CLAIMS:

1. A security module comprising:

an interface configured to connect to a bus system of a host device;

a processor; and

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

capture diagnostic data transmitted through the bus system of the host device when diagnostic tests are executed by the host device during a Power-on-Reset (POR) cycle of the host device;

identify, from the captured diagnostic data, hardware components associated with the host device and retrieve databases associated with each of the identified hardware components;

acquire new data associated with a first identified hardware component from the bus system; and

determine, based on the newly acquired data and based on a retrieved database associated with the first identified hardware component, that a security violation is occurring at the first identified hardware component.

2. The security module according to claim 1 wherein the captured diagnostic data comprise addresses of the host device's main memory and wherein the first identified hardware component comprises the host device's main memory, and further comprises instructions that when executed by the processor, before the step of determining that a security violation is occurring at the first identified hardware component, cause the processor to:

generate a virtual disk based on the addresses of the host device's main memory; and

write the newly acquired data to the virtual disk as the new data is concurrently acquired from the host device's main memory.

3. The security module according to claim 2 wherein the instructions to determine that a security violation is occurring further comprises instructions that when executed by the processor cause the processor to:

identify, based on the data newly written to the virtual disk, a software application that is being loaded in the main memory of the host device;

retrieve, from the main memory, a checksum associated with the software application; and

determine that the security violation is occurring at the main memory when the retrieved checksum does not match with a verified checksum obtained from the retrieved database associated with the main memory.

4. The security module according to claim 2 wherein the instructions to determine that a security violation is occurring further comprises instructions that when executed by the processor cause the processor to:

compare the newly written data in the virtual disk with malware patterns obtained from the retrieved database associated with the main memory; and

determine that the security violation is occurring at the main memory when at least a part of the newly written data matches with the obtained malware patterns.

5. The security module according to claim 4 wherein the malware patterns comprise instructions to encrypt large parts of the main memory, instructions to modify a Unified Extensible Firmware Interface (UEFI) or Basic Input Output System (BIOS) of the host device, abnormal interrupt routines or instructions to continuously transmit data through unsecured wireless or wired transmission means.

6. The security module according to claim 2 wherein the instructions to determine that a security violation is occurring further comprises instructions that when executed by the processor cause the processor to:

provide the data newly written to the virtual disk to a trained supervised machine learning model, whereby the trained supervised machine learning model is configured to detect anomalies in the data; and

determine that the security violation is occurring at the main memory when the number of detected anomalies exceeds a predetermined threshold.

7. The security module according to claim 1 wherein the first identified hardware component comprises a direct memory access (DMA) enabled component and wherein the instructions to determine that a security violation is occurring further comprises instructions that when executed by the processor cause the processor to:

compare the newly acquired data associated with the DMA enabled component with malware patterns obtained from the retrieved database associated with the DMA enabled component whereby it is determined that the security violation is occurring at the DMA enabled component when at least a part of the newly written data matches with the obtained malware patterns,

wherein the newly acquired data comprises data that is directly addressed to the DMA enabled component or data that is generated directly by the DMA enabled component.

8. The security module according to claim 1 wherein the first identified hardware component comprises an electronic device and wherein the instructions to determine that a security violation is occurring further comprises instructions that when executed by the processor cause the processor to:

compare the newly acquired data associated with the electronic device with malware patterns obtained from the retrieved database associated with the electronic device whereby it is determined that the security violation is occurring at the electronic device when at least a part of the newly written data matches with the obtained malware patterns.

9. The security module according to claim 1 wherein the first identified hardware component comprises a peripheral device and wherein the instructions to determine that a security violation is occurring further comprises instructions that when executed by the processor cause the processor to:

compare the newly acquired data associated with the peripheral device with malware patterns obtained from the retrieved database associated with the peripheral device whereby it is determined that the security violation is occurring at the peripheral device when at least a part of the newly written data matches with the obtained malware patterns.

10. The security module according to claim 1 further comprising instructions that when executed by the processor cause the processor to:

acquire new data associated with a second identified hardware component from the bus system; and

determine, based on the newly acquired data and based on a retrieved database associated with the second identified hardware component, that a security violation is occurring at the second identified hardware component.

11. A method for detecting security violations associated with a host device using a security module communicatively connected to a bus system of the host device, the method comprising the steps of:

capturing, using the security module, diagnostic data transmitted through the bus system of the host device when diagnostic tests are executed by the host device during a Power-On-Reset (POR) cycle of the host device;

identifying from the captured diagnostic data, using the security module, hardware components associated with the host device and retrieving databases associated with each of the identified hardware components;

acquiring, using the security module, new data associated with a first identified hardware component from the bus system; and

determining based on the newly acquired data and based on a retrieved database associated with the first identified hardware component, using the security module, that a security violation is occurring at the first identified hardware component.

12. The method according to claim 11 wherein the captured diagnostic data comprise addresses of the host device's main memory and wherein the first identified hardware component comprises the host device's main memory, and before the step of determining that a security violation is occurring at the first identified hardware component, the method further comprises the steps of:

generating, using the security module, a virtual disk based on the addresses of the host device's main memory; and

writing, using the security module, the newly acquired data to the virtual disk as the new data is concurrently acquired from the host device's main memory.

13. The method according to claim 12 wherein the determining that a security violation is occurring further comprises the steps of:

identifying based on the data newly written to the virtual disk, using the security module, a software application that is being loaded in the main memory of the host device;

retrieving from the main memory, using the security module, a checksum associated with the software application; and

determining, using the security module, that the security violation is occurring at the main memory when the retrieved checksum does not match with a verified checksum obtained from the retrieved database associated with the main memory.

14. The method according to claim 12 wherein the determining that a security violation is occurring further the steps of:

comparing, using the security module, the newly written data in the virtual disk with malware patterns obtained from the retrieved database associated with the main memory; and

determining, using the security module, that the security violation is occurring at the main memory when at least a part of the newly written data matches with the obtained malware patterns.

15. The method according to claim 14 wherein the malware patterns comprise instructions to encrypt large parts of the main memory, instructions to modify a Unified Extensible Firmware Interface (UEFI) or Basic Input Output System (BIOS) of the host device, abnormal interrupt routines or instructions to continuously transmit data through unsecured wireless or wired transmission means.

16. The method according to claim 12 wherein the determining that a security violation is occurring further comprises the steps of:

providing, using the security module, the data newly written to the virtual disk to a trained supervised machine learning model, whereby the trained supervised machine learning model is configured to detect anomalies in the data; and

determining, using the security module, that the security violation is occurring at the main memory when the number of detected anomalies exceeds a predetermined threshold.

17. The method according to claim 11 wherein the first identified hardware component comprises a direct memory access (DMA) enabled component and wherein the determining that a security violation is occurring further comprises the steps of:

comparing, using the security module, the newly acquired data associated with the DMA enabled component with malware patterns obtained from the retrieved database associated with the DMA enabled component whereby it is determined that the security violation is occurring at the DMA enabled component when at least a part of the newly written data matches with the obtained malware patterns,

wherein the newly acquired data comprises data that is directly addressed to the DMA enabled component or data that is generated directly by the DMA enabled component.

18. The method according to claim 11 wherein the first identified hardware component comprises an electronic device and wherein the determining that a security violation is occurring further comprises the steps of:

comparing, using the security module, the newly acquired data associated with the electronic device with malware patterns obtained from the retrieved database associated with the electronic device whereby it is determined that the security violation is occurring

at the electronic device when at least a part of the newly written data matches with the obtained malware patterns.

19. The method according to claim 11 wherein the first identified hardware component comprises a peripheral device and wherein the determining that a security violation is occurring further comprises the steps of:

comparing, using the security module, the newly acquired data associated with the peripheral device with malware patterns obtained from the retrieved database associated with the peripheral device whereby it is determined that the security violation is occurring at the peripheral device when at least a part of the newly written data matches with the obtained malware patterns.

20. The method according to claim 11 further comprising the steps of:

acquiring, using the security module, new data associated with a second identified hardware component from the bus system; and

determining, using the security module, based on the newly acquired data and based on a retrieved database associated with the second identified hardware component, that a security violation is occurring at the second identified hardware