a verification response request and transmitting the verification response request from the verifier module to the scanner module,

wherein the verification response request instructs the scanner module to generate an encrypted verification response, and transmit the encrypted verification response to the verifier module; and

determining, by the verifier module, whether the encrypted verification response is valid, whereby in response to a determination that the response is invalid, performing the mitigation action.

5. The method according to claim 4, wherein the determining whether the encrypted verification response is valid comprises:

decrypting, by the verifier module, the encrypted verification response, whereby in response to a determination that the verification response is decrypted, matching the decrypted verification response with verification data contained in a secure database provided in the secure environment, wherein when a match is not found, the verification response is determined as invalid.

6. The method according to any one of claims 1 to 5, wherein the mitigation action comprises:

preventing execution of software modules provided in the normal environment.

7. The method according to any one of claims 1 to 6, wherein the secure environment in the electronic device comprises a secure world virtual processor for the electronic device, the normal environment in the electronic device comprises a normal world virtual processor for the electronic device, and the secure environment is hardware isolated from the normal environment.

8. The method according to any one of claims 1 to 7, further comprising:

determining whether a preset time interval has lapsed; and

repeating the method for verifying the system integrity of the electronic device when the preset time interval has lapsed.

9. A system for verifying system integrity of an electronic device, the system comprising:

a processing unit having a secure environment and a normal environment; and

a non-transitory media readable by the processing unit, the media storing instructions that when executed by the processing unit cause the processing unit to:

verify integrity of a scanner module provided within the normal environment using a verifier module provided within the secure environment;

generate a challenge using the verifier module provided within the secure environment;

transmit the challenge from the verifier module to the scanner module provided within the normal environment, wherein the challenge instructs the scanner module to execute an integrity verification function in the normal environment to generate a response;

encrypt the response using the scanner module, and transmit the encrypted response to the verifier module; and

verify an integrity of the scanner module using the verifier module by decrypting the encrypted response and verifying the integrity of the scanner module if the response may be successfully decrypted, and once the integrity of the scanner module has been verified, determine the system integrity of the electronic device by assessing the validity of the received response and perform a mitigation action if the received response is invalid.

10. The system according to claim 9, wherein the verification function comprises:

instructions for directing the processing unit to:

scan a kernel code;

scan a process list;

scan a memory page table; or

check a status and parameter of a kernel protection mechanism.

11. The system according to claims 9 or 10, wherein the instructions to assess the validity of the received response comprises:

instructions for directing the processing unit to:

match the response with data contained in a secure database provided in the secure environment, wherein when a match is not found, the response is determined as invalid.

12. The system according to claim 9 wherein the instructions to verify the integrity of the scanner module provided within the normal environment comprises:

instructions for directing the processing unit to:

generate a verification response request using the verifier module and to transmit the verification response request from the verifier module to the scanner module, wherein the verification response request instructs the scanner module to generate an encrypted verification response, and transmit the encrypted verification response to the verifier module; and

determine whether the encrypted verification response is valid using the verifier module, whereby in response to a determination that the response is invalid, to perform the mitigation action.

13. The system according to claim 12, wherein the instructions to determine if the encrypted verification response is valid comprises:

instructions for directing the processing unit to:

decrypt the encrypted verification response using the verifier module, whereby in response to a determination that the verification response is decrypted, to match the decrypted verification response with verification data contained in a secure database provided in the secure environment, wherein when a match is not found, the verification response is determined as invalid.

14. The system according to any one of claims 9 to 13, wherein the mitigation action comprises:

instructions for directing the processing unit to prevent execution of software modules provided in the normal environment.

15. The system according to any one of claims 9 to 14, wherein the secure environment in the electronic device comprises a secure world virtual processor for the electronic device, the normal environment in the electronic device comprises a normal world virtual processor for the electronic device, and the secure environment is hardware isolated from the normal environment.

16. The system according to any one of claims 9 to 15, wherein the system further comprises:

instructions for directing the processing unit to:

determine whether a preset time interval has lapsed; and

repeat the system for verifying the system integrity of the electronic device when the preset time interval has lapsed.