

CLAIMS

1. A computer system (102) to facilitate secure processing within a computing environment (100), the computer system comprising:

a memory (104);

a processor (110) coupled to the memory (104), wherein the computer system is configured to perform a method comprising:

incrementally decrypting a secure operating system image, by a secure interface control (115, 410) of the computer system (102), the secure interface control (115, 410) being a trusted entity of the computer system (102), the incrementally decrypting including for a page of a plurality of pages of the secure operating system image:

receiving, by the secure interface control (115, 410) from a hypervisor (114, 400), a page address of the page and a tweak value used during encryption of the page, wherein pages and page addresses of the plurality of pages are provided in a fixed order to facilitate the incrementally decrypting;

placing the page address of the page in a current address register (412) and the tweak value used during encryption of the page in a current tweak register (411);

determining that the page address is different than any previous page address of previously decrypted pages of the plurality of pages of the secure operating system image, the determining that the page address is different including comparing the current address register (412) to a last address register (418) containing a page address of a last page incrementally decrypted;

÷

determining that the tweak value has not previously been used during decryption of another page of the plurality of pages of ~~the secure operating system image; and the secure operating system image, the determining that the tweak value has not been previously used during decryption of another page comprising comparing the current tweak register (411) to a last tweak register (417) containing a tweak value of a last page of the plurality of pages incrementally decrypted; and~~

decrypting memory page content at the page address using an image encryption key used in encrypting the page and the tweak value to facilitate obtaining a decrypted secure operating system image;

verifying ~~by the secure interface control (115, 410),~~
integrity of the secure operating system image; and

based on verifying integrity of the secure operating system image, starting execution of the decrypted secure operating system image.

~~2. — The computer system of claim 1, wherein the incrementally decrypting and the verifying integrity are performed by a secure interface control of the computer system, the secure interface control being a trusted entity of the computer system, and the page address and the tweak value are received by the secure interface control from a hypervisor.~~

~~3.2. The computer system of any one of the preceding claims 1, wherein page addresses of the plurality of pages are non-contiguous and in a fixed order, and the incrementally decrypting the secure operating system image includes determining that the page address is different than any previous page address of previously decrypted pages of the plurality of pages of the secure operating system image.~~

~~4. — The computer system of any one of the preceding claims, wherein the incrementally decrypting the secure operating system image further includes determining~~

~~that the tweak value is different than previous tweak values used during decryption of previously decrypted pages of the plurality of pages of the secure operating system image.~~

5 ~~5.3.~~ The computer system of any one of the preceding claims, wherein the verifying integrity includes employing, in part, a cumulative content hash (415) obtained using memory page content of the plurality of pages and a cumulative address hash (416) obtained using page addresses of the plurality of pages.

10 ~~6.4.~~ The computer system of claim ~~53~~, wherein the verifying integrity of the secure operating system image includes comparing the cumulative content hash (415) to an integrity content hash (307) received by the secure interface control (115, 410), and comparing the cumulative address hash (416) to an integrity address hash (308) received by the secure interface control.

15 ~~7.5.~~ The computer system of claim ~~64~~, further comprising extracting, by the secure interface control (114, 410), the image encryption key (306) and the integrity content hash (308) and integrity address hash from metadata received from the hypervisor (114, 400).

20 ~~8.6.~~ The computer system of any one of the preceding claims, wherein the secure interface control (115, 410) comprises one or more elements of the computer system (102), the one or more elements being selected from the group consisting of hardware elements and firmware elements, and the secure operating system image is to be run as a secure guest operating system within the computing environment (102).

25 ~~9.7.~~ The computer system of any one of the preceding claims, wherein a private-public key pair is associated with the computer system (102), the private key being known only to the secure interface control (115, 410), and not accessible by software running on the computer system (102), and wherein the public key is used by an owner of the secure operating system image to generate key agreement data to securely communicate the image encryption key (306) used for encrypting the secure operating system image with the secure interface control (115, 410) and store the key agreement data in a metadata structure (301).

30 ~~10.8.~~ The computer system of claim ~~97~~, further comprising receiving by the secure interface control (115, 410) the metadata structure (301) with a call from the

hypervisor, the metadata structure (301) further comprising integrity hash values used in the verifying integrity of the secure operating system image.

11.9. A computer program product comprising:

a computer-readable storage medium readable by a processing circuit and storing instructions for performing a method comprising:

incrementally decrypting a secure operating system image, by a secure interface control (115, 410) of the computer system (102), the secure interface control (115, 410) being a trusted entity of the computer system (102), the incrementally decrypting including for a page of a plurality of pages of the secure operating system image:

receiving, by the secure interface control (115, 410) from a hypervisor (114, 400), a page address of the page and a tweak value used during encryption of the page; wherein pages and page addresses of the plurality of pages are provided in a fixed order to facilitate the incrementally decrypting;

placing the page address of the page in a current address register (412) and the tweak value used during encryption of the page in a current tweak register (411);

determining that the page address is different than any previous page address of previously decrypted pages of the plurality of pages of the secure operating system image, the determining that the page address is different including comparing the current address register (412) to a last address register (418) containing a page address of a last page incrementally decrypted;

determining that the tweak value has not previously been used during decryption of another page of the plurality of pages of the secure operating system image; ~~and, the~~

5

determining that the tweak value has not been previously used during decryption of another page comprising comparing the current tweak register (411) to a last tweak register (417) containing a tweak value of a last page of the plurality of pages incrementally decrypted; and

decrypting memory page content at the page address using an image encryption key used in encrypting the page and the tweak value to facilitate obtaining a decrypted secure operating system image;

10

verifying, by the secure interface control (115, 410), integrity of the secure operating system image; and

based on verifying integrity of the secure operating system image, starting execution of the decrypted secure operating system image.

15

12.10. The computer program product of claim 119, wherein page addresses of the plurality of pages are non-contiguous and are in a the fixed order, ~~and the incrementally decrypting the secure operating system image includes determining that the page address is different than any previous page address of previously decrypted pages of the plurality of pages of the secure operating system image.~~

20

~~13.—The computer program product of any one of claims 11 to 12, wherein the incrementally decrypting the secure operating system image further includes determining that the tweak value is different than any previous tweak values used during decryption of previously decrypted pages of the plurality of pages of the secure operating system image.~~

~~14.—The computer program product of any one of claims 12 to 13,~~

25

11. The computer program product of claim 10, wherein the verifying integrity includes employing, in part, a cumulative content hash obtained using memory page content of the plurality of pages and a cumulative address hash obtained using page addresses of the plurality of pages.

15.12. The computer program product of claim 1411, wherein the verifying integrity of the secure operating system image includes comparing the cumulative content

hash (415) to an integrity content hash (307) received by the secure interface control (115, 410).

~~16.13.~~ The computer program product of any one of claims ~~14.11~~ to ~~15.12~~, wherein the verifying integrity of the secure operating system image further includes
5 comparing the cumulative address hash (416) to an integrity address hash (308) received by the secure interface control (115, 410).

~~17.14.~~ The computer program product of claim ~~16.13~~, further comprising extracting the image encryption key (306) and the integrity content hash (307) and integrity address hash (308) from metadata received from a hypervisor.

10 ~~18.15.~~ A computer-implemented method comprising:

incrementally decrypting a secure operating system
image, by a secure interface control (115, 410) of the computer
system (102), the secure interface control (115, 410) being a
trusted entity of the computer system (102), the incrementally
15 decrypting including for a page of a plurality of pages of the
secure operating system image:

receiving, by the secure interface control (115, 410) from a
hypervisor (114, 400), a page address of the page and a tweak
value used during encryption of the page, wherein pages and page
20 addresses of the plurality of pages are provided in a fixed order to
facilitate the incrementally decrypting;

placing the page address of the page in a current address
register (412) and the tweak value used during encryption of the
page in a current tweak register (411);

25 determining that the page address is different than any
previous page address of previously decrypted pages of the plurality
of pages of the secure operating system image, the determining that
the page address is different including comparing the current

address register (412) to a last address register (418) containing a page address of a last page incrementally decrypted;

determining that the tweak value has not previously been used during decryption of another page of the plurality of pages of the secure operating system image; and, the determining that the tweak value has not been previously used during decryption of another page comprising comparing the current tweak register (411) to a last tweak register (417) containing a tweak value of a last page of the plurality of pages incrementally decrypted; and

decrypting memory page content at the page address using an image encryption key used in encrypting the page and the tweak value to facilitate obtaining a decrypted secure operating system image;

verifying, by the secure interface control (115, 410), integrity of the secure operating system image; and

based on verifying integrity of the secure operating system image, starting execution of the decrypted secure operating system image.

~~19.—The computer implemented method of claim 18, wherein the incrementally decrypting and the verifying integrity are performed by a secure interface control of a host computer system, the secure interface control being a trusted entity, and the page address and the tweak value used are received by the secure interface control from a hypervisor.~~

~~20.—The computer implemented method of any one of claims 18 to 19, wherein page addresses of the plurality of pages are in a fixed order, and the incrementally decrypting the secure operating system image includes determining that the page address is different than any previous page address of previously decrypted pages of the plurality of pages of the secure operating system image, and wherein the incrementally decrypting the secure operating system image further includes determining that the tweak value is different than any previous tweak values used during decryption of previously decrypted pages of the plurality of pages of the secure operating system image.~~