

What is claimed is:

1. A computer implemented method of securely executing a Just-In-Time (JIT) compiled code in a runtime environment, comprising:
using at least one hardware processor for:
receiving, by an application, from a JIT executing process that is executing in a context of the application a request to compile in runtime a code segment;
initiating, by the application, a JIT compiling process to compile said code segment to generate an executable code segment, wherein said JIT compiling process is executed at an application level in the context of the application;
storing said executable code segment in a shared memory; and
providing to said JIT executing process a pointer to said executable code segment in said shared memory, said JIT executing process having read-execute access rights to said shared memory;
wherein said JIT executing process and said JIT compiling process are different processes.
2. The computer implemented method according to claim 1, wherein said JIT compiling process employs a JIT compiler adapted to generate said executable code segment according to an architecture of said at least one hardware processor.
3. The computer implemented method according to claim 1, wherein said JIT executing process is denied code generation privileges.
4. The computer implemented method according to claim 1, wherein said JIT executing process is denied of write access rights to said shared memory.
5. The computer implemented method according to claim 1, wherein said JIT compiling process is granted with read-write access rights to said shared memory to allow said storing.
6. The computer implemented method according to claim 1, wherein said JIT compiling process is denied of execution access rights from said shared memory.

7. The computer implemented method according to claim 1, further comprising analyzing said code segment before generating said executable code segment to identify at least one potentially malicious operation initiated by said code segment.
8. The computer implemented method according to claim 1, further comprising analyzing said executable code segment after generated to identify at least one potentially malicious operation initiated by said code segment.
9. The computer implemented method according to claim 1, wherein:
the runtime environment is provided by an operating system (OS),
said JIT compiling process obtains said code segment from said JIT executing process using at least one of a plurality of services provided by the OS,
said shared memory is managed by the OS, and
said pointer is provided to said JIT executing process by said JIT compiling process using at least one service provided by the OS.
10. The computer implemented method according to claim 1, wherein a ProcessDynamicCodePolicy setting is enabled for said JIT executing process and said JIT compiling process.
11. The computer implemented method of claim 1, wherein the application comprises a local agent that provides a remote service provided by a remote web server, a remote computing node, a remote computing cluster or a remote cloud service.
12. The computer implemented method of claim 1, wherein management of said JIT compiling process is built into the application.
13. The computer implemented method of claim 1, wherein management of said JIT compiling process is added to the application via a plug-in.
14. The computer implemented method of claim 1, wherein the application comprises a web browser application.

15. A system for securely executing a Just-In-Time (JIT) compiled code in a runtime environment, comprising:
at least one hardware processor adapted to execute code, said code comprising:
code instructions of an application to receive from a JIT executing process executing in a context of the application a request to compile in runtime a code segment;
code instructions of the application to initiate a JIT compiling process to compile said code segment to generate an executable code segment, wherein said JIT compiling process is executed at an application level in the context of the application;
code instructions to store said executable code segment in a shared memory; and
code instructions to provide to said JIT executing process a pointer to said executable code segment in said shared memory, said JIT executing process having read-execute access rights to said shared memory;
wherein said JIT executing process and said JIT compiling process are different processes.
16. The system of claim 15, wherein the application comprises a local agent to provide a remote service provided by a remote web server, a remote computing node, a remote computing cluster or a remote cloud service.
17. The system of claim 15, wherein management of said JIT compiling process is built into the application.
18. The system of claim 15, wherein management of said JIT compiling process is added to the application via a plug-in.
19. The system of claim 15, wherein the application comprises a web browser application.
20. A system for securely executing a Just-In-Time (JIT) compiled code in a runtime environment, comprising:
at least one hardware processor adapted to execute code, said code comprising:
code instructions of an application to initiate, in a context of the application, a JIT executing process comprising at least one un-compiled code segment; and
code instructions of the application to execute, separate and independent from said JIT executing process, a JIT compiling process to compile said at least one code segment to

generate at least one corresponding executable code segment, wherein said JIT compiling process is executed at an application level in the context of the application;
wherein in response to a request from said JIT executing process to compile said at least one code segment, said JIT compiling process compiles said at least one code segment to generate said corresponding executable code segment and stores said corresponding executable code segment in a shared memory to which said executing process has read-execute access rights.