

REIVINDICACIONES

1. Un método de identificación de enclave realizado por un dispositivo informático que comprende un procesador y una memoria, el método comprende:

Recibir (1503) un tipo de identidad y una solicitud de una operación relacionada con un enclave instanciado;

determinar (1508) un valor de identidad para el enclave con base en el tipo de identidad y la información obtenida a partir de una imagen de enclave a partir de la cual se creó una instancia del enclave; y

realizar (1512) la operación con el valor de identidad,

en donde:

el valor de identidad se determina como una salida de una función hash;

el enclave se sometió a la creación de instancias con una pluralidad de imágenes de enclave; y

el tipo de identidad indica cuál de la pluralidad de imágenes de enclave se incluye, al menos en parte, en la función hash para determinar el valor de identidad.

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

verificar la integridad del valor de identidad al verificar una firma en la imagen de enclave con una clave pública relacionada con un autor de la imagen de enclave.

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

determinar, con base, al menos en parte, en el tipo de identidad, una porción de identidad de la imagen de enclave; y

computar la función hash con respecto a la porción de identidad.

4. El método de acuerdo con la reivindicación 3, en donde la imagen de enclave incluye referencias a imágenes de enclave dependientes adicionales, y que comprende, además:

determinar, con base, al menos en parte, en el tipo de identidad, qué imágenes de enclave dependientes adicionales se incluyen como entrada a la función hash.

5. El método de acuerdo con la reivindicación 3, en donde la porción de identidad incluye uno o más de: código binario copiado en un contenedor de enclave seguro durante la creación de instancias del enclave instanciado, y uno o más identificadores que no son código ejecutable.

6. El método de acuerdo con la reivindicación 1, en donde:

la operación incluye generar un informe de certificación con el valor de identidad.

7. El método de acuerdo con la reivindicación 1, en donde:

la operación incluye codificar los datos en el enclave al codificar los datos con el valor de identidad.

8. El método de acuerdo con la reivindicación 1, en donde:

la operación incluye incrementar un contador monotónico, en donde el contador monotónico se identifica por el valor de identidad.

9. El método de acuerdo con la reivindicación 1, en donde:

la operación incluye realizar una medición de tiempo confiable, en donde el tiempo confiable se determina de acuerdo con el valor de identidad.

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 (1503) un tipo de identidad y una solicitud de una operación relacionada con un enclave

instanciado;

determinar (1508) un valor de identidad para el enclave con base en el tipo de identidad y la información obtenida a partir de una imagen de enclave a partir de la cual se creó una instancia del enclave;

y

realizar (1512) la operación con el valor de identidad,

en donde:

el valor de identidad se determina como una salida de una función hash;

el enclave se sometió a la creación de instancias con una pluralidad de imágenes de enclave; y

el tipo de identidad indica cuál de la pluralidad de imágenes de enclave se incluye, al menos en parte, en la función hash para determinar el valor de identidad.

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

verificar la integridad del valor de identidad al verificar una firma en la imagen de enclave con una clave pública relacionada con un autor de la imagen de enclave.

12. El sistema de acuerdo con la reivindicación 10, en donde el valor de identidad se determina como una salida de una función hash, y en donde las instrucciones producen, además, al menos las etapas de:

determinar, con base, al menos en parte, en el tipo de identidad, una porción de identidad de la imagen de enclave; y

computar la función hash con respecto a la porción de identidad.

13. El sistema de acuerdo con la reivindicación 12, en donde la imagen de enclave incluye referencias a las imágenes de enclave dependientes adicionales, y en donde las instrucciones producen, además, al menos las etapas de:

determinar, con base, al menos en parte, en el tipo de identidad, qué imágenes de enclave dependientes adicionales se incluyen como entrada a la función hash.

14. Un dispositivo informático configurado para:

recibir un tipo de identidad y una solicitud de una operación relacionada con un enclave instanciado;

determinar un valor de identidad para el enclave con base en el tipo de identidad y los datos almacenados en un contenedor de enclave; y

realizar la operación con el valor de identidad,

en donde:

el valor de identidad se determina como una salida de una función hash;

el enclave se sometió a la creación de instancias con una pluralidad de imágenes de enclave; y

el tipo de identidad indica cuál de la pluralidad de imágenes de enclave se incluye, al menos en parte, en la función hash para determinar el valor de identidad.