CLAIMS

1. A computer system for providing perfect forward secrecy in a virtual machine, the system comprising:

a data processing component;

a physical memory; and

local data storage having stored thereon computer executable program code, which when executed by the data processing component causes the data processing component to:

receive, from an application operating within a virtual machine, a secure memory allocation function for a connection secret, wherein the secure memory allocation function includes a memory size parameter;

allocate memory for the connection secret according to the memory size parameter, wherein the memory includes a memory location and a memory size;

transmit the memory location and the memory size to a virtual machine host to be stored as an entry in a secure database;

store the entry in the secure database;

monitor an operation state relating to the virtual machine;

receive, from the application, a secure reallocation function containing a new memory size for the memory;

resize the memory into the new memory size provided by the secure reallocation function;

transmit a new memory location and the new memory size to the virtual machine host to update the entry in the secure database;

sanitize the memory location; and

update the entry relating to the memory stored in the secure database with the new memory location and the new memory size.

2. The computer system of claim 1, further comprising:

receive, from the application, a secure deallocation function relating to the connection secret;

retrieve the entry from the secure database;

deallocate the memory by overwriting the memory location; and

sanitize the memory location indicated by the entry.

3. The computer system of claim 2, wherein the sanitize comprises overwriting the memory location with random data at least once.

4. The computer system of claim 1, wherein the connection secrets include a session key relating to a secure connection between the application and a server.

5. The computer system of claim 1, wherein the secure memory allocation function includes a number of memory blocks parameter.

6. The computer system of claim 1, further comprising:

receive a notice indicating a change to the operation state of the virtual machine;

determine the operation state of the virtual machine;

retrieve the entry from the secure database relating to the virtual machine; and

sanitize, based on the operation state of the virtual machine, the memory location indicated by the entry.

7. The computer system of claim 6, further comprising:

determine the memory, including the connection secret, is stored in storage;

locate a storage location within the storage storing the connection secret; and

sanitize the storage location.

8. A computer-implemented method for providing perfect forward secrecy in a virtual machine, the computer-implemented method comprising:

receiving, from an application operating within a virtual machine, a secure memory allocation function for a connection secret, wherein the secure memory allocation function includes a memory size parameter;

allocating memory for the connection secret according to the memory size parameter, wherein the memory includes a memory location and a memory size;

transmitting the memory location and the memory size to a virtual machine host to be stored as an entry in a secure database;

storing the entry in the secure database;

monitoring an operation state relating to the virtual machine;

receiving, from the application, a secure reallocation function containing a new memory size for the memory;

resizing the memory into the new memory size provided by the secure reallocation function;

transmitting a new memory location and the new memory size to the virtual machine host to update the entry in the secure database;

sanitizing the memory location; and

updating the entry relating to the memory stored in the secure database with the new memory location and the new memory size.

9. The computer-implemented method of claim 8, further comprising:

receiving, from the application, a secure deallocation function relating to the connection secret;

retrieving the entry from the secure database;

deallocating the memory by overwriting the memory location; and

sanitizing the memory location indicated by the entry.

10. The computer-implemented method of claim 9, wherein sanitizing comprises overwriting the memory location with random data at least once.

11. The computer-implemented method of claim 8, wherein the connection secrets include a session key relating to a secure connection between the application and a server.

12. The computer-implemented method of claim 8, wherein the secure memory allocation function includes a number of memory blocks parameter.

13. The computer-implemented method of claim 8, further comprising:

receiving a notice indicating a change to the operation state of the virtual machine;

determining the operation state of the virtual machine;

retrieving the entry from the secure database relating to the virtual machine; and

sanitizing, based on the operation state of the virtual machine, the memory location indicated by the entry.

14. The computer-implemented method of claim 8, further comprising:

determining the memory, including the connection secret, is stored in storage;

locating a storage location within the storage storing the connection secret; and

sanitizing the storage location.

15. A non-transitory computer-readable storage medium having stored thereon instruction for controlling a computer system to:

receiving, from an application operating within a virtual machine, a secure memory allocation function for a connection secret, wherein the secure memory allocation function includes a memory size parameter;

allocating memory for the connection secret according to the memory size parameter, wherein the memory includes a memory location and a memory size;

transmitting the memory location and the memory size to a virtual machine host to be stored as an entry in a secure database;

storing the entry in the secure database;

monitoring an operation state relating to the virtual machine;

receiving, from the application, a secure reallocation function containing a new memory size for the memory;

resizing the memory into the new memory size provided by the secure reallocation function;

transmitting a new memory location and the new memory size to the virtual machine host to update the entry in the secure database;

sanitizing the memory location; and

updating the entry relating to the memory stored in the secure database with the new memory location and the new memory size.

16. The non-transitory computer-readable storage medium of claim 15, further comprising:

receiving, from the application, a secure deallocation function relating to the connection secret;

retrieving the entry from the secure database;

deallocating the memory by overwriting the memory location; and

sanitizing the memory location indicated by the entry.

17. The non-transitory computer-readable storage medium of claim 15, further comprising:

receiving a notice indicating a change to the operation state of the virtual machine;

determining the operation state of the virtual machine;

retrieving the entry from the secure database relating to the virtual machine; and

sanitizing, based on the operation state of the virtual machine, the memory location indicated by the entry.