

REAL-TIME DATA PROTECTION METHOD AND DATA PROTECTION
DEVICE FOR IMPLEMENTING THE SAME

This invention relates to a data protection method,
particularly to a real-time data protection method.

5 As the information industry progresses, computers
and the Internet, through which computer information
are accessed, have become indispensable communication
tools in our daily lives. This results in proliferation
of hackers who intentionally and maliciously intrude
10 into a computer system and alter or destroy data or
programs in the computer system. This poses a major threat
to the reliability of computer information. Various
techniques have been proposed to counter that threat.

One conventional technique utilizes a computer
15 firewall. Unfortunately, computer firewalls have
security loopholes that may be exploited by a hacker
to get through the computer firewall and gain access
to information in a computer.

In another conventional technique, input data are
20 manually inspected to determine whether the input data
have been modified. This conventional technique,
however, is time consuming.

In yet another conventional technique, a program
calculates a hash value for each packet of input data
25 using a hash function and stores the input data in a
storage device. A different hash value calculated at
a later time indicates whether or not the corresponding

packet of the input data has been modified. The modified input data may be recovered using an original copy of the input data previously stored in the storage device. This conventional technique is disadvantageous in that a large capacity storage device is required. In addition, the program is vulnerable to viruses and hackers.

Embodiments of the present invention seek to provide a real-time data protection method that can overcome the aforesaid drawbacks of the prior art.

Embodiments of the present invention also seek to provide a data protection device that implements the real-time data protection method.

According to an aspect of the present invention, a real-time data protection method is implemented by a data protection device coupled to an input device and a computing device, the real-time data protection method comprising: A) configuring the data protection device to receive input data from the input device; B) configuring the data protection device to store the input data received in step A); C) configuring the data protection device to send the input data stored in step B) to the computing device, the computing device generating result data based on the input data sent thereto by the data protection device; D) configuring the data protection device to receive the result data from the computing device ; E) configuring the data protection device to generate test data that correspond to the result data received in step D); F) configuring the data protection device to compare the

test data generated in step E) to the input data stored in step B); and G) when it is determined in step F) that the test data are not identical to the input data, configuring the data protection device to indicate that
5 the result data have been modified.

According to another aspect of the present invention, a data protection device comprises a comparing unit and a test data-generating unit. The comparing unit is adapted to be coupled to an input device and a computing
10 device, and is configured to receive input data from the input device, to store the input data received thereby, and to send the input data to the computing device. The computing device generates result data based on the input data sent thereto by the comparing unit. The test
15 data-generating unit is coupled to the comparing unit, is adapted to be coupled to the computing device, and is configured to receive the result data from the computing device, to generate test data that correspond to the result data received thereby, and to send the
20 test data generated thereby to the comparing unit. The comparing unit is further configured to receive the test data sent thereto by the test data-generating unit, to compare the test data received thereby to the input data stored thereby, and to indicate that the result data
25 have been modified when it is determined thereby that the test data are not identical to the input data.

Other features and advantages of the present

invention will become apparent in the following detailed description of the preferred embodiment with reference to the accompanying drawings, of which:

Figure 1 is a circuit block diagram of the preferred embodiment of a data protection device according to the present invention; and

Figures 2 and 3 are flow charts of the preferred embodiment of a real-time data protection method according to the present invention to be implemented using the data protection device shown in Figure 1.

Referring to Figure 1, the preferred embodiment of a data protection device 3 according to this invention is shown to include a comparing unit 31 and a test data-generating unit 32.

The comparing unit 31 is connected to an input device 1, a computing device 2, and a storage device 5.

The input device 1 may be a computer keyboard, a computer mouse, or a touch panel.

The computing device 2 is installed with an operating system, and a word processing application program 24, e.g., Microsoft Word, which resides in the operating system, and is connected to a display device 4.

The storage device 5 stores therein first, second, and third executable files, each of which has an attribute that is set to hidden.

The test data-generating unit 32 is connected to the comparing unit 31 and the computing device 2.

The data protection device 3 further includes a controlling unit 33 connected to and controlling operations of the comparing unit 31 and the test data-generating unit 32.

5 The preferred embodiment of a real-time data protection method to be implemented by the aforementioned data protection device 3 according to this invention will now be described with further reference to Figures 2 and 3.

10 In step 51, the comparing unit 31 sets the attributes of the first, second, and third executable files stored in the storage device 5 to read-only, and subsequently installs the first, second, and third executable files into the computing device 2, whereby the first, second,
15 and third executable files serve as first, second, and third application programs 21, 22, 23 that reside in the operating system, respectively.

 In step 52, the comparing unit 31 receives input data from the input device 1.

20 In step 53, the comparing unit 31 stores therein the input data received in step 52.

 Alternatively, in this step, the input data may be stored in the storage device 5.

 In step 54, the comparing unit 31 sends the input
25 data stored in step 53 to the first application program 21.

 The first application program 21 receives the input

data sent thereto by the comparing unit 31, generates result data based on the input data received thereby, and sends the result data to the word processing application program 24.

5 The second application program 22 detects the result data generated by the first application program 21, and sends the result data detected thereby to the third application program 23.

10 The third application program 23 receives the result data sent thereto by the second application program 22, and sends the result data received thereby to the test data-generating unit 32.

15 In step 55, the test data-generating unit 32 receives the result data sent thereto by the third application program 23.

 In step 56, the test data-generating unit 32 generates test data that correspond to the result data received in step 55.

20 For example, suppose that the first application program 21 is a Chinese input method editor (IME). Suppose further that the input data received in step 52 are in the form of pinyin. The result data generated by the first application program 21 are thus associated with Chinese characters and the test data generated in this
25 step are thus in the form of pinyin.

 In step 57, the test data-generating unit 32 sends the test data generated in step 56 to the comparing unit

31.

In step 58, the comparing unit 31 receives the test data sent thereto in step 57.

5 In step 59, the comparing unit 31 compares the test data received in step 58 to the input data stored in step 53.

10 In step 60, when it is determined in step 59 that the test data are not identical to the input data, the flow proceeds to step 61. Otherwise, i.e., it is determined in step 59 that the test data are identical to the input data, the flow proceeds to step 62.

15 In step 61, the comparing unit 31 indicates that the result data have been modified, prompts the third application program 23 to discard the result data, generates a warning message, and sends the warning message to the third application program 23. Thereafter, the flow goes back to step 52.

20 The third application program 23 controls the display device 4 to show the warning message sent to the third application program 23 by the comparing unit 31.

25 In step 62, the comparing unit 31 indicates that the result data have not been modified, stores the result data received in step 55 in the storage device 5, and sets an attribute of the result data stored thereby to hidden. Thereafter, the flow goes back to step 52.

The result data stored in this step can be used for data recovery when required in the future.

From the above description, since the comparing unit 31 stores an original copy of the input data, based on which the computing device 2 generates the result data, since the test data-generating unit 32 generates the test data that correspond to the result data, and since the comparing unit 31 compares the test data to the original copy of the input data stored thereby, the data protection device 3 of this invention determines in real-time whether the result data have been modified.

Furthermore, since the attributes of the first, second, and third executable files are set to read-only prior to installation thereof in the computing device 2 by the comparing unit 31, the first, second, and third executable files are prevented from being modified.

CLAIMS:

1. A real-time data protection method to be implemented by a data protection device coupled to an input device and a computing device, said real-time data protection method comprising:

A) configuring the data protection device to receive input data from the input device;

B) configuring the data protection device to store the input data received in step A);

C) configuring the data protection device to send the input data stored in step B) to the computing device, the computing device generating result data based on the input data sent thereto by the data protection device;

D) configuring the data protection device to receive the result data from the computing device;

E) configuring the data protection device to generate test data that correspond to the result data received in step D);

F) configuring the data protection device to compare the test data generated in step E) to the input data stored in step B); and

G) when it is determined in step F) that the test data are not identical to the input data, configuring the data protection device to indicate that the result data have been modified.

2. The real-time data protection method as claimed in Claim 1, further comprising:

H) when it is determined in step F) that the test data are identical to the input data, configuring the data protection device to indicate that the result data have not been modified.

5 3. The real-time data protection method as claimed in Claim 2, the data protection device being further coupled to a storage device, wherein step H) includes the sub-steps of:

10 h1) configuring the data protection device to store the result data received in step D) in the storage device; and

 h2) configuring the data protection device to set an attribute of the result data stored in sub-step h1) to hidden.

15 4. The real-time data protection method as claimed in Claim 1, the data protection device being further coupled to a storage device, wherein, in step B), the input data is stored in one of the data protection device and the storage device.

20 5. The real-time data protection method as claimed in Claim 1, the computing device being coupled to a display device, wherein step G) includes the sub-steps of:

 g1) configuring the data protection device to prompt the computing device to discard the result data;

25 g2) configuring the data protection device to generate a warning message; and

 g3) configuring the data protection device to send

the warning message generated in sub-step g2) to the computing device, the computing device controlling the display device to show the warning message sent thereto by the data protection device.

- 5 6. The real-time data protection method as claimed in Claim 1, the data protection device being further coupled to a storage device, said real-time data protection method further comprising:

10 I) configuring the data protection device to set an attribute of an executable file stored in the storage device to read-only; and

15 J) configuring the data protection device to install the executable file into the computing device, thereby permitting the computing device to generate the result data.

7. The real-time data protection method as claimed in Claim 1, the data protection device being further coupled to a storage device, said real-time data protection method further comprising:

20 I) configuring the data protection device to set an attribute of an executable file stored in the storage device to read-only; and

25 J) configuring the data protection device to install the executable file into the computing device, thereby permitting the computing device to send the result data generated thereby to the data protection device.

8. The real-time data protection method as claimed in

Claim 1, the result data generated by the computing device being associated with Chinese characters, wherein the test data generated in step E) are in the form of pinyin.

9. A data protection device, comprising:

5 a comparing unit adapted to be coupled to an input device and a computing device, and configured to receive input data from the input device, to store the input data received thereby, and to send the input data to the computing device, the computing device generating
10 result data based on the input data sent thereto by said comparing unit; and

 a test data-generating unit coupled to said comparing unit, adapted to be coupled to the computing device, and configured to receive the result data from the
15 computing device, to generate test data that correspond to the result data received thereby, and to send the test data generated thereby to said comparing unit;

 wherein said comparing unit is further configured to receive the test data sent thereto by said test
20 data-generating unit, to compare the test data received thereby to the input data stored thereby, and to indicate that the result data have been modified when it is determined thereby that the test data are not identical to the input data.

25 10. The data protection device as claimed in Claim 9, wherein said comparing unit is further configured to store the result data received by said test

data-generating unit from the computing device when it is determined thereby that the test data are identical to the input data.

11. The data protection device as claimed in Claim 9,
5 wherein said comparing unit is further configured to generate a warning message, and to send the warning message generated thereby to the computing device when it is determined thereby that the test data are not identical to the input data, the computing device
10 controlling a display device to show the warning message sent to the computing device by said comparing unit.

12. The data protection device as claimed in Claim 9, wherein said comparing unit is further configured to prompt the computing device to discard the result data
15 when it is determined thereby that the test data are not identical to the input data.

13. The data protection device as claimed in Claim 9, the result data generated by the computing device being associated with Chinese characters, wherein the test
20 data generated by said test data-generating unit are in the form of pinyin.