DATA PROCESSOR SYSTEMS

The present invention relates to data processor systems, and particularly to a processor unit for use with a general purpose data processor system, such as a personal computer. The invention is especially useful as a security unit to be attached to a computer and its peripheral units to enable the computer to perform various security functions in a manner which does not jeopardize the security information, and the invention is therefore described below with respect to such an application.

Security functions, such as encryption, decryption, the computation of a message authentication code (MAC), digital signature geneation, public key certification, etc., are often performed in a dedicated processor unit to be attached to a general purpose computer. Such an attached processor isolates the secret data, e.g., keys and passwords, from the general purpose computer in a manner so as not to compromise the secured activities while permitting the general purpose computer to perform the non-secured activities. However, a general purpose computer, such as a PC (personal computer), provides a large set of possible ways of compromising the security, e.g., Trojan horse or virus software. Since the general purpose computer must be able to communicate with the security unit, and since the software of the general purpose computer is corruptible, it is possible to compromise secret information or to "trick" the security unit into performing improper operations involving security risks. Where the security unit may have special purpose I/O devices, such as a smartcard reader, the danger of compromising security is even increased.

Ideally, to minimize security risks, the following rules should be observed:

(1) Secret key operations should be performed in the privacy of the security unit to be attached to the general purpose computer, and not in the general purpose

computer where such data may be compromised, e.g., by resident Trojan horse software;

(2) The password or personal identification number (PIN) used to allow access to secret keys (via data encryption or other means) should not pass through the general purpose computer since, if this secret information is keyed into the general purpose computer, it may be compromised, e.g., by resident Trojan horse software;

(3) There should be no opportunity of having data to be signed, encrypted or authenticated, being forged by resident Trojan horse software in the general purpose computer. This is of particular importance in the context of digital signatures. The corrupted general purpose computer may display one set of data on the display terminal, and may request that the attached security unit sign a completely different set of data.

One way of addressing these problems is to provide the security unit with its own independent keyboard, display, printer, and/or other interface hardware components, such that the data processor system would have two keyboards in the immediate vicinity of the general purpose computer, two displays, etc., one for the computer and one for the security unit. However, such systems requiring the duplication of keyboards, displays, printers, etc., are very costly, are inconvenient to use because the work area is cluttered with extra but seldom used keyboards, displays, etc., require an independent power supply, and/or require additional data links.

It would therefore be highly desirable to provide a processor unit in general, and a security unit in particular, which may be used with a conventional computer unit, keyboard unit, etc., but which takes over control of the connecting lines between the computer unit and its perhipheral units. It would be particularly desirable to provide such a capability in a security unit so as to prevent the compromise of security information to be processed in the security unit.

THIS SHEET HAS BEEN
REPLACED

According to the present invention, there is provided, for use in a data procesor system including a computer unit and a keyboard unit communicating with the computer unit via keyboard ports in the keyboard unit and computer unit, a processor unit connectible between the computer unit and the keyboard unit; the processor unit comprising: a keyboard I/O port connectible to the keyboard port on the keyboard unit for receiving data inputted from the keyboard unit; a memory for storing the inputted data; a keyboard I/O port connectible to the keyboard port on the computer unit; a processor storing a plurality of programs for operating the processor unit according to either a Transparent Mode wherein the stored data inputted from the keyboard unit via the keyboard I/O port is transmitted via the keyboard I/O port to the computer unit, or according to a Special Handling Mode; and control means for controlling the processor to select either the Transparent Mode or a Special Handling Mode.

According to further features in the described preferred embodiment, the processor unit further includes a smartcard reader/writer for reading data from and/or writing data into a smartcard inserted therein, which data is also stored in the memory. The control means also controls the processor to process such data according to the selected mode of operation.

The novel processor unit thus takes over control of the connecting lines between the computer unit and its peripherals. Such a capability is particularly useful where the processor unit is a security unit for performing various security functions while isolating the computer unit from its peripherals so as not to jeopardize security information.

Preferably, and according to the preferred embodiment described below, the control means comprises preprogrammed software automatically controlling the processor according to the commands inputted from the keyboard unit or the computer unit. It is contemplated,

This Sheet Has Been Replaced



however, as described in a second embodiment, that the control means could comprise a manual switching device for manually selecting either the Transparent Mode or a Special Handling Mode.

It will thus be seen that the present invention addresses the above-described security problems by having the peripheral I/O devices (e.g., keyboard, display, printer, etc.) of the data processor system connected via cables to the security unit, and not to the computer unit. The security unit has another set of I/O ports connected via cables to the I/O ports of the computer unit and its peripheral devices. This means that the security unit can "take over control" of the peripheral devices, effectively disconnecting them from the computer unit, and thereby assure the user that the data to or from the peripheral devices is not compromised or forged by resident software in the computer unit. Usually, the peripheral I/O devices, will be "transparently connected" to the security unit, in that the security unit simply passes the data flow transparently. Where security is not to be compromised, however, these peripheral devices will be effectively disconnected from the computer unit so as to prevent the possibility of corruption or compromise of the data by the computer unit.

A data processor system including a security unit constructed in accordance with the present invention provides a number of advantages:

1. Such a system provides a large saving in cost because peripheral I/O devices (keyboards, displays, printers, etc.) need not be duplicated for the security unit;

2. Such a system can also use the higher-quality peripheral devices generally provided for the computer unit, rather than the lower quality peripheral devices generally provided for the security unit;

3. Such a system is more convenient for the user, in that the work area is not cluttered with extra but seldom used keyboards, displays, etc.;

4. Such a system does not require an independent power supply for the security unit, since it can use the power line to the keyboard as a source of power; and

5. Such a system requires no additional data link cables for communication, as data communication between the computer unit and the security unit can be done using the conventional keyboard, printer, video or other connections.

Further features and advantages of the invention will be apparent from the description below.

The invention is herein described, by way of example only, with reference to the accompanying drawings, wherein:

Fig. 1 is a block diagram illustrating one form of data processor system including a security unit constructed in accordance with the present invention;

Fig. 2 is a flow chart illustrating the main program run of the security unit included in the data processor system of Fig. 1;

Figs. 3-12 are flow charts illustrating a plurality of Special Handling Mode programs which may be stored in the security unit of Fig. 1; and

Fig. 13 is a block diagram illustrating another manner of connecting the security unit into a data processor system in accordance with the present invention.

The data processor system illustrated in Fig. 1 of the drawings includes a conventional computer unit CU, such as a PC general purpose computer, a conventional keyboard unit KU, and a conventional display unit DU commonly provided in such systems. Also illustrated in Fig. 1 is a separate security unit SU capable of performing various sensitive security functions such as encryption, decryption, computation of a message authentication code (MAC), digital signature generation, public key certification, etc. Security unit SU is connected to the computer unit CU,

keyboard unit KU, and display unit DU in a manner enabling the security unit to communicate with all of the above units to perform non-secured activities in the normal manner, but also to isolate secret data (such as keys and passwords) from the computer unit so as not to permit the latter unit to compromise or corrupt such secret data.

The keyboard unit KU includes a conventional I/O port 2, and similarly the display unit DU includes a conventional I/O port 4, which ports are normally connected to I/O port 6 and I/O port 8 of the computer unit CU. In this case, however, the keyboard I/O port 2 is connected to a keyboard I/O port 10 in the security unit SU; and the latter unit includes another I/O port 12 which is connected to the I/O port 6 of the computer unit CU; similarly, the security unit SU includes a display I/O port 14 connected to the corresponding port 8 in the computer unit CU, and another display I/O port 16 connected to the corresponding port 4 in the display unit DU. Thus, the security unit SU isolates the computer unit CU from its peripheral keyboard unit KU and display unit DU.

The security unit SU includes a keyboard interface 20 for controlling the flow of data between its two keyboard I/O ports 10 and 12. The keyboard interface 20 is in turn controlled by a processor, generally designated 22, including a CPU 24, a RAM/ROM memory 26, an I/O system 28, and a real-time internal clock 30. The operating software is stored in the ROM section of memory 26, and the other data is stored in the RAM section of this memory. The real-time clock 30 keeps track of the time and date independently of the real-time clock generally included in the computer unit CU.

The processor 22 further controls a display interface 32 to the display I/O port 16 connected to the display unit DU. The security unit SU further includes its own display 34, such as an LCD or LED display, also controlled by the display interface 32, e.g., for indicating the status of the security unit. The security unit SU

THIS SHEET HAS BEEN REPLACED

further includes a speaker controlled by processor 22 to generate sounds (e.g., warning signals) at appropriate times, as will be described more particularly below.

Finally, the security unit SU includes a smartcard reader/writer 38 adapted to receive a smartcard 40 for reading information from the smartcard and/or writing information into it, according to particular commands.

The processor 30 in the security unit SU stores a plurality of programs for operating the system. The plurality of programs are stored in the ROM section of memory 26, and are selected according to the data and commands introduced into the security unit via the computer unit CU, the keyboard KU or the smartcard 40. This data is stored in the RAM section of memory 26, while the command associated with the data is examined to determine whether a security function is involved. If not, the security unit operates according to a "Transparent Mode" wherein the stored data inputted via the keyboard unit KU or the smartcard 40 is transmitted via the I/O ports 12, 16, to the computer unit CU or display unit DU after a minor time delay; however, if a security function is involved, as determined by the command associated with the inputted data, the processor 22 of the security unit SU operates according to a Special Handling Mode, depending on the command involved.

Fig. 2 is a flow chart illustrating the main program run of the security unit SU. Thus, upon start, the hardware is initialized (block 51), and the security unit SU then begins its main loop. For any data (D) received from any unit connected to the security unit, e.g., the keyboard unit KU or the display unit DU, the security unit SU checks to see if the data is a special sequence for a command (C). If not, the data is sent to the intended unit for that data. For exmaple, if the data was received from the keyboard unit KU via its I/O port 2 and was intended to the I/O port 6 of the computer unit CU, the data enters the security unit SU via its I/O port 10, and after processing,

This Sheet Has Been Replaced

is fed from its I/O port 12 to the I/O port 6 of the computer unit. Thus, in this mode the security unit is "transparent", and all units connected to it function as if the security unit were not there, except for the delay in transferring the data by te security unit.

If, however, the data involves a special sequence for a command specifying a Special Handling Mode, the appropriate Special Handling Mode program is executed.

It is to be noted that the main loop as illustrated in Fig. 2 is a forever-loop: it only ends upon power failure. The command can be active or inactive, depending on the existence of the appropriate program in the memory of the security unit SU. Some programs (e.g., the load program of Fig. 3) are always active and they reside in the ROM section of the memory 26. Other programs, however, e.g., some new version of one of the other programs, may still be unloaded, and the command will only cause an error message from the security unit SU to the computer unit CU.

Figs. 3-12 illustrate some example programs which handle commands as described above.

Fig. 3 illustrates the program for the Load command, in which the security unit SU receives a program and a signature from the computer unit CU (block 60), computes the program's fingerprint (block 61), and checks to see whether the signature is valid (block 62). If not, it produces a warning (block 63), in a manner described more particularly below with respect to Fig. 12; but if the signature is valid, it loads the program and activates the appropriate command (block 64).

The commands may be stored in a Look-up Table within the ROM section 26 of the security unit SU. If needed, a special sequence may be added to the table which identifies the commands.

Fig. 4 illustrates the program for Generate Smartcard command. To generate the information for the smartcard 40 (Fig. 1), the security unit SU first obtains the information from the smartcard's user from the computer

unit CU (block 65). The password is then introduced into the security unit via the keyboard unit KU (block 66). This assures that no virus programs can be steal the password as the password never reaches the computer unit CU. Assuming no escape sequence is initiated by the operator (block 67), e.g., by the operator depressing an escape key because of an error, the security unit SU generates the RSA keys (block 68); and the information about the user and the RSA keys is written into the smartcard 40 (block 69).

RSA is a special algorithm used in ciphering and deciphering, and includes a public key involving public information available to anyone, and a private key which is used with the password to decipher the enciphered message. Further details of this ciphering and deciphering system are described, for example, in US Patent 4,405,829.

Fig. 5 illustrates the program when the command is Read Smartcard Public Information. Under this command, the smartcard is read (block 70), and the public data is sent to the computer unit CU (block 71). It is to be noted that the computer unit has no access to the private data (e.g., the RSA keys) which is on the smartcard.

Fig. 6 illustrates the operations performed when the command is Login Smartcard. Here, the data is read from the smartcard (block 72); and the current time and date are read at the same time from the internal clock 30 (block 73). A decision is then made (block 74) whether the smartcard time has expired (e.g., valid only during certain times, or up to a certain deadline). If the smartcard has expired, a warning is produced (bock 75), as described more particularly below with respect to Fig. 12. If the smartcard did not expire, the user then enters the user's password via the keyboard unit KU (bock 76). If no escape sequence has been selected (block 77), and the entered password is valid (block 78), the security unit SU sets its Smartcard mode to the "Logged in" Mode (block 79), wherein the information is read from the smartcard.

Fig. 7 illustrates the operations for the command Logoff Smartcard, wherein the security unit SU sets the Smartcard Mode to the "Logged off" Mode (block 80).

Fig. 8 illustrates the operations performed when receiving the Read Clock Command. When receiving this command, the security unit reads its internal clock 31 (block 81) and transmits the current time and date to the computer unit CU (block 82).

Fig. 9 illustrates the operations when receiving the Change Password Command. During this operation, the password must be entered via the keyboard unit KU (block 83) and assuming no escape sequence has been selected (block 84), and the entered password is valid (block 85), a new password may then be entered via the keyboard unit KU (block 86). Again, assuming no escape sequence is selected (block 87), the new password is stored on the smartcard (block 88).

Fig. 10 illustrates the operations when receiving the command: Perform diagnostics. This command causes the security unit CU to energize all its indicator lamps and wait for the user's acknowledgment (block 90). Then, the existing programs are checked off by Checksum (block 91), and the results, as well as the programs' version numbers, are sent to the computer unit CU (block 92).

Fig. 11 illustrates the operations when receiving the command: RSA sign block. When receiving this command, the security unit SU checks to see whether the Smartcard Mode is locked in (block 93); if not, it actuates a warning (block 94), as described more particularly below with respect to Fig. 12; but if the Smartcard Mode is logged in, the security unit SU receives a block of data from the computer unit CU (block 95) reads the RSA keys from the smartcard (block 96), signs the block with the keys (block 97), and sends the signed block to the computer unit CU (block 98).

Fig. 12 illustrates the Warning Program, which is an internal program by which the other programs warn the

computer unit CU. Thus, the security unit SU sends a warning message to the computer unit CU (block 100) through one of its lines (e.g., the computer unit's keyboard line), beeps its internal speaker 36 (block 101), disables the display (boock 102), and waits for a password from the keyboard unit KU (block 103). Only when the correct password has been entered (block 104) is the display enabled again (block 105).

It will be seen that the above-described system, the control for controlling the processor 22 of the security unit SU, to select either the Transparent Mode (Fig. 2), or one of the Special Handling Modes (Figs. 3-12), is by pre-programmed software stored in the memory 26 of the security unit SU, which software automatically controls the security unit according to the command data inputted, i.e., via the keyboard unit KU or the smartcard 40. It is contemplated, however, that the control means could also be in the form of a switchbox connected to the computer unit, peripheral devices, and the security unit. Such an arrangement is illustrated in Fig. 13, wherein it will be seen that the switchbox SB is connected between the computer unit CU, its peripheral devices KU and DU, and the security unit SU, and enables manually selecting either the Transparent Mode, or a Special Handling Mode, such as described above with respect to Figs. 3-12. Such an implementation of the invention is less preferable than the software implementation described above, but has the advantage over the previous known systems in that the security unit, with or without the smartcard reader, is not cluttered with many cables leading to and from it as in the previously known arrangements.

It will also be appreciated that the above description illustrates the invention as implemented in a data processor system including a general purpose computer, such as PC, the invention could be implemented in other types of data processor systems, such as one including a work station or the like.

THIS SHEET HAS BEEN REPLACED

WHAT IS CLAIMED IS:

1. For use in a data processor system including a computer unit and a keyboard unit communicating with the computer unit via keyboard ports in the keyboard unit and computer unit, a processor unit connectible between said computer unit and said keyboard unit; said processor unit comprising:

a keyboard I/O port connectible to said keyboard I/O port on the keyboard unit for receiving data inputted from said keyboard unit;

a memory for storing said inputted data;

a keyboard I/O port connectible to said keyboard I/O port on the computer unit;

a processor storing a plurality of programs for operating the processor unit according to either a Transparent Mode wherein the stored data inputted from the keyboard unit via said keyboard I/O port is transmitted via said keyboard I/O port to said computer unit, or according to a Special Handling Mode;

and control means for controlling said processor to select either the Transparent Mode or a Special Handling Mode.

2. The processor unit according to Claim 1, wherein said unit further includes a smartcard reader for reading data from a smartcard inserted therein, which data is also stored in said memory; said control means also controlling said processor to process the data inputted via said smartcard reader according to the selected mode of operation.

3. The processor unit according to Claim 2, wherein said unit further includes a smartcard writer for writing data onto a smartcard inserted therein; said control means also controlling said processor to write data on the smartcard according to the selected mode of operation.

4. The processor unit according to Claim 3, wherein said processor unit is a security unit capable of performing various security functions.

This Sheet Has Been Replaced

This Sheet Has Been Replaced



THIS SHEET HAS BEEN REPLACED



5. The security unit according to Claim 3, wherein said programs stored in said processor of the security unit include a plurality of Special Handling Modes of operation.

6. The ~~security~~ unit according to Claim 5, wherein said stored Special Handling Modes includes a Load Program Mode, wherein the security unit receives a program from the computer unit, receives a signature, computes the program's fingerprint, checks to determine whether the signature matches the program's fingerprint, and if so, loads the program into the computer unit.

7. The security unit according to either of Claims 5 or 6, wherein said stored Special Handling Modes includes a Generate Smartcard Mode, wherein the security unit receives information from the smartcard's user from the computer unit, receives a password from the keyboard, generates ciphering, deciphering keys, and writes information received from the computer unit and the ciphering, deciphering keys into the smartcard.

8. The security unit according to any one of Claims 5-7, wherein said stored Special Handling Modes include a Read Smartcard Mode, wherein the inserted smartcard is read, and only the public data is sent to the computer unit.

9. The security unit according to any one of Claims 5-8, wherein said security unit further includes an internal real-time clock, and wherein said stored Special Handling Modes include a Login Smartcard Mode, in which data is read from an inserted smartcard, the current time and date are read from the internal clock, and a warning is produced if the current time and date on the smartcard do not match the current time and date read from the internal clock.

10. The security unit according to Claim 9, wherein said stored Special Handling Modes further include a Sign Block Mode, wherein the security unit checks to determine whether the Smartcard Mode is logged in, issues a

THIS SHEET HAS BEEN REPLACED

* C L M S *

warning signal if it is not; and if it is, receives a block to sign, reads the signature keys from the smartcard, signs the block, and sends the results to the computer unit.

11. The security unit according to any one of Claims 5-10, wherein said stored Special Handling Modes include a Change Password Mode, wherein the old password and the new password are both entered in the keyboard, and a new password is generated and is recorded on the inserted smartcard, or is used to enter data on the smartcard, or is used as an internal PIN for the smartcard.

12. The security unit according to any one of Claims 5-11, wherein the security unit includes light indicators; and wherein said stored Special Handling Modes include a Perform Diagnostic Mode, wherein all said indicators are energized, the existing stored programs are checked, and the results are transmitted to the computer unit.

13. The security unit according to any one of Claims 1-12, wherein said unit further includes two display I/O ports connectible to the computer unit and a display unit, respectively; said control means also controlling said processor to transmit data via said display port to the display unit.

14. A processor unit connectable between a computer unit and a keyboard unit in a data processor system, substantially as hereinbefore described with reference to, and as illustrated in, the accompanying drawings.

This Sheet Has Been Replaced