

WHAT IS CLAIMED IS:

- 1                   1.       A method comprising:  
2                   initiating a secure string instance of a program module;  
3                   receiving sensitive data at the secure string instance of the program module,  
4                   the sensitive data being in plaintext;  
5                   retrieving one or more parameters that are sourced from outside of an  
6                   allocated memory used for execution of the program module;  
7                   encrypting the sensitive data using the one or more parameters to obtain  
8                   encrypted data;  
9                   storing the encrypted data;  
10                  receiving a trigger to send a message that is to be generated using the sensitive  
11                  data;  
12                  retrieving the one or more parameters that are sourced from outside the  
13                  allocated memory;  
14                  decrypting the encrypted data using the one or more parameters to obtain the  
15                  sensitive data;  
16                  overwriting the one or more parameters in the allocated memory;  
17                  using the sensitive data to generate the message; and  
18                  overwriting the sensitive data in the allocated memory so as to delete the  
19                  sensitive data.
- 1                   2.       The method of claim 1, wherein the one or more parameters that are  
2                   sourced from outside of the allocated memory are parameters associated with the program  
3                   module.
- 1                   3.       The method of claim 1, further comprising overwriting the one or more  
2                   parameters in the allocated memory immediately after encrypting the sensitive data.
- 1                   4.       The method of claim 1, wherein the one or more parameters comprises  
2                   at least one or more of a start time of the program module, a space associated with a physical  
3                   memory, a process ID, and a network stack property.
- 1                   5.       The method of claim 1, wherein retrieving the one or more parameters  
2                   comprises:

3                   retrieving a first parameter from a first hardware module and a second  
4                   parameter from a second hardware module, wherein the first hardware module and the second  
5                   hardware module are separate from the allocated memory.

1                   6.       The method of claim 1, wherein encrypting the sensitive data further  
2                   comprises:  
3                   generating a key using the one or more parameters;  
4                   overwriting the one or more parameters in the allocated memory;  
5                   encrypting the sensitive data using the key to obtain the encrypted data; and  
6                   overwriting the key in the allocated memory.

1                   7.       The method of claim 6 wherein decrypting the sensitive data further  
2                   comprises:  
3                   generating the key using the one or more parameters;  
4                   overwriting the one or more parameters in the allocated memory;  
5                   decrypting the sensitive data using the key to obtain the sensitive data; and  
6                   overwriting the key in the allocated memory.

1                   8.       The method of claim 1, wherein the trigger is initiated by a device  
2                   requesting access to a resource associated with the sensitive data.

1                   9.       The method of claim 1, wherein using the sensitive data to generate the  
2                   message further comprises:  
3                   accessing an encryption key associated with the trigger;  
4                   encrypting the sensitive data using the encryption key to obtain encrypted  
5                   sensitive data; and  
6                   generating the message using the encrypted sensitive data.

1                   10.      The method of claim 1 further comprising transmitting the message to  
2                   a second secure string instance of the program module.

1                   11.      The method of claim 1, wherein the message is a request to access  
2                   services over a network.

1                   12.      The method of claim 1, wherein the trigger is associated with an  
2                   authorization process associated with the sensitive data.

1                   13.     The method of claim 1, further comprising:  
2                   storing the sensitive data in a mutable object; and  
3                   overwriting the sensitive data in the mutable object with the encrypted data.

1                   14.     A computing device comprising:  
2                   a processor; and  
3                   one or more non-transitory computer readable media storing instructions that,  
4                   when executed by the processor, cause the computing device to perform the method of any  
5                   one of claims 1-12.

1                   15.     A computer product comprising a non-transitory computer readable  
2                   medium storing a plurality of instructions, that when executed on one or more processors of a  
3                   computer system, perform the method of any one of claims 1-12.  
4