CLAIMS

1. A computer-implemented method implemented in a computer comprising a processor, memory accessible by the processor, and computer program instructions stored in the memory and executable by the processor, the method comprising:

creating a namespace in an operating system kernel-space in the memory of the computer;

creating an address space for the namespace that maps only kernel objects owned by the namespace by:

generating a namespace page table comprising kernel-space mappings for kernel objects owned by the namespace, and

constructing a combined page table accessible to at least one user process comprising a user-space page table of the user process and the namespace page table; and

providing access to kernel objects owned by the namespace only to the least one user process using the combined page table.

2. The method of claim 1, wherein the operating system is a Linux operating system.

3. The method of claim 2, wherein the namespace is a namespace type selected from: a Mount namespace, a Process Identifier (ID) namespace, a Network namespace, an Interprocess Communication namespace, a UNIX Time-Sharing (UTS) namespace, a User Identifier (ID) namespace, and a Control group namespace.

4. The method of claim 1, further comprising destroying the namespace by destroying the combined page table, the namespace page table, and the kernel object owned by the namespace.

5. A system comprising a processor, memory accessible by the processor, and computer program instructions stored in the memory and executable by the processor to perform:

creating a namespace in an operating system kernel-space in the memory of the computer;

creating an address space for the namespace that maps only kernel objects owned by the namespace by:

generating a namespace page table comprising kernel-space mappings for kernel objects owned by the namespace, and

constructing a combined page table accessible to at least one user process comprising a user-space page table of the user process and the namespace page table; and

providing access to kernel objects owned by the namespace only to the least one user process using the combined page table.

6. The system of claim 5, wherein the operating system is a Linux operating system.

7. The method of claim 6, wherein the namespace is a namespace type selected from: a Mount namespace, a Process Identifier (ID) namespace, a Network namespace, an Interprocess Communication namespace, a UNIX Time-Sharing (UTS) namespace, a User Identifier (ID) namespace, and a Control group namespace.

8. The system of claim 5, further comprising destroying the namespace comprising destroying the combined page table, the namespace page table, and the kernel object owned by the namespace.

9. A computer program product comprising a non-transitory computer readable storage having program instructions embodied therewith, the program instructions executable by a computer, to cause the computer to perform a method comprising:

creating a namespace in an operating system kernel-space in the memory of the computer;

creating an address space for the namespace that maps only kernel objects owned by the namespace by:

generating a namespace page table comprising kernel-space mappings for kernel objects owned by the namespace, and

constructing a combined page table accessible to at least one user process comprising a user-space page table of the user process and the namespace page table; and

providing access to kernel objects owned by the namespace only to the least one user process using the combined page table.

10. The computer program product of claim 9, wherein the operating system is a Linux operating system.

11. The computer program product of claim 10, wherein the namespace is a namespace type selected from: a Mount namespace, a Process Identifier (ID) namespace, a Network namespace, an Interprocess Communication namespace, a UNIX Time-Sharing (UTS) namespace, a User Identifier (ID) namespace, and a Control group namespace.

12. The computer program product of claim 9, further comprising destroying the namespace comprising destroying the combined page table, the namespace page table, and the kernel object owned by the namespace.