

CLAIMS

What is claimed is:

1. A computer implemented method, comprising:

receiving, by a source host computing device, a request to migrate secured information from ~~a-the~~ source host computing device to a destination host computing device, the request including a destination key for the destination host computing device;

performing mutual authentication between the source host computing device and the destination host computing device by:

authenticating, by the source host computing device, the destination host computing device using the destination key; and

receiving, by the source host computing device, an indication that the destination host computing device authenticated the source host computing device using a source key associated with the source host computing device;

establishing, by ~~a-the~~ source host computing device, a migration key, the migration key established by the source host computing device ~~authenticating the destination host computing device using the destination key and receiving an indication that the destination host computing device authenticated the source host computing device using a source key for the source host computing device~~ using the destination key and the source key; and

causing the secured information to be migrated from the source host computing device to the destination host computing device using the ~~established~~ migration key.

2. The computer implemented method of claim 1, wherein the secured information is a virtual machine executing on the source host computing device.

3. The computer implemented method of claim 2, wherein causing the secured information to be migrated further comprises:

copying at least a portion of random access memory (RAM) state information from the source host computing device to the destination host computing device using the ~~established~~ migration key;

stopping the virtual machine on the source host computing device; and

sending an indication to the destination host computing device to run the virtual machine on the destination host computing device.

4. The computer implemented method of claim 1, wherein the source key is a public key that is part of a key pair generated at boot time of the source host computing device, wherein the source host computing device sends the public key to an administration server, wherein the administration server is operable to initiate the request to migrate the secured information using the public key.

5. The computer implemented method of claim 1, wherein establishing the migration key is performed according to a Diffie-Hellman key exchange process.

6. The computer implemented method of claim 1, wherein causing the secured information to be migrated further comprises:

copying a set of random access memory (RAM) state information from the source host computing device to the destination host computing device, wherein the copying takes a duration of time to complete;

transmitting a set of changes in the RAM state information from the source host computing device to the destination host computing device, wherein the changes were made on the source host computing device during the duration of time taken to complete the copying.

7. The computer implemented method of claim 1, wherein the request to migrate the secured information is signed to prevent unauthorized parties from submitting the ~~at least one~~ request.

8. The computer implemented method of claim 1, wherein the request further includes a certificate for at least one of: the source host computing device or the destination host computing device.

9. A computing system, comprising:
at least one processor; and

memory including instructions that, when executed by the at least one processor, cause the computing system to:

receive at least one request to migrate a virtual machine from a source host computing device to a destination host computing device, the at least one request

including a first key and a second key, the first key being associated with the source host computing device, and the second key being associated with the destination host computing device;

perform mutual authentication between the source host computing device and the destination host computing device by:

the source host computing device authenticating the destination host computing device using the second key; and

receiving an indication that the destination host computing device authenticated the source host computing device using the first key;

establish a secure session between the source host computing device and the destination host computing device, the secure session established by using at least the first key and the second key; and

migrate the virtual machine from the source host computing device to the destination host computing device using the secure session in response to the at least one request.

10. The computing system of claim 9, wherein migrating the virtual machine further comprises:

copying at least a portion of random access memory (RAM) state information from the source host computing device to the destination host computing device using the secure session;

stopping the virtual machine on the source host computing device; and

starting a new instance of the virtual machine on the destination host computing device.

11. The computing system of claim 9, wherein receiving the at least one request to migrate the virtual machine further comprises:

receiving a first request by the source host computing device, the first request including the second key; ~~and~~ wherein the destination host computing device

receives ~~receiving~~ a second request ~~by the destination host computing device, the second request~~ including the first key.

12. The computing system of claim 9, wherein establishing the secure session further comprises:

negotiating a session key to be used for transmitting state information between the source host computing device and the destination host computing device during the secure session; and

encrypting information transmitted between the source host computing device and the destination host computing device by using the session key.

13. The computing system of claim 12, wherein negotiating the session key is performed according to Diffie-Hellman key exchange process.

14. The computing system of claim 9, wherein migrating the virtual machine further comprises:

copying a set of random access memory (RAM) state information from the source host computing device to the destination host computing device, wherein the copying takes a duration of time to complete;

transmitting a set of changes in the RAM state information from the source host computing device to the destination host computing device, wherein the changes were made on the source device by the virtual machine during the duration of time taken to complete the copying.

15. The computing system of claim 9, further comprising:

a second computing device, the second computing device including at least one second processor; and a second memory including second instructions that, when executed by the at least one second processor, cause the second computing device to:

select the virtual machine executing on the source host computing device for migration to the destination host computing device; and

submit, using an application programming interface (API), the at least one request to migrate the virtual machine, the at least one request including the first key and the second key.

CLAIMS

What is claimed is:

1. A computer implemented method, comprising:

receiving, by a source host computing device, a request to migrate secured information
5 from the source host computing device to a destination host computing device, the request including a destination key for the destination host computing device;

performing mutual authentication between the source host computing device and the destination host computing device by:

10 authenticating, by the source host computing device, the destination host computing device using the destination key; and

receiving, by the source host computing device, an indication that the destination host computing device authenticated the source host computing device using a source key associated with the source host computing device;

establishing, by the source host computing device, a migration key, the migration key
15 established by the source host computing device using the destination key and the source key; and

causing the secured information to be migrated from the source host computing device to the destination host computing device using the migration key.

20 2. The computer implemented method of claim 1, wherein the secured information is a virtual machine executing on the source host computing device.

3. The computer implemented method of claim 2, wherein causing the secured information to be migrated further comprises:

25 copying at least a portion of random access memory (RAM) state information from the source host computing device to the destination host computing device using the migration key;

stopping the virtual machine on the source host computing device; and

30 sending an indication to the destination host computing device to run the virtual machine on the destination host computing device.

4. The computer implemented method of claim 1, wherein the source key is a public key that is part of a key pair generated at boot time of the source host computing

device, wherein the source host computing device sends the public key to an administration server, wherein the administration server is operable to initiate the request to migrate the secured information using the public key.

5 5. The computer implemented method of claim 1, wherein establishing the migration key is performed according to a Diffie-Hellman key exchange process.

6. The computer implemented method of claim 1, wherein causing the secured information to be migrated further comprises:

10 copying a set of random access memory (RAM) state information from the source host computing device to the destination host computing device, wherein the copying takes a duration of time to complete;

transmitting a set of changes in the RAM state information from the source host computing device to the destination host computing device, wherein the changes were made
15 on the source host computing device during the duration of time taken to complete the copying.

7. The computer implemented method of claim 1, wherein the request to migrate the secured information is signed to prevent unauthorized parties from submitting the request.

20

8. The computer implemented method of claim 1, wherein the request further includes a certificate for at least one of: the source host computing device or the destination host computing device.

25 9. A computing system, comprising:
at least one processor; and
memory including instructions that, when executed by the at least one processor, cause the computing system to:

receive at least one request to migrate a virtual machine from a source host
30 computing device to a destination host computing device, the at least one request including a first key and a second key, the first key being associated with the source host computing device, and the second key being associated with the destination host computing device;

