CLAIMS

1. A system comprising:

a volatile memory device; and

a processing device configured to process an initial set of command types, the processing device, operatively coupled with the volatile memory device, configured to perform operations comprising:

receiving a command extension module and a digital signature, the digital signature being generated based on the command extension module using a private key of a key pair, the command extension module, once installed by the processing device, enabling the processing device to process a new command type that is not included in the initial set of command types, the command extension module comprising a time to live (TTL) value;

verifying the digital signature using a public key of the key pair;

based on a successful verification of the digital signature, temporarily installing the command extension module on the system, the temporarily installing of the command extension module comprising loading the command extension module in the volatile memory device;

the processing device comprising an extension redirect component configured to forward a command to the command extension module based on the command corresponding to the new command type; and

the processing device further configured to erase the command extension module based on expiration of the TTL value.

2. The system of claim 1, wherein the extension redirect component is further configured to:

receive the command; and

determine the command corresponds to the new command type.

3. The system of claim 1, wherein the command extension module processes the command.

4. The system of claim 3, wherein the command extension module performs one or more callbacks to the processing device in processing the command.

5. The system of claim 1, wherein the command extension module is erased upon system reboot.

6. The system of claim 1, wherein the operations further comprise:

determining a security version of the command extension module; and

validating the security version of the command extension module based on stored information.

7. The system of claim 6, wherein the validating of the security version of the command extension module comprises comparing the security version of the command extension module to a security version counter.

8. The system of claim 7, wherein the operations further comprise:

incrementing the security version counter based on temporarily installing the command extension module.

9. The system of claim 1, further comprising non-volatile memory media to store the public key.

10. The system of claim 1, further comprising a host interface, wherein the command extension module and digital signature are received via the host interface as part of a command extension request.

11. The system of claim 1, wherein the verifying of the digital signature by the processing device comprises using an asymmetric cryptographic algorithm to verify the digital signature based on a combination of the public and private key.

12. A method comprising:

receiving, by a memory sub-system controller comprising one or more processors of a machine, a command extension module and a digital signature, the digital signature being generated based on the command extension module using a private key of a key pair, the memory sub-system controller comprising firmware that enables the memory sub-system to process an initial set of command types, the command extension module comprising a set of machine-readable instructions, that once installed by the memory sub-system controller, enables the memory sub-system controller to process a new command type that is not included in the initial set of command types, the command extension module comprising a time to live (TTL) value;

verifying, by the memory sub-system controller, the digital signature using a public key of the key pair;

based on a successful verification of the digital signature, temporarily installing, at the memory sub-system controller, the command extension module, the temporarily installing of the command extension module comprising storing the command extension module in a volatile memory device of the memory sub-system controller;

forwarding a command to the command extension module based on the command corresponding to the new command type; and

erasing the command extension module based on expiration of the TTL value.

13. The method of claim 12, further comprising:

receiving the command; and

determining the command corresponds to the new command type.

14. The method of claim 12, further comprising:

processing, by the command extension module, the command.

15. The method of claim 12, further comprising:

initiating a TTL countdown upon installing the command extension module; and

detecting the expiration of the TTL value based on the TTL countdown.

16. The method of claim 12, further comprising:

determining a security version of the command extension module; and

validating the security version of the command extension module based on stored information.

17. The method of claim 16, wherein:

the validating of the security version of the command extension module comprises comparing the security version of the command extension module to a security version counter; and

the method further comprises:

incrementing the security version counter based on temporarily installing the command extension module.

18. The method of claim 12, the command extension module and digital signature are received, from a host system, via a host interface of the memory sub-system controller, as part of a command extension request.

19. The method of claim 12, wherein the verifying of the digital signature by the processing device comprises using an asymmetric cryptographic algorithm to verify the digital signature based on a combination of the public and private key.

20. A non-transitory computer-readable storage medium comprising instructions that, when executed by a processing device, configure the processing device to perform operations comprising:

receiving a command extension module and a digital signature, the digital signature being generated based on the command extension module using a private key of a key pair, the processing device comprising firmware that enables the processing device to process an initial set of command types, the command extension module comprising a set of machine-readable instructions, that once installed by the processing device, enables the processing device to

process a new command type that is not included in the initial set of command types, the command extension module comprising a time to live (TTL) value;

verifying the digital signature using a public key of the key pair;

based on a successful verification of the digital signature, temporarily installing the command extension module, the temporarily installing of the command extension module comprising storing the command extension module in a volatile memory device of the processing device;

forwarding a command to the command extension module based on the command corresponding to the new command type; and

erasing the command extension module based on expiration of the TTL value.