

Description

Multiuser data processing system with memory protection

A data processing system generally has as the main resources a processor and a memory. In the memory there are stored, on the one hand, the command instructions to be processed by the processor, on the other hand the processor can write processing results back into the memory. Usually, the memory altogether available, i.e. addressable by the processor, is subdivided into at least two individual areas. In the first area, which is referred to in the following as the operating system memory area, there is entered during the manufacture of the data processing system a so-called operating system coding, with which in particular the hardware components of the system are managed. In the second area, which is referred to in the following as the user memory area, programs and data created by users of the data processing system themselves can be stored.

From the viewpoint of the processor of a data processing system, there is in fact no distinction drawn between these two memory areas. In particular, it is immaterial whether, as is the case with mobile data processing systems, such as for example processor chip cards, the entire address area of the microprocessor is physically divided into an unalterable memory (for example ROM) for the operating system and a non-volatile application memory (for example EEPROM). Utilizing the entire address area, if required, the processor accesses any memory element, irrespective of whether it is in the operating system memory area or in the user memory area. However, this has the consequence that, by means of an individual program code, i.e. user command instructions which have been stored by a user in a user memory area reserved for him of the mobile data processing system,

both the operating system memory area and user memory areas assigned to other users, and the user programs or user data installed there, can be accessed unhindered in a reading and/or altering manner intentionally or
5 coincidentally.

In EP 05 61 509 A1 there is represented a networked computer system with a multiplicity of user terminals and input and output interfaces. The computer system is operated by an operating system, such as for
10 example a UNIX operating system instruction set. In the computer system, operating system commands intended for users for input and output interfaces can generally be inhibited. Monitored by the operating system, they can be called up or activated by a user of the computer system
15 by an additional operating system command if the said user has an access authorization stored in a memory.

In DE 41 15 152 A1, a data-protecting microprocessor circuit for portable data media is disclosed. This circuit contains an additional protective circuit,
20 decoupled from the actual microprocessor circuit, which ensures that an unknown program can access only those memory areas which are authorized for access. In this case, in a first embodiment, the additional protective circuit contains a first comparator with auxiliary
25 register and a second comparator with auxiliary register. The user-dependent limit values for accesses to memory areas are stored either in hard-wired logic or in safe memories and are loaded into the auxiliary registers by the actual microprocessor circuit. These limit values are
30 compared by the comparators with the address register and the program counter of the actual microprocessor circuit. The output values of the comparators are logically combined by an AND gate and passed to the control circuit of the actual microprocessor circuit. In a second hard-
35 ware variant, the additional protective

circuit contains an own back-up processor with frequency clock dividing circuit and own memory arrangement. In the latter, the user-dependent limit values for accesses to memory areas are stored and are compared by the back-up
5 processor with the address register and the program counter of the actual microprocessor circuit.

The invention is thus based on the object of specifying for a portable chip card memory access protection which manages as far as possible without any
10 intervention in the hardware structures of the chip card.

The object is achieved by, first of all, the processor being adapted, in particular with respect to the internal microcode, in such a way that the execution of standard commands of the processor which are loaded in
15 a user memory area and request reading or writing access to the content of memory cells is inhibited. In the operating system memory area there is, furthermore, a memory area access table, in which there is stored per user memory area the authorized address area for the
20 commands loaded in the respective user memory area. Finally, in the operating system of the processor there is an additional program routine which is called up by a command loaded in a user memory area and requesting reading or writing access to a memory cell, and checks by
25 means of the memory area access table before command execution whether the access to a memory cell requested by the respective command lies in the authorized address area, and otherwise inhibits the execution of the command.

30 The invention has the advantage that the "radius of action" of one or more application programs contained in the user program memory area can be restricted in a simple way by software means alone to a specific area of the memory of the data processing system, without addi-
35 tional hardware components being required. The

address area of the memory enabled for writing and reading accesses of commands of a user program can be stored user-dependently in the memory area access table. Generally, the authorized address area will coincide with
5 the user memory area made available to a user and containing an individual user program code. Consequently, a user is denied writing and reading accesses by means of his user program code from the user program memory area assigned to him to memory cells which lie either in the
10 user memory area assigned to another user or in the operating system memory area.

The invention is further explained with an example represented in the figure. This shows a typical division of the memory of a data processing system, also
15 referred to as memory layout. In this case, the memory is essentially divided into two parts. An upper, so-called operating system memory area, the address area of which begins at the start address 0000h (h = hexadecimal coding), serves for receiving the operating system code.
20 The operating system essentially organizes the controlling of the microprocessor, the operation of any further resources of the data processing system there are and the accesses to the memory. An adjoining user memory area, the address area of which in the example represented
25 begins at a start address 8000h (h = hexadecimal coding), serves for receiving the application program and application data codings of generally various users. This memory area is consequently divided itself into individual subareas. In the example of the figure, two such sub-
30 areas are represented. One area, extending for example from the start addresses 8000h to 8FFFh, is provided for a user A for receiving a user program code and user data code. An adjoining area, extending from the start addresses 9000h to 9FFFh, is provided for a second user
35 B, likewise for

receiving a user program code and user data code. From the following start address A000h to the end of the memory, with the address FFFFh, there may adjoin subareas assigned to further users.

5 In the example represented, consequently the user A, for example, to whom the user memory area in the address area from 8000h to 8FFFh has been assigned, can, on account of a user program code installed therein, access only user data of which the code is likewise
10 stored in cells of which the address area extends from the starter address 8000h to the end address 8FFFh. This is ensured according to the invention by a corresponding entry in the cell of the operating system memory area denoted by "user program A" in the memory area access
15 table. In the example of the figure, this is represented by a permissible program branch of the user program code A, denoted by S1, represented by a solid line and directed forwards, within the own user program memory area. All other program branches extending from this user
20 program memory area, for instance a branch S5 extending into the operating system memory area or a branch S3 extending into the neighbouring user program memory area of the user A having the range width 9000h to 9FFFh, are impermissible and are consequently not executed. These
25 are respectively represented in the figure by a dotted line.

 In the same way, with the application program code installed by a further user B in the user program memory area from 9000h to 9FFFh, it is only possible to
30 execute reading or writing accesses to memory cells lying within the own user program memory area, for example the backwardly directed program branch S2. An access originating from this user program memory area and directed at the memory area of the user A, represented in the figure
35 by a dotted line

S4, are likewise impermissible and can be prevented according to the invention.

The adaptation of the processor with respect to its internal microcode is advantageously performed in such a way that, before the execution of standard commands of the processor which request reading or writing access to the content of memory cells, first of all the current content of the program counter of the processor belonging to the respective standard command is checked. This "points" as it were to the source address of the command currently awaiting execution. If the situation arises in which the content of the program counter refers to the address of a memory cell lying in the operating system memory area, the command is thus, for example, an integral part of the operating system, the execution of the command is enabled. If this is the case, the origin of the command is consequently not user-dependent but system-dependent. If, on the other hand, the situation arises in which the content of the program counter refers to the address of a memory cell lying in the user memory area, the execution of the command is inhibited. In this case, the source of the command is clearly user-dependent.

According to the invention, the execution of such commands is made possible by the indirect way via the program routine present in the operating system of the processor. This routine is advantageously designed in such a way that first of all the current content of the stack of the processor belonging to the respective command requesting reading or writing access to a memory cell is checked. Contained in this stack is the return address of the command, which likewise reflects the "source" of the command awaiting execution. Then, the entry belonging to the content of the stack in the memory area access table is compared with the access to a memory cell requested by the respective command. If the situation arises in which the requested access refers to a memory cell lying outside the authorized address area contained in the memory area access table,

the execution of the command is inhibited, otherwise it is enabled.

5 A data processing system according to the invention is suitable in particular for mobile use, since specifically in that case concurrent use by a plurality of users is often necessary. Each user can in this case use the data processing system undisturbed by possible other users and without adverse effects, possibly only unintentional, on the programs and data of the other
10 users. In particular, the data protection of the users among one another is safeguarded, and unauthorized, possibly also unprofessional, reading and writing interventions in the operating system from an application program code installed in a user program memory area are
15 prevented. Particularly suited as mobile data processing systems according to the invention are processor chip cards.

This Sheet Has Been Replaced



Patent Claims

1. Portable chip card having a processor and a memory, which is divided into an operating system memory area and at least one user memory area, in which card
- 5 a) the processor is adapted with respect to the internal microcode in such a way that the execution of processor standard commands which are loaded in a user memory area and request reading or writing access to the content of memory cells is inhibited,
- 10 b) in the operating system memory area there is a memory area access table, in which there is stored per user memory area the authorized address area for the processor standard commands loaded in the respective user memory area, and
- 15 c) in the operating system of the processor there is a program routine which
- c1) is called up by a processor standard command loaded in a user memory area and requesting reading or writing access to a memory cell,
- 20 c2) checks by means of the memory area access table whether the access to a memory cell requested by the respective processor standard command lies in the authorized address area, and
- c3) otherwise inhibits the execution of the processor standard command.
- 25



2. Device according to Claim 1, the adaptation of the processor with respect to the internal microcode being performed in such a way that

- 5 a) before the execution of the processor standard commands which request reading or writing access to the content of memory cells, the current content of the memory counter of the processor belonging to the respective processor standard command is checked,
- 10 b) in the event that the content of the program counter refers to the address of a memory cell lying in the operating system memory area, the execution of the processor standard command is enabled, and
- 15 c) in the event that the content of the program counter refers to the address of a memory cell lying in the user memory area, the execution of the processor standard command is inhibited.

3. Device according to Claim 1 or 2, the program routine present in the operating system of the processor being designed in such a way that

- 20 a) the current content of the stack of the processor belonging to the respective processor standard command requesting reading or writing access to a memory cell is checked, and
- 25 b) the entry belonging to the content of the stack in the memory area access table is compared with the access to a memory cell requested by the respective processor standard command, and



- c) in the event that the requested access refers to a memory cell lying outside the authorized address area contained in the memory area access table, the execution of the processor standard command is inhibited.

5

