

limited to user-supplied passwords. In most systems, three consecutive false presentations results in a intelligent token account being disabled. However, if biometric authentication is incorporated into the card, it will be possible to achieve higher assurance and user authentication.

Because of the mode in which the invention is used it might be wrongly compared with a boot from a floppy disk. While it is true that inserting a intelligent token is similar to inserting a floppy, the interaction during the boot sequence is entirely different. The intelligent token-based system incorporates at least three separate authentications, user to card, card to local host, and card to remote host. These authentications are entirely absent from the floppy boot. Further, the integrity of the boot information on a floppy is protected only by an easily removed write-protect tab; while the intelligent token requires the authentication of the security officer in order to update boot information. One may also note that the ease of carrying a intelligent token as compared with a floppy disk.

The invention is described as implemented with PC's. However, the invention may be easily implemented in any computing environment including main frame, microcomputer, work station, or laptop.

While several embodiments of the invention have been described, it should be understood that the invention encompasses various modifications and alternative forms of the embodiments. It should also be understood that the specific embodiments are not intended to limit the invention, but are intended to cover all modifications, equivalents and alternatives falling within this greater scope of the claims.

I claim:

1. In a system including a local host computer and a remote host computer, a method of accessing the remote host computer comprising:

- selecting an intelligent token having critical information stored thereon;
- communicating user authentication information between a user and the intelligent token to authenticate the user to the intelligent token;
- communicating host authentication information between the intelligent token and the local host computer responsive to authentication of the user to the intelligent token to authenticate the local host computer to the intelligent token; and
- communicating user authentication information between the intelligent token and the remote host computer without further user input to allow the remote host computer access to the critical information stored on the intelligent token responsive to authentication of the local host computer to the intelligent token.

2. The method of accessing the remote host computer of claim **1** wherein communicating user authentication information between the intelligent token and the remote host computer includes: sending a request for access from the intelligent token to the remote host computer and sending a challenge from the remote host computer to the intelligent token in response to the request for access.

3. The method of accessing the remote host computer of claim **2** wherein communicating user authentication information between the intelligent token and the remote host computer further includes: storing the challenge in a memory of the remote host computer, generating a response to the challenge in the intelligent token, sending the response to the remote host computer, and validating the response using the stored challenge.

4. The method of accessing the remote host computer of claim **3** wherein the challenge is randomly generated.

5. The method of accessing the remote host computer of claim **3** wherein the response to the challenge is based on a secret.

6. the method of accessing the remote host computer of claim **2** wherein communicating user authentication information between the intelligent token and the remote host computer includes validating the response to the challenge using the remote host computer.

7. An intelligent token for use in a computer system, comprising:

- a CPU;
- a first memory unit storing an operating system; and
- a second memory unit storing authentication information for a local host computer and access information for a remote domain to provide a user with access to the local host computer and the remote domain.

8. The intelligent token of claim **7** wherein said second memory unit stores critical information for a remote host computer.

9. The intelligent token of claim **8** wherein the critical information includes authentication information for the remote host computer.

10. The intelligent token of claim **8** wherein the critical information includes a remote access code.

11. The intelligent token of claim **7** wherein the operating system includes an operating system of a local host computer.

12. A system comprising:

- a local host computer;
- a remote domain in communication with said local host computer; and
- an intelligent token coupled to said local host computer, said intelligent token including a memory storing authentication information for said local host computer and access information for said remote domain to provide a user with access to said local host computer and to said remote domain.

13. The system of claim **12** wherein said remote domain includes a network of computers.

14. The system of claim **12** wherein said remote domain includes a remote host computer.

15. The system of claim **14** wherein said intelligent token includes means for generating a request for access to said remote host computer and said remote computer includes a challenge generator that generates a challenge responsive to the request for access and transmits the challenge to said intelligent token.

16. The system of claim **15** wherein said intelligent token includes means for generating a response to the challenge and the remote host computer includes means for validating the response.

17. In a system including a local host computer and a remote domain, a method of accessing the local host computer and the remote domain comprising:

- selecting an intelligent token having critical information stored thereon including boot information, host access codes;
- reading the host access code from the intelligent token;
- validating the host access code in the local host computer;
- reading boot information from the intelligent token upon validation of the host access code;
- executing the boot operation using boot information read from the intelligent token;
- communicating user authentication information between the intelligent token and the remote domain, the remote