

REIVINDICACIONES

1. Un método para determinar la equivalencia de enclave, que comprende
recibir un primer informe de certificación a partir de un primer enclave instanciado en una primera plataforma de enclave nativa;
extraer un primer valor de identidad de enclave asociado con un tipo de identidad de enclave a partir del primer informe de certificación;
recibir un segundo informe de certificación a partir de un segundo enclave instanciado en una segunda plataforma de enclave nativa, en donde la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes;
extraer un segundo valor de identidad de enclave asociado con el tipo de identidad de enclave a partir del segundo informe de certificación;
determinar que el primer valor de identidad de enclave es el mismo que el segundo valor de identidad de enclave; y
realizar, con base en la determinación, una operación de computación al completar parcialmente la operación de computación en el primer enclave y al completar parcialmente la operación de computación en el segundo enclave.
2. El método de acuerdo con la reivindicación 1, en donde la operación de computación se realiza en serie con el primer y segundo enclave, y comprende, además:
codificar los datos de estado de enclave del primer enclave después de completar parcialmente la operación de computación en el primer enclave para producir los datos codificados, en donde los datos de estado se codifican para el tipo de identidad de enclave;
copiar los datos codificados desde el primer enclave al segundo enclave; y
decodificar los datos codificados en el segundo enclave.
3. El método de acuerdo con la reivindicación 1, en donde la operación de computación se realiza simultáneamente con el primer y segundo enclave, y comprende, además:
copiar una primera porción de un conjunto de datos en el primer enclave;
copiar una segunda porción de un conjunto de datos en el segundo enclave; y
en donde la operación de computación se completa parcialmente en el primer enclave utilizando la primera porción y se completa parcialmente en el segundo enclave utilizando la segunda porción.
4. El método de acuerdo con la reivindicación 1, en donde:
completar parcialmente la operación de computación en el primer enclave incluye la lectura, por el primer enclave, de un contador monotónico o un tiempo confiable asociado con el valor de identidad; y
completar parcialmente la operación de computación en el segundo enclave incluye la lectura, por el segundo enclave, del contador monotónico o del tiempo confiable asociado con el valor de identidad.
5. El método de acuerdo con la reivindicación 1, que comprende, además:
crear una firma para el primer informe de certificación al realizar al menos una primera operación

de plataforma nativa; y

crear una firma para el segundo informe de certificación al realizar al menos una segunda operación de plataforma nativa.

6. El método de acuerdo con la reivindicación 1, en donde la primera plataforma de enclave nativa se adapta a una arquitectura de enclave de extensiones de protección de *software* (SGX, por sus siglas en inglés) de Intel y la segunda plataforma de enclave nativa se adapta a una arquitectura de enclave de modo seguro virtual (VSM, por sus siglas en inglés) de Microsoft, y que comprende, además:

generar el primer informe de certificación al realizar al menos una operación nativa de SGX; y

generar el segundo informe de certificación al realizar al menos una operación nativa de VSM.

7. El método de acuerdo con la reivindicación 1, que comprende, además:

verificar una primera firma del primer informe de certificación con una clave pública asociada con la primera plataforma de enclave nativa; y

verificar una segunda firma del segundo informe de certificación con una clave pública asociada con la segunda plataforma del enclave nativa, en donde la primera clave pública y la segunda clave pública son diferentes.

8. El método de acuerdo con la reivindicación 1, que comprende, además:

verificar un primer certificado de aprobación de la primera plataforma nativa con una primera clave pública asociada con un fabricante de la primera plataforma de enclave nativa; y

verificar un segundo certificado de aprobación de la segunda plataforma de enclave nativa con una segunda clave pública asociada con el fabricante de la segunda plataforma de enclave nativa, en donde la primera clave pública y la segunda clave pública no son las mismas.

9. El método de acuerdo con la reivindicación 1, que comprende, además:

generar el primer informe de certificación al computar un valor *hash* con respecto a una primera porción de memoria en un contenedor seguro del primer enclave, en donde el contenido de la primera porción de memoria es independiente de la primera plataforma nativa; y

generar el segundo informe de certificación al computar un valor *hash* con respecto a una segunda porción de memoria en un contenedor seguro del segundo enclave, en donde el contenido de la segunda porción de memoria es independiente de la segunda plataforma nativa.

10. Un sistema que comprende al menos un procesador y una memoria que almacena en la misma las instrucciones que, cuando se ejecutan por el sistema, producen al menos las etapas de:

recibir un primer informe de certificación a partir de un primer enclave instanciado en una primera plataforma de enclave nativa;

extraer un primer valor de identidad de enclave asociado con un tipo de identidad de enclave a partir del primer informe de certificación;

recibir un segundo informe de certificación a partir de un segundo enclave instanciado en una segunda plataforma de enclave nativa, en donde la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes;

extraer un segundo valor de identidad de enclave asociado con el tipo de identidad de enclave a

partir del segundo informe de certificación;

comparar el primer valor de identidad de enclave con el segundo valor de identidad de enclave; y
realizar una operación de computación al completar parcialmente la operación de computación en el primer enclave y al completar parcialmente la operación de computación en el segundo enclave.

11. El sistema de acuerdo con la reivindicación 10, en donde la operación de computación se realiza en serie con el primer y segundo enclave, y en donde las instrucciones producen, además, al menos las etapas de:

codificar los datos de estado de enclave del primer enclave después de completar parcialmente la operación de computación en el primer enclave para producir los datos codificados, en donde los datos de estado se codifican para el tipo de identidad de enclave;

copiar los datos codificados desde el primer enclave al segundo enclave; y
decodificar los datos codificados en el segundo enclave.

12. El sistema de acuerdo con la reivindicación 10, en donde la operación de computación se realiza simultáneamente con el primero y segundo enclave, y en donde las instrucciones producen, además, al menos las etapas de:

copiar una primera porción de un conjunto de datos en el primer enclave;
copiar una segunda porción de un conjunto de datos en el segundo enclave; y
en donde la operación de computación se completa parcialmente en el primer enclave utilizando la primera porción y se completa parcialmente en el segundo enclave utilizando la segunda porción.

13. El sistema de acuerdo con la reivindicación 10, en donde las instrucciones producen, además, al menos las etapas de:

verificar un primer certificado de aprobación de la primera plataforma nativa con una primera clave pública asociada con un fabricante de la primera plataforma de enclave nativa; y

verificar un segundo certificado de aprobación de la segunda plataforma de enclave nativa con una segunda clave pública asociada con el fabricante de la segunda plataforma de enclave nativa, en donde la primera clave pública y la segunda clave pública no son las mismas.

14. El sistema de acuerdo con la reivindicación 10, en donde las instrucciones producen, además, al menos las etapas de:

generar el primer informe de certificación al computar un valor *hash* con respecto a una primera porción de memoria en un contenedor seguro del primer enclave, en donde el contenido de la primera porción de memoria es independiente de la primera plataforma nativa; y

generar el segundo informe de certificación al computar un valor *hash* con respecto a una segunda porción de memoria en un contenedor seguro del segundo enclave, en donde el contenido de la segunda porción de memoria es independiente de la segunda plataforma nativa.

15. Un sistema que comprende:

medios para recibir un primer informe de certificación desde un primer enclave instanciado en una primera plataforma de enclave nativa;

medios para extraer un primer valor de identidad de enclave asociado con un tipo de identidad de

enclave a partir del primer informe de certificación;

medios para recibir un segundo informe de certificación desde un segundo enclave instanciado en una segunda plataforma de enclave nativa, en donde la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes;

medios para extraer un segundo valor de identidad de enclave asociado con el tipo de identidad de enclave a partir del segundo informe de certificación;

medios para comparar el primer valor de identidad de enclave con el segundo valor de identidad de enclave; y

medios para realizar una operación de computación al completar parcialmente la operación de computación en el primer enclave y al completar parcialmente la operación de computación en el segundo enclave.