



159159

The present invention concerns a fail-safe down-loading system of a terminal.

It is known that down-loading can be effected from data processing machines, but the problem that arises is to protect these machines from untimely or even fraudulent down-loading operations. Thus, if a machine has memories divided into certified program zones "CPZ" and into non-certified program zones "NPZ", it is necessary to provide means that can ensure that the programs down-loaded into the certified zone have been so down-loaded by a procedure that guarantees that they have not been subject to fraud. Furthermore, there is also the problem of proposing a flexible hybrid system that also makes it possible, as desired and according to the application, to be highly protected or open to a greater or lesser extent.

Another problem to be solved is to provide the terminal with means for carrying out authorisations for programs to be transferred between memory zones with different security levels.

Document EP-A-0.218.176 discloses means for loading an instruction into a microprocessor card, in one given memory zone thereof among several: to this end the instruction contains a piece of information defining the memory zone to be loaded. However, there is no provision to transfer an instruction from one zone of the card to another.

Document EP-A-0.205.095 also discloses a method of security data transmission between a host computer and peripherals: these data are encrypted over the path connecting these apparatuses. However, the data are not routed into a given zone of the receiving apparatus.

The invention therefore concerns a system according to the subject-matter of Claim 1.

Other characteristics and advantages of the present invention will become more clearly apparent on reading the following description given with reference to the attached drawings in which:

- Figure 1 gives a diagrammatic view of a system according to the invention;
- Figure 2 shows the organisation chart of the memories of a terminal;



G00002

- Figure 3 shows the content of the word of the two registers expressing the possibilities offered to the terminal;
- Figure 4 summarises the division of the memories of the terminal;
- Figure 5 shows a down-loading procedure according to the invention;
- Figure 6 shows the information transfers that can be carried out between the entities of the invention.

Figure 1 shows a main or host computer (1), connected by a data transmission line (2) to a terminal or reader (3) remote from that main computer (1). This terminal (3) contains a set of memories (30, 31, 32) organised as follows. A first memory (31) is constituted by a RAM-type volatile memory, a second memory (32) is constituted by a RAM-type non-volatile memory backed up by an EEPROM memory or stack, and a third memory (30) is constituted by a PROM- or ROM-type resident memory. The terminal also has a reader (33) of portable objects (34) constituted by a microcomputer circuit, comprising a microprocessor and a programmable memory, capable of connection to the outside by contacts. For further details on the constitution of such a portable object, reference may be had to patent application FR 2 401 459 corresponding to US patent 4 211 919 and, for details on the microcomputer associated with a programmable memory, reference may be had to patent application FR 2 461 301 corresponding to US patent 4 382 279.

These memories as a whole are used as an executable and interpretable program memory and as a working zone constituted by general usage registers. The working zone is essentially constituted by a portion (314) of the RAM memory (31). The program memory (Fig. 2) contains twenty memory pages, each of sixteen kbytes, of the volatile memory (31). The non-volatile memory is constituted by thirty-six sixteen-kbyte pages of the memory (32) and the resident memory is constituted by eight sixteen-kbyte pages of the memory (30). Each volatile memory zone, non-volatile memory zone and resident memory zone is subdivided into two or three sub-zones known as certified program zone "CPZ", non-certified program zone "NPZ" and mailbox "BL".

The subdivisions of the memories define security levels for the programs contained in these memories. In this way, the programs installed in a "CPZ" zone will be described as of a certified security level, while the programs installed in an "NPZ"

zone are programs of a non-certified security level. The mailboxes are access zones controlled by a key. They contain essentially data. An interpreting and order-handling program (GdC) resident in a ROM- or PROM-type memory (35) carries out interpreting between programs written in a highly evolved compact language, independent of the hardware used, and the language specific to the microprocessor installed in the terminal. As for the order handler, it is given the task of executing an order authorised by one of the command bytes ECW1, ECW2 described below. The widest access rights are given to this interpreting and order-handling program, said rights being higher than those of the "NPZ" or "CPZ" zones. The programs installed in the "CPZ" zones of the memory allow reading/writing in all the "NPZ", or "CPZ" zones, both of the volatile memory (31), and of the non-volatile memory (32) or the resident memory (30) and only reading and writing under the control of the interpreting program and of an application program in the mailbox zones, with reading and writing rules defined by the application program, at the time that the mailbox is created. Programs installed in the "NPZ" zones (311, 321, 301) are assigned the non-certified security level and only have the right to perform reading/writing in the "NPZ" zone (311, 321) of the volatile non-volatile and resident memories, and can only perform reading and writing under the control of the interpreter in the mailbox zones (313, 323) of the volatile (31) or non-volatile (32) memories.

Figure 4 summarises the division of the memories of the terminal and the different access rights to these memories.

The functioning of the system will be explained below.

Initially, a terminal equipped with a reader contains, in the non-volatile memory zone, at least one instruction CHSB, the command bytes of which, in association with this instruction, allow certain orders sent by the down-loading host computer to be accepted or otherwise. This instruction CHSB has two command bytes "ECW1", "ECW2", the bits of which, illustrated in Figure 3, are loaded into the registers of the working memory (314) at the addresses FFEB and FFEC of the latter, to indicate to the order handler the orders that can be accepted or otherwise. At the time of the execution and decoding of an instruction to down-load, to launch a program, to read, or to start a session, the order handler will read the command bytes. In this way,

moving on from the least significant bits to the most significant bits, the first bit of the first byte ECW1 authorises the down-loading and reading of the NPZ zone;

the second bit authorises the down-loading and reading of the "CPZ" zone;

the third bit authorises the external launching from the host (1) of a program in "NPZ";

the fourth bit authorises the external launching from the host (1) of a program in "CPZ";

the fifth most significant bit, constituted by the first bit of the second command word ECW2, authorises the down-loading and reading of a register bank constituted by a portion of the working memory (314);

the sixth bit, constituted by the second bit of the second byte ECW2, authorises the start of a session.

When the bits of these two words are set to zero, the corresponding orders to down-load, to launch a program or to start a session are not taken into account by the order handler of the terminal, and when these bits are set to one, the orders are taken into account.

When the terminal is delivered, the words ECW1, ECW2 have their bits positioned, by default, so as to allow all the possibilities for accepting the different orders. This therefore allows the host computer to down-load directly, into "CPZ" zone, a program "TELE SEC" (3220) which will subsequently make it possible to carry out security down-loading. It being possible for this down-loading to be preceded or otherwise by certification or authentication.

Another solution can also consist in delivering terminals already equipped in a "CPZ" zone (322) of the non-volatile memory of a security down-loading program. This program modifies, if necessary, the registers ECW1/ECW2 and executes a set of instructions that make it possible to bring into play two possible scenarios. In a first scenario, the program down-loaded by the host computer can, by a "GOTO" or "CALL" branch instruction followed by the address (ADCPZ1) of the start of the security down-loading program "TELE SEC", call up this program installed in the "CPZ" zone, it being imperative for this program to start with an ENTRY instruction. This program "TELE SEC", illustrated in Figure 5, contains among other things a

TPP instruction RSC1, RSC2 and ends with an "RET" instruction handing over to the program located in "NPZ".

The "ENTRY" instruction is an obligatory entry point for a routine of certified level for any program located in NPZ. This makes it possible to prevent the host or a program in "NPZ" from being able to access any point of a program located in "CPZ". Thus, as illustrated in Fig. 5, where the program in "NPZ" contains an instruction "CALL AD CPZ2" requesting branching to the address CPZ2 of a zone "CPZ" and where the instruction to this address is other than an "ENTRY" instruction, the interpreter will detect a prohibited access.

The TPP instruction makes it possible to copy over a program memory block SC1 into a block of program memory SC2. However, before this instruction is executed the interpreter will check, by comparing the address at which this TPP instruction is located and the address of the memory block SC2, that this instruction is executable. Indeed, where the TPP instruction is located in the "NPZ" memory zone and requests copying over from a block of program memory located in an "NPZ" zone to a program memory block located in a "CPZ" zone, the interpreter does not authorise the execution of this instruction. In this case the interpreter will stop or be diverted to an error-processing sub-program in order to indicate to the user that it did not want to execute this instruction.

In fact, the interpreter carries out systematic monitoring of any instruction, wherever it comes from, manipulating an address in order to check whether the place that it is asking to access is authorised on the basis of the place from which this instruction comes. By this means a check is made that the program levels corresponding to the place from which the instruction comes is indeed in accord with the access authorisations corresponding to this level as given by Figure 4. Thus the word ECW1 must have the bit 0 and the bit 2 at level "1" and the word ECW2 must have the bit 1 at level "1" in order to permit the start of a down-loading session, for example. Only the possibility of down-loading and reading in "NPZ" zone and of launching a program in "NPZ" zone is retained. Consequently, any program down-loaded by the host in "NPZ" zone will comprise an instruction to call up the program "TELE SEC" stored in a "CPZ" zone, which will permit transfer from a memory block of an "NPZ" zone to a memory block of a "CPZ" zone.

Another scenario can consist in down-loading a program "X" in "NPZ", then in having this program authenticated by an authentication and certification program in "CPZ". The program "X" can be launched by a "RUN" launch instruction coming from the host if ECW authorises this.

If the program "X" is launched while it is in an "NPZ" zone, it has few rights. Another possibility consists in having the program "X" installed in "CPZ" zone, as has been seen above and, in this case, it will have all the rights of a program in "CPZ" zone.

An authentication procedure can, for example, be a procedure similar to that described in French patent application no. 86 08 654 of 16 June 1986 filed in the name of Bull CP8. Similarly, a procedure for certifying the authenticity of data can, for example, be a procedure similar to that described in French patent application no. 86 10 206 filed on 11 July 1986 in the name of Bull CP8. By modifying the command words ECW1/ECW2, it has been seen that it is possible to modify the conditions of down-loading from an "NPZ" zone to a "CPZ" zone and the order handler is capable of determining these conditions by reading the command words ECW1/ECW2 that are stored in the registers of the working zone.

We should note that ECW1, ECW2 determine a number of levels:

- the start of a session can be authorised or not:
if "not" the machine is shut down completely.
- the start of a session is authorised:
then it is possible to load either into "CPZ" or "NPZ", depending on ECW. But the external launch may very well be prohibited in order to allow for the possibility of authentication internally by a CALL or GOTO instruction making it possible to divert to the authentication program. In order for the "RUN" launch to be authorised, if it was not already, it is authorised by modifying ECW.

The possibilities and flexibility of the system of the invention are illustrated by Figure 6.

The diagram shown in Figure 6 presents the information transfers that can be made between the following entities of the invention:

- NPZ zone of the program memory,

- CPZ zone of the program memory,
- resources, which can be a keyboard, display panel, etc.
- data memory constituted by a portion of the RAM (31),
- host.

The arrows in the figure indicate the direction of the information flow and the text associated with the arrow defines:

- the instruction that permits the transfer action.

The instructions are:

- OUT or IN, input/output instructions,
- TPP, transfer from program memory to program memory,
- TPR or GPTR, transfer from program memory to data memory,
- TRP or PPTR, transfer from data memory to program memory.
- The type of memory where the instruction has to be located. The type is specified by one or two letters attached to the mnemonic.

The lower case "c" specifies that the instruction is in CPZ only. The lower case letters "n, c" specify that the instruction is in CPZ or NPZ. For example, the loop marked 60 denotes that it is possible to transfer information from CPZ to CPZ solely through the TPP instruction installed in CPZ.

Exchanges represented by the reference 61 specify that it is possible to transfer information between the resources of the system and the CPZ zone solely through an input/output instruction installed in CPZ zone.

Exchanges represented by the reference 62 specify that it is possible to transfer information between an NPZ zone and another entity of the system solely through an instruction installed in CPZ or in NPZ.

As concerns the order handler, this will execute the down-loading/reading orders depending on the value ECW1/ECW2, which is positioned through the CHSB instruction installed only in CPZ.

CLAIMS

1. System comprising a terminal (3) connected by a transmission line (2) to a central unit (1), the terminal comprising:

- a microprocessor and a memory divided into a program memory and a working random access memory (314), the working random access memory being constituted by registers, the program memory comprising a volatile memory (31), a non-volatile backed-up memory (32) and a resident memory (30), characterised in that each of the memories constituting the program memory is split into at least one zone known as "non-certified" (NPZ 311, 321, 301) intended to receive programs of a non-certified security level, and one zone known as "certified" (CPZ 312, 322, 302) intended to receive programs of a certified security level, higher than that of the non-certified zone, the execution of an instruction to transfer a program from a non-certified zone to a certified zone being subject to a procedure of checking access rights to the certified zone;

and in that the terminal comprises:

- an interpreter and order-handling program arranged so as to perform interpretation between a compact, advanced and independent language of the terminal used, and a language specific to said microprocessor, and to execute orders sent to the terminal, this program being able to access each of the parts of the memory;
- a program for monitoring down-loading (TELESEC) comprising at least one instruction (CHSB) having a control word (ECW) stored in one of said registers of said working random access memory and defining whether the down-loading of a program into the various zones from a source outside the terminal is authorised, the control word (ECW) having a value defined by said instruction (CHSB) as a function of predetermined rights given to the terminal, the interpreter and order-handling program executing an order to down-load a program after having read the control word (ECW) and verified that it authorises this order.

2. System according to Claim 1, characterised in that said process for checking access rights comprises an authentication of the content of the program located in a non-certified zone (NPZ).
3. System according to Claim 1, characterised in that said procedure for checking access rights comprises verification that said instruction to transfer a program is stored in a certified zone (CPZ).
4. System according to Claim 3, characterised in that it is only possible to access the program monitoring down-loading at a program address starting with a specific instruction (ENTRY).
5. System according to Claim 1, characterised in that the control word (ECW) comprises:
 - a first field intended to control down-loading and reading in a non-certified zone (NPZ);
 - a second field intended to control down-loading and reading in a certified zone (CPZ);
 - a third field intended to authorise the launch of a program in a non-certified zone (NPZ);
 - a fourth field intended to authorise the launch of a program in a certified zone (CPZ);
 - a fifth field intended to control down-loading and reading of the registers of the working memory (314); and
 - a sixth field making it possible to authorise the start of a session;

the interpreter and order-handling program executing or not, depending on the control word, the down-loading, reading and launch of a program in one of the aforementioned regions, or the start of a session.