

CLAIMS:

1. An apparatus, ~~characterized in~~ comprising:
5 a manager (103, 3500) configured to manage access to at least one server based on secure shell protocol (SSH) related authentication keys, said authentication keys being utilized between a first managed host (110) having an SSH client and a second managed host (120) having an SSH server, and said SSH ~~related authentication keys being~~ stored on said managed hosts (110, 120);
10 wherein said manager (103, 3500) is external to said first managed host (110) and second managed host (120).
2. The apparatus according to claim 1, wherein the manager (103, 3500) comprises a discoverer (3502, 3700) configured to discover information about at
15 least one of trust relationships, keys, credentials, certificates, and configurations on at least one of the managed hosts.
3. The apparatus according to claim 1 ~~or 2~~, wherein the manager (103, 3500) further comprises a key installer (3506) configured to install an authorized key on at
20 least one of the managed hosts.
4. The apparatus according to claim ~~any of claims 1-3~~, wherein the manager (103, 3500) further comprises a key remover (3507) configured to remove an authorized key from at least one of the managed hosts.
25
5. The apparatus according to claim ~~any of claims 1-4~~, wherein the manager (103, 3500) further comprises a trust relationship installer (3508) configured to install a trust relationship between the managed hosts.
- 30 6. The apparatus according to claim ~~any of claims 1-5~~, wherein the manager (103, 3500) further comprises a trust relationship remover (3509) configured to remove a trust relationship from between the managed hosts.

7. The apparatus according to claim any of claims 1-6, wherein the manager ~~(103, 3500)~~ further comprises a key rotator ~~(3513)~~ configured to rotate existing key pairs.
- 5 8. The apparatus according to claim any of claims 1-7, wherein the manager ~~(103, 3500)~~ further comprises a trust relationship converter ~~(3514)~~ configured to convert an existing trust relationship of a first type to a trust relationship of a second type.
- 10 9. The apparatus according to claim any of claims 1-8, wherein the manager ~~(103, 3500)~~ further comprises a command restriction enforcer ~~(3516)~~ configured to add a command restriction to an existing trust relationship.
- 15 10. A method, ~~characterized in~~ comprising:
managing access to at least one server based on authentication secure shell protocol (SSH) related keys, said authentication keys being utilized between a first managed host ~~(110)~~ having a ~~n~~ SSH client and a second managed host ~~(120)~~ having a ~~n~~ SSH server, and said SSH related authentication keys being stored on said managed hosts ~~(110, 120)~~;
- 20 wherein said managing is performed externally to said first managed host ~~(110)~~ and second managed host ~~(120)~~.
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.
- 25 12. The method according to claim 10 ~~or 11~~, wherein the managing further comprises installing an authorized key on at least one of the managed hosts.
- 30 13. The method according to claim any of claims 10-12, wherein the managing further comprises removing an authorized key from at least one of the managed hosts.

14. The method according to claim ~~any of claims 10-13~~, wherein the managing further comprises installing a trust relationship between the managed hosts.
15. The method according to claim ~~any of claims 10-14~~, wherein the managing further comprises removing a trust relationship from between the managed hosts.
16. The method according to claim ~~any of claims 10-15~~, wherein the managing further comprises rotating existing key pairs.
17. The method according to claim ~~any of claims 10-16~~, 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 ~~any of claims 10-17~~, wherein the managing further comprises adding a command restriction to an existing trust relationship.
19. A non-transitory computer program comprising computer readable program code means embodied therein, operable to cause a computer to perform the steps of 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 stored are on said managed hosts and wherein the managing is performed externally to said first managed host and second managed host ~~any of claims 10-18~~.
20. A system, comprising at least ~~two of the apparatuses of any of claims 1-9~~. 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 host.
21. A method, ~~characterized in comprising:~~

deploying, with a security protocol ~~secure shell protocol (SSH)~~ management host, one of a security protocol ~~n-SSH~~ management agent and authorization credentials for agentless security protocol ~~SSH~~ management on a plurality of hosts each having at least one of a ~~n-SSH~~ client and a ~~n-SSH~~ server operable according to the security protocol, thereby causing said hosts to become managed hosts;

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

analyzing, with said ~~SSH~~ security protocol management host, the discovered ~~SSH~~ user authentication keys to detect authorized connections between user accounts on said managed hosts; and

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

22. The method according to claim 21, wherein the ~~SSH~~ related management operations include at least one of addition of an ~~SSH~~ user authentication key, removal of an ~~SSH~~ user authentication key, rotation of an ~~SSH~~ 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.

23. A ~~secure shell protocol (SSH)~~ security protocol management host, comprising:

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

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

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

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

5 performing ~~SSH~~-related management operations related to the security protocol on the detected authorized connections.

10 24. The ~~SSH~~-management host according to claim 23, wherein the ~~SSH~~-security protocol related management operations include at least one of addition of an ~~SSH~~ user authentication key, removal of an ~~SSH~~-user authentication key, rotation of an ~~SSH~~-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.

15

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

20

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.

25

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.