

CLAIMS:

1. An apparatus, comprising:
5 a manager configured to manage access to at least one server based on authentication keys, said authentication keys being utilized between a first managed host having a client and a second managed host having a server, and said authentication keys being stored on said managed hosts;
wherein said manager is external to said first managed host and second
10 managed host,
the manager comprises a discoverer configured to discover information about said managed hosts, and
the manager is further configured to automatically manage said authentication keys stored on said managed hosts based on the discovered
15 information.
2. The apparatus according to claim 1, wherein the manager comprises a discoverer configured to discover information about at least one of trust relationships, keys, credentials, certificates, and configurations on at least one of
20 the managed hosts.
3. The apparatus according to claim 1, wherein the manager further comprises a key installer ~~(3506)~~ configured to install an authorized key on at least one of the managed hosts.
25
4. The apparatus according to claim 1, wherein the manager further comprises a key remover configured to remove an authorized key from at least one of the managed hosts.
- 30 5. The apparatus according to claim 1, wherein the manager further comprises a trust relationship installer configured to install a trust relationship between the managed hosts.

6. The apparatus according to claim 1, wherein the manager further comprises a trust relationship remover configured to remove a trust relationship from between the managed hosts.

5 7. The apparatus according to claim 1, wherein the manager further comprises a key rotator configured to rotate existing key pairs.

8. The apparatus according to claim 1, wherein the manager further comprises a trust relationship converter configured to convert an existing trust relationship of a
10 first type to a trust relationship of a second type.

9. The apparatus according to claim 1, wherein the manager further comprises a command restriction enforcer configured to add a command restriction to an existing trust relationship.

15

10. A method, comprising:

managing access to at least one server based on authentication keys, said authentication keys being utilized between a first managed host having a client and a second managed host having a server, and said authentication keys being stored
20 on said managed hosts;

wherein said managing is performed externally to said first managed host and second managed host;

discovering information about said managed hosts; and

managing automatically said authentication keys stored on said managed
25 hosts based on the discovered information.

11. The method according to claim 10, wherein the managing comprises discovering information about at least one of trust relationships, keys, credentials, certificates, and configurations on at least one of the managed hosts.

30

12. The method according to claim 10, wherein the managing further comprises installing an authorized key on at least one of the managed hosts.

13. The method according to claim 10, wherein the managing further comprises removing an authorized key from at least one of the managed hosts.

14. The method according to claim 10, wherein the managing further comprises
5 installing a trust relationship between the managed hosts.

15. The method according to claim 10, wherein the managing further comprises removing a trust relationship from between the managed hosts.

10 16. The method according to claim 10, wherein the managing further comprises rotating existing key pairs.

15 17. The method according to claim 10, wherein the managing further comprises converting an existing trust relationship of a first type to a trust relationship of a second type.

18. The method according to claim 10, wherein the managing further comprises adding a command restriction to an existing trust relationship.

20 19. A non-transitory computer program comprising computer readable program code means embodied therein, operable to cause:
managing of access to at least one server based on authentication keys,
wherein said authentication keys are utilized between a first managed host having a client and a second managed host having a server and said authentication keys are
25 stored are on said managed hosts and wherein the managing is performed externally to said first managed host and second managed host;
discovering information about said managed hosts; and
managing automatically said authentication keys stored on said managed
hosts based on the discovered information.

30

20. A system, comprising at least manager apparatus, a first managed host having a client, and a second managed host having a server, wherein the manager apparatus is configured to:

manage access to at least one server based on authentication keys, said authentication keys being utilized between the first managed host and the second managed host and said keys being stored on said managed hosts and said manager apparatus is external to said first managed host and second managed

5 host;

discover information about said managed hosts, and
automatically manage said authentication keys stored on said managed
hosts based on the discovered information.

10 21. The A-method according to claim 10, comprising:

Deploying, at the manager provided, with a security protocol management host, one of a security protocol management agent and authorization credentials for agentless security protocol management on a plurality of hosts each having at least one of a client and a server operable according to the security protocol, thereby

15 causing said hosts to become managed hosts;

discovering, with said security protocol management host, existing user authentication keys on at least a portion of said managed hosts;

analyzing, with said security protocol management host, the discovered user authentication keys to detect authorized connections between user accounts on

20 said managed hosts; and

performing, with said security protocol management host, management operations related to said security protocol on the detected authorized connections.

22. The method according to claim 21, wherein the management operations

25 include at least one of addition of an user authentication key, removal of an user authentication key, rotation of an user authentication key, addition of a trust relationship, removal of a trust relationship, conversion of an existing trust relationship of a first type to a trust relationship of a second type, and addition of a command restriction to an existing trust relationship.

30

23. The apparatus of claim 1, wherein the manager comprises a A-security
protocol management host, comprising:

at least one processor; and at least one memory including computer program code, wherein the at least one memory and the computer program code are

configured to, with the at least one processor, cause the management host at least to perform:

deploying one of a security protocol management agent and authorization credentials for agentless security protocol management on a plurality of hosts each having at least one of a client and a server configured to operate according to the security protocol, thereby causing said hosts to become managed hosts;

discovering existing user authentication keys on at least a portion of said managed hosts;

analyzing the discovered user authentication keys to detect authorized connections between user accounts on said managed hosts; and

performing management operations related to the security protocol on the detected authorized connections.

24. The ~~apparatus management host~~ according to claim 23, wherein the security protocol related management operations include at least one of addition of an user authentication key, removal of an user authentication key, rotation of an user authentication key, addition of a trust relationship, removal of a trust relationship, conversion of an existing trust relationship of a first type to a trust relationship of a second type, and addition of a command restriction to an existing trust relationship.

25. The ~~apparatus management host~~ according to claim 23, wherein the security protocol comprises secure shell protocol (SSH).

26. The apparatus according to claim 1, wherein the authentication keys comprise user authentication keys according to secure shell protocol (SSH), and the first managed host comprises an SSH client and the second managed host comprises an SSH server.

27. The method according to claim 10, wherein the authentication keys comprise user authentication keys according secure shell protocol (SSH), and the first managed host comprises an SSH client and the second managed host comprises an SSH server.