## CLAIMS

1. A method for detecting high-level functionality of an application executing on a computing device, the method comprising:

storing, in a secure memory on a computing device, a plurality of virtual address mapping tables, each virtual address mapping table corresponding to one of a plurality of applications, each virtual address mapping table comprising a plurality of virtual addresses of the application binary code mapped to corresponding target application functionalities in source code of the application;

registering the application with a high-level operating system (HLOS); and

during execution of the application binary code, the HLOS detecting when one or more of the virtual addresses corresponding to the target application functionalities are executed based on the virtual address mapping table.

2. The method of claim 1, wherein the secure memory resides in a trusted zone in the HLOS.

3. The method of claim 1, further comprising:

updating the virtual address mapping table with revised virtual addresses for the target application functionalities when the application binary code is updated.

4. The method of claim 1, further comprising:

providing the executed target application functionalities as detected from the virtual addresses into an exception handling module configured to detect one or more exceptions or behaviors associated with execution of the application.

5. The method of claim 4, wherein the exception handling module comprises a malicious code detection algorithm.

6. The method of claim 1, wherein the application comprises one of a secure web application and a web browser.

7. The method of claim 1, wherein the application binary code is executed as native binary code.

8. The method of claim 1, wherein the application binary code comprises an associated virtual machine.

9. A system for detecting high-level functionality of an application executing on a computing device, the system comprising:

means for securely storing on a computing device, a plurality of virtual address mapping tables, each virtual address mapping table corresponding to one of a plurality of applications, each virtual address mapping table comprising a plurality of virtual addresses of the application binary code mapped to corresponding target application functionalities in source code of the application;

means for registering the application with a high-level operating system (HLOS); and

means for detecting, during execution of the application binary code, when one or more of the virtual addresses corresponding to the target application functionalities are executed based on the virtual address mapping table.

10. The system of claim 9, wherein the secure memory comprises a trusted zone in the HLOS.

11. The system of claim 9, further comprising:

means for updating the virtual address mapping table with revised virtual addresses for the target application functionalities when the application binary code is updated.

12. The system of claim 9, further comprising:

means for providing the executed target application functionalities as detected from the virtual addresses into an exception handling module configured to detect one or more exceptions associated with execution of the application.

13. The system of claim 12, wherein the exception handling module comprises a malicious code detection algorithm.

14. The system of claim 9, wherein the application comprises one of a secure web application and a web browser.

15. The system of claim 9, wherein the application binary code is executed as native binary code.

16. The system of claim 9, wherein the application binary code comprises an associated virtual machine.

17. A computer program embodied in a memory and comprising a non-transitory computer usable medium having a computer readable program code embodied therein executable by a processor for detecting high-level functionality of an application executing on a computing device, the computer program implementing a method comprising:

storing, in a secure memory on a computing device, a plurality of virtual address mapping tables, each virtual address mapping table corresponding to one of a plurality of applications, each virtual address mapping table comprising a plurality of virtual addresses of the application binary code mapped to corresponding target application functionalities in source code of the application;

registering the application with a high-level operating system (HLOS); and

during execution of the application binary code, the HLOS detecting when one or more of the virtual addresses corresponding to the target application functionalities are executed based on the virtual address mapping table.

18. The computer program of claim 17, wherein the secure memory comprises a trusted zone in the HLOS.

19. The computer program of claim 17, wherein the method further comprises:

updating the virtual address mapping table with revised virtual addresses for the target application functionalities when the application binary code is updated.

20. The computer program of claim 17, wherein the method further comprises:

providing the executed target application functionalities as detected from the virtual addresses into an exception handling module configured to detect one or more exceptions or behaviors associated with execution of the application.

21. The computer program of claim 20, wherein the exception handling module comprises a malicious code detection algorithm.

22. The computer program of claim 17, wherein the application comprises one of a secure web application and a web browser.

23. The computer program of claim 17, wherein the application binary code is executed as native binary code.

24. The computer program of claim 17, wherein the application binary code comprises of an associated virtual machine.

25. A system for detecting high-level functionality of an executing application, the system comprising:

a processing device configured to execute application binary code; and

a high-level operating system (HLOS) comprising a plurality of virtual address mapping tables, each virtual address mapping table corresponding to one of a plurality of applications, each virtual address mapping table comprising a plurality of virtual addresses of the application binary code mapped to corresponding target application functionalities in source code of the application, the HLOS configured to detect when one or more of the virtual addresses corresponding to the target application functionalities are executed.

26. The system of claim 25, wherein the secure memory comprises a trusted zone in the HLOS.

27. The system of claim 25, wherein the HLOS further comprises an exception handling module configured to receive the executed target application functionalities as detected from the virtual addresses and detect one or more exceptions associated with execution of the application.

28. The system of claim 27, wherein the exception handling module comprises a malicious code detection algorithm.

29. The system of claim 25, wherein the application comprises one of a secure web application and a web browser.

30. The system of claim 25, wherein the application binary code comprises of an associated virtual machine.