



159159

VEHICLE SECURITY SYSTEM



G00002

Field of invention

- 5 The present invention relates to security systems for granting access and enabling operation of a vehicle.

Background of invention

- 10 Nowadays, vehicles such as cars are typically provided with a central processor unit (CPU), which provides computerised operation and control. This has led to widespread use of remote locking systems, in which the processor unit is responsive to an infra-red-based remote key to unlock a car door.
- 15 With such systems, in the event that a locked car is broken into, an alarm is given off which will alert the public to the break-in. However, such systems are usually overly sensitive and are prone to raising false alarms even when there is no intentional forced entry. Therefore, the general public is usually de-sensitised to the alarm and does not always recognise a car theft even when the car is
- 20 driven away by a thief.

There are available some vehicle security systems which use wireless positioning technology for tracking stolen cars, e.g. GPS (Global Positioning Systems). GSM, CDMA, 3G etc.. However, these systems require a special

network and hardware. For example, a special radio channel/frequency band, receiver (Rx) and transmitter (Tx) stations are required for tracking the location of a transponder concealed in the stolen car, which are costly to provide.

Furthermore, such systems are service-provider-dependent; the car owner must
5 subscribe to service of a service provider providing such tracking in order to track his car.

Such systems thus have disadvantages in preventing theft and tracking stolen cars. There is therefore a need for a better means of protecting a car from
10 unauthorised access and use, and for a means, in the event that the car has been stolen and driven off, to locate and retrieve the stolen car.

Summary of the invention

15 In a first aspect, the invention provides a vehicle security system comprising a vehicle processor unit capable of disabling and enabling operation of the vehicle wherein the processor unit is arranged to enable the vehicle when an identifying signal from a mobile phone is detected.

20 In a second aspect, the invention provides a vehicle security system comprising, a processor unit capable of disabling and enabling the vehicle, wherein the processor unit enables the vehicle when an identifying signal from a mobile phone is detected and the processor unit continuously enables the

vehicle when the identifying signal from the mobile phone is periodically detected.

In a third aspect, the invention provides a method of enabling a vehicle

5 comprising the steps of a) a processor unit in the vehicle detecting the presence of a mobile phone; b) the processor unit enabling a function in the vehicle in response to said detection; and c) repeating steps a) and b) and disabling the vehicle when the mobile phone ceases to be detected.

10 In a fourth aspect, the invention provides a remote vehicle communication system comprising a processor unit, the processor unit being responsive to a signal from a mobile phone and the mobile phone being responsive to a signal from a network service provider, wherein the network service provider is able to remotely instruct the processor unit to operate one or more functions.

15

The invention therefore provides the possibility of having an advantage of enabling a vehicle to operate by continual permission of the owner. Therefore, if the vehicle is stolen or taken away, the owner can request the network provider to locate the vehicle.

20

Furthermore, the invention provides the possibility of having an advantage of reducing the number of gadgets carried by the owner of a vehicle and a mobile phone.

Brief description of the drawings

Embodiments of the invention will now be described by way of example, with reference to the accompanying drawings in which:

5

Figure 1a illustrates an embodiment of the present invention;

Figure 1b illustrates a flowchart of an embodiment of the embodiment of figure 1a;

10

Figure 2 is an expanded flowchart of the embodiment of figure 1b;

Figure 3 illustrates a flowchart of a second embodiment of the invention; and

15 Figure 4 illustrates a further function of the embodiments.

Detailed description of the preferred embodiments

20 In a first embodiment, a car is fitted with a vehicle security system (VSS) which comprises a mobile phone used to enable the car to be driven. The owner of the car also owns the mobile phone which is registered with a processor unit in the car. The processor unit is of a conventional design which controls operation of car functions from engine ignition timing to air compressor functions. In this

embodiment, at least one operation of the processor essential for vehicle operation, such as ignition timing, is disabled in an initial state.

5 The vehicle security system (VSS) also comprises an interface board which is shown in Figure 1a. The interface board 502 communicates with and is controlled by the processor unit 501 of the vehicle, via input/output ports 501a, 502a on the interface board 502 and on the processor 501.

When the owner attempts to start the car, the processor unit 501 is triggered to
10 communicate with the interface board 502 to poll wirelessly for presence of the mobile phone 305 within a specific detection distance of the interface board 502 (for example, within the car). Preferably, the polling is done by a Bluetooth transmitter/receiver. Alternatively, the mobile phone may be detected by the processor unit 501 via a hardwire cabling 504b, of the sort which is known in
15 the art such as USB, between the interface 502 and the mobile phone 305. Figure 1a also shows the alternative hardwire cable link 504b, in which case, the hardwire cable link may optionally provide power for operating the mobile phone 305.

20 In response to the polling, the mobile phone 305 sends a signal which contains an identification of itself to the Bluetooth transceiver 502b. The interface board then forwards the signal to the processor unit 501. If the mobile phone 305 is thus detected by the processor unit 501, the processor unit 501 enables certain operations in the car which are for starting the car, for example the engine

ignition timing control function in the car. On the other hand, if the mobile phone 305 is not detected, the processor unit 501 disables certain operations critical for starting the car. Preferably, these operations are disabled by default until enabled by the processing unit 501. In this way, as long as the processing unit 501 does not enable the disabled operation, the car engine cannot start and the car cannot thus be driven away.

Even after the mobile phone 305 has been detected by the processor unit 501 via the interface board 502 and the car engine has started, the processor unit 501 continues to poll for the presence of the mobile phone 305 at regular intervals, via interface board 502. If at any interval the mobile phone 305 ceases to be detected, the processor unit 501 will disable the selected function. Thus, even while the car is being driven, the car will be forced to cruise to a stop if the mobile phone 305 can no longer be detected at any point in time. Optionally, the operation may be disabled by a time period, for example 60 seconds from the time when the processor 501 determines that the mobile phone 305 is not (or is no longer) present. Therefore, in order for the operation to be enabled continuously, the mobile phone 305 is kept in an operation mode (so that the mobile phone 305 can respond to the polling) and is kept within a detectable range of the interface board.

The mobile phone 305 is registered with the processor unit 501 by having the mobile phone's International Mobile Equipment Identification (IMEI) number and phone number entered into the memory of the processor unit 501.

The IMEI (International Mobile Equipment Identity) numbering system is a 15 digit unique code that is used to identify the mobile phone to the network. The IMEI is internationally unique to every mobile phone and is programmed or

5 burned into the mobile phone 305 by the mobile phone's manufacturer. When a phone is switched on, its unique IMEI number is transmitted and checked against a database of phones in the network's EIR (Equipment ID Register).

This EIR determines whether the phone can log onto the network to initiate and receive calls.

10

When polled by the interface board 502, the mobile phone 305 responds to the polling with a signal containing the IMEI of the mobile phone 305. The IMEI is independent of any SIM (Subscriber Identity Module) in the mobile phone 305 (the SIM's serial number is known as the International Mobile Subscriber

15 Identification, IMSI, which is unique to the SIM, not the mobile phone).

By using the IMEI instead of the IMSI in this embodiment, the enablement of the car is independent of the SIM inside the mobile phone 305 but is reliant on the mobile phone 305 itself. Therefore, the car and mobile phone 305 form a pair.

20

The IMEI may be pre-programmed into the processor unit 501 by the car's manufacturer or car dealer before the car is sold to the owner, or a method of registering the IMEI of the mobile phone with the processor unit 501 may be provided to the owner.

For example, the interface board 502 may have a card reader 502d with which the car owner on his/her own may register the mobile phone 305 with the processing unit.

5

Preferably, the card reader 502d is integrated with the interface board 502 and may be a magnetic card reader, smart card reader or a reader for any other type of security cards. In order to register a mobile phone into the memory of the processor unit 501, the driver first let the card reader read the security card.

10 The security card is one which has been pre-registered with the processor unit 501 and, thus, the card reader is able to authenticate the security card.

Preferably, the card is pre-registered with the processor unit by the manufacturer/car dealer who sold the car. When the card reader 502d has authenticated the security card, the interface board 502 sends out polling

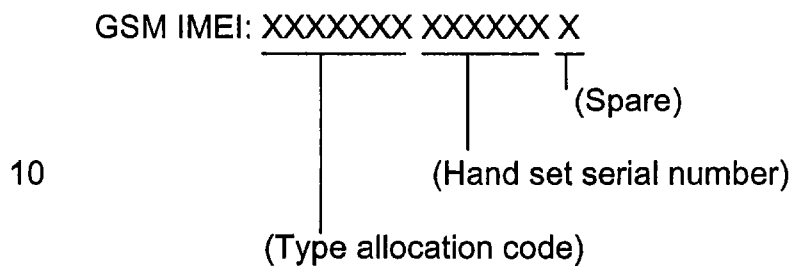
15 signals to search for the presence of a new mobile phone 305 which has not been registered in the memory of the processor unit 501. When such a new mobile phone 305 is detected, the mobile phone's identity, in this example the IMEI, is obtained and the interface board 502 then registers the mobile phone 305 identity into the memory of the processor unit 501.

20

As the IMEI of the mobile phone 305 is used for registration with the processor unit 501 of the car, the mobile phone 305 owner's choice of tele-communication network service provider (SIM) is not critical or relevant to enabling the car. In fact, the presence of a SIM in the mobile phone 305 is not necessary for

enabling the vehicle and is only needed for the mobile phone 305 to communicate with the phone network provider.

An example of an IMEI sequence according to GSM ("Group Special Mobile") standard is:



As described above, the mobile phone 305 must be in operation and within a detectable distance of the wireless polling of the interface board 502 in order for the car to be enabled. Thus, even if the car is stolen, perhaps because the owner of the car left his mobile phone 305 inside the car, the car is traceable to the mobile phone 305 by the tele-communication network service provider with which the mobile phone 305 is registered, at a first level, by simply determining the car in which the mobile phone 305 is located or, at a second level, by triangulating the location of the mobile phone 305.

Tracking of the car is possible even if the SIM card has been removed from the mobile phone 305 and is substituted by another SIM card. As mentioned above, a unique IMEI number of mobile phone 305 is transmitted and checked against

a database of phones in the network's EIR when logging in to the network service provider. Therefore, in the event that a car thief has stolen the mobile phone 305 and has driven away the car, the car owner may contact the network service provider to track the car through searching the IMEI number. The owner
5 may even request the network service provider to trace the new phone number of the new SIM card.

The present embodiment therefore improves security of the car in that a thief would have to get the mobile phone 305 first before he can get away with the
10 car. Furthermore, the present embodiment is more robust in preventing a car from being stolen and driven away than the conventional alarm-based systems.

Optionally, the car has an armed mode and an un-armed mode. In the armed mode, the embodiment is used to access and enable the car. In the un-armed
15 mode, the car is protected and operable with conventional lock and key systems. Figure 1b is a flow chart showing an example of a program routine useable in this embodiment. The program as shown in figure 1b is activated, at 100, only when set to the armed mode. In the un-armed mode, a Bluetooth transceiver 502b of the interface board 502 which is connected to the processor
20 unit in car does not poll for the presence of the mobile phone 305. In the armed mode, the processor unit 501 causes the Bluetooth transceiver 502b to emit regular polling, at 102, to search for the mobile phone 305. Furthermore, on being activated, the engine is initialised to being disabled, at 103, as the default state 101.

In order to drive the car in the armed mode, the mobile phone 305 has to be detected by the Bluetooth transceiver 502b, at 106. The detection process, at 106, entails the Bluetooth transceiver 502b sending out poll signals, at 102, and
5 receiving a response from the mobile phone, which includes the mobile phone's IMEI, to confirm the presence of the mobile phone 305 within detectable range of the Bluetooth transceiver 502b, at 104. If, at step 104, there is no mobile phone 305 which is responsive to the processor unit 501, the engine remains disabled.

10

When the mobile phone 305 responds to the polling with an IMEI, at 105, the processor unit 501 proceeds to determine if the IMEI is the one registered into its memory, at 106. If the IMEI is one which has been registered into the memory of the processor unit 501, the processor unit 501 enables the engine
15 timer, and thus enabling the engine, at 108, to be started by the owner, at 101. If the mobile phone 305 detected by the Bluetooth transceiver 502b is not the one which is registered with the processor unit 501, the processor unit 501 will continue to keep the car engine disabled, at 103.

20 Even on after successfully enabling the engine, at 108, the detection process, at 106, is cyclically repeated to enable the engine continually, at a regular interval (i.e. delay) 107, as long as the car is in operation. If at any cycle of the detection process, at 106, the mobile phone 305 ceases to be detected, the engine will be disabled, at 103. Optionally, the embodiment may be de-sensitised to disable

the engine only after a pre-determined number of non-detections of the mobile phone 305's presence. Therefore, the mobile phone 305 has to be kept within detectable distance of the Bluetooth transceiver 502b and has to be kept in continuous operation in order for the car to be enabled.

5

If the car is to be left with a car workshop for servicing, the car has first to be unarmed so that the car may be operable in the conventional way and the mobile phone is not needed for the workshop technicians to test the car. In this embodiment, the car may be unarmed using the security card.

10

An example of how to arm the car is by pressing on a button which is provided at the interface board. When the button is pressed, the car will be disabled. The processor unit first disables the engine timer. Successful disabling may be signalled by lighting up an LED of the interface board.

15

In a further example, unarming of the car needs to be done via the security card. The interface board 502 waits for the security card to be presented to the card reader 502d for authentication. If the security card is authenticated, the engine is defaulted back to an enabled state (just as in the conventional state)

20

and the car is protected in the conventional way, without using the security features of the embodiment.

When the car is unarmed, the Bluetooth transceiver stops polling for the presence of the mobile phone 305 and the interface board 502 remains passively waiting for the arming security card.

- 5 In general, the security card is only needed when unarming the car or when a new mobile phone 305 is to be registered with the processor unit 501.

Therefore, the security card may be put away in safekeeping when the car is used daily under normal armed operation. Advantageously, having a security card-based mobile phone registration system prevents a car thief from

- 10 registering a new mobile phone with the car processor unit 501 to enable the engine. Typically, the security card is provided by the car dealer who sold the car to the present owner.

- Optionally, the embodiment may also include an alarm system by which an
15 alarm is raised, at 109 (optional process distinguished by the dotted lines), after one or more specific number of failed attempts to detect or authenticate the mobile phone 305, at 104 or 106.

- The embodiment may also include a wireless car-locking system (not shown in
20 the figures) which may replace the conventional infra-red based wireless door key. For example, a button may be provided on the mobile phone for unlocking the car door. Alternatively, a special key sequence may be entered into the mobile phone via the mobile phone's keypad which will cause the mobile phone to send a signal to the car to unlock the car door. This provides the advantage

that the owner is freed from having to carry a mobile phone 305 as well as a wireless car door key. Such wireless car keys are often too bulky to be placed on a normal key ring and are carried separately. Replacing the wireless key with a mobile phone 305 may thus reduce the number of gadgets carried by the
5 owner.

The car locking system may also be linked to an alarm system wherein the alarm is set off when there is a forced entry.

10 Figure 2 is an illustration of the embodiment of Figure 1b, wherein a mobile phone 305 is registered with the processor unit in a car 303 such that the communication 307 between the processor 501 and the mobile phone 305 enables the car to be driven.

15 A network service provider 301 is able to locate the mobile phone 305, at 309, with the mobile phone 305 camped on to network.

Therefore, as a car thief who has gotten away with the car 303 and mobile phone 305 is forced to keep the mobile phone 305 in operation in order to
20 enable the car 303, the network service provider 301 is able to locate the car 305.

In the above-described embodiment, the processor unit 501 is the active component while the mobile phone 305 is the passive component responsive to

the processor unit 501's polling, via the Bluetooth transceiver. However, in a second embodiment, the processor unit 501 of the car does not search or poll for the presence of the mobile phone 305. Instead, the mobile phone 305 is the active component and sends out signals continuously to the interface board 502, i.e. the master component, and thus the processor unit 501 is responsive to the signals, i.e. the slave component. As long as the processor unit 501 in the car receives the signals from the mobile phone 305 indicating presence of the mobile phone 305, the processor unit 501 enables the car to be driven.

Optionally, the driver may have to key in a sequence of pass code into the mobile phone to trigger the sending out of signals to the processor unit 501. In this way, the mobile phone 305 does not have to be actively signalling its presence to the processor unit 501 until activated to do so, and so saves energy.

The second embodiment is also described by the flowchart of figure 3. As in figure 1b, the car is protected by the conventional lock-and-key method until armed, at 100, which sets, at 103, the engine to "disabled" as its default state 101. When the owner of the car wants to start the armed car, he activates a trigger on his mobile phone by keying in sequence of pass code from the keypad to start sending signals to the processor unit 501, at 300, via the Bluetooth transceiver. The signals include information on the IMEI of the mobile phone 305. The processor unit 501 then determines if the IMEI received is one which has been registered with the processor unit 501, at 302. If so, the

processor unit 501 enables the engine of the car by enabling the engine timer, at 108. The mobile phone 305 continues to signal to the processor the IMEI at regular intervals or delays, at 107, in order to maintain the engine enabled, at 108. If the processor unit 501 stop receiving the signal from the mobile phone 5 305 for a pre-determined period of time, the processor unit 501 disables the engine, at 103.

Alternatively, the IMEI of the mobile phone 305 may be communicated to the processor unit 501 by a cable and not wirelessly.

10

In order for the mobile phone 305 to remain sufficiently charged during a journey, the interface board 502 may have a built-in charger terminal to which the mobile phone is connected and secured while the car is in use; this ensures that the battery of the mobile phone does not flat out and that the phone is kept 15 securely in place during a journey.

In a variation of the embodiment, a plurality of mobile phones may be registered with the processor unit 501 in car so that the car may be driven by more than one authorised person.

20

The information sent to the processor unit 501 may be encoded to discourage and prevent reverse engineering of the mobile phone's IMEI number, or other identification information.

The vehicle need not be a car, it may be a motor cycle or any other form of transportation, be it for land sea or air transportation.

In a further embodiment, the mobile phone 305 is also responsive to signals
5 from the network service provider to perform functions other than disabling a car. Such other functions may include collecting data on car performance. For example, the processor unit 501 may log historical data on engine temperature, mileage etc. Therefore, the owner of the car may authorise a car maintenance garage to regularly download the data and analyse the car's condition for pro-
10 active maintenance, i.e. the car maintenance garage is permitted to contact the network service provider to send a signal to the mobile phone 305, which causes the mobile phone 305 to consolidate data logged by the processor unit 501, and forward the data to the network service provide, which then further forwards the data to the car maintenance garage. Similarly, the car's
15 manufacturer can collect data on test results conducted on their cars.

An example of such a remote operation via the service network provider of the mobile phone is illustrated in the flowchart in figure 4. A user, intending to download logged data from the processor unit 501, sends a request to the
20 mobile network service provider, at 401 (maybe by just calling the customer service person). The mobile network service provider then responds to the request by sending an instruction to the mobile phone 501. The mobile phone then communicates with the processor unit 501 via the Bluetooth transceiver, at 405, and causes the processor unit 501 to transmit log data via the mobile

phone to the network service provider, at 407, 409. The network service provider then transmits the log data to the car maintenance garage.

In general, it is preferable that the processor unit 501 (and the interface board)
5 is in a listening mode, i.e. slave component, with reference to the mobile phone except when processor unit 501 is required to consolidate the performance data of the car to send the data to the workshop.

In a further embodiment, the mobile phone is a modified one having a feature
10 that the modified mobile phone is able identify the SIM card in the mobile phone. Thus, the mobile phone may be programmed to expect a pre-determined SIM card and, thus, to determine whether the SIM card has been changed. If the mobile phone detects that the SIM card has been changed, the mobile phone's functions, especially the Bluetooth feature for communication
15 with the interface board, may be disabled. Consequently, the mobile phone is unable to handshake with the interface board to enable the vehicle. Thus, a further degree of robustness in the security features is provided in this embodiment. If both the car and the mobile phone are stolen, the car thief will not be able to enable the vehicle if he changes the SIM card in the mobile
20 phone.

In further variations of the embodiments, the interface board may be embedded in the car CPU or integrated with the car CPU. Alternatively, the interface board

may be installed remotely from the CPU board, such as on the dashboard, and is not permanently integrated into the car.

In a further variation of the embodiments, the interface board further comprises
5 a processor unit which speeds up the processing of the Bluetooth communication with the mobile phone, as well as the passing of information to the processor unit in the vehicle.

It should be understood that the embodiments described herein are but
10 embodiments of underlying concepts of the invention. Alternatives to the embodiments, though not described, are intended to be within the scope of this invention as claimed. For example, the interface board 501 is just one way of allowing communication between the processor unit 501 and the mobile phone 305. Other methods are possible within the scope of the invention, such as a
15 communication port which is in the same motherboard or integrated circuit board in which the car processor unit 501 is installed.

Claims

1. A vehicle security system comprising:
a vehicle processor unit capable of disabling and enabling
5 operation of the vehicle; wherein
the processor unit is arranged to enable the vehicle when an
identifying signal from a mobile phone is detected.
2. A vehicle security system as claimed in claim 1 wherein the processor unit
10 disables the vehicle when the identifying signal from the mobile phone is not
detected.
3. A vehicle security system as claimed in any one of claims 1 and 2 wherein
the processor unit continuously enables the vehicle when the identifying
15 signal from the mobile phone is periodically detected.
4. A vehicle security system as claimed in any one of the preceding claims
wherein the identifying signal comprises identification of the mobile phone.
- 20 5. A vehicle security system as claimed in claim 4 wherein the identification is a
unique serial number identifying the mobile phone.

6. A vehicle security system as claimed in claim 5 wherein the unique serial number is the International Mobile Equipment Identification of the mobile phone.
- 5 7. A vehicle security system as claimed in claim 5 wherein the unique serial number is the International Mobile Subscriber Identification of a SIM card in the mobile phone.
8. A vehicle security system as claimed in any one of the preceding claims
10 wherein the mobile phone is able to receive remote communication from the owner to issue to a command to the processor unit to disable the vehicle.
9. A vehicle security system as claimed in any one of the preceding claims wherein the mobile phone enables the vehicle to be located.
15
10. A vehicle security system as claimed in claim 9 wherein the mobile phone enables the vehicle to be located by GPS system or any local network service providers.
- 20 11. A vehicle security system as claimed in any one of claims 7 to 10 wherein the mobile phone is able to identify the SIM card installed in the mobile phone;
the mobile phone is able to communicate with the processor unit to enable the vehicle; and

the SIM card installed in the mobile phone being a predetermined SIM card.

12. A vehicle security system as claimed in any one of the above claims further

5 comprising an alarm; wherein

the alarm is raised when there is an attempt to start the vehicle and no identifying signal is received from the mobile phone.

13. A vehicle security system as claimed in any one of claims 4 to 10 further

10 comprising an alarm; wherein

the alarm is raised when the identification of the mobile phone is not an identification expected by processor unit.

14. A vehicle security system as claimed in any one of the above claims further

15 comprising a remote locking system wherein the processor unit locks or unlocks the vehicle for physical access on receiving a command or signal from the mobile phone.

15. A vehicle security system as claimed in any one of the above claims wherein

20 the vehicle is enabled by enabling an engine timer in the vehicle.

16. A vehicle security system as claimed in any one of the above claims wherein

the processor unit detects the identifying signal wirelessly.

17. A vehicle security system as claimed in claim 16 wherein the processor unit detects the identifying signal by Bluetooth technology.

18. A vehicle security system as claimed in claim in any one of the preceding
5 claims wherein the processor unit enables and disables the vehicle via an interface board.

19. A vehicle security system as claimed in claim 18 wherein the processor unit detects the identifying signal via the interface board.

10

20. A vehicle security system as claimed in any one of claims 18 and 19 wherein the vehicle processor unit has an unarmed mode and an armed mode; wherein

when the processor unit is set to the unarmed mode, the vehicle
15 processor unit is not capable of disabling and/or enabling the operation of the vehicle.

21. A vehicle security system as claimed in claim 20 wherein the vehicle processor is arranged to be set to the unarmed mode by a physical
20 identification means.

22. A vehicle security system as claimed in claim 21 wherein physical identification means is a smart card or magnetic strip card.

23. A vehicle security system comprising:

a processor unit capable of disabling and enabling the vehicle; wherein the processor unit enables the vehicle when an identifying signal from a mobile phone is detected; and

5 the processor unit continuously enables the vehicle when the identifying signal from the mobile phone is periodically detected.

24. A method of enabling a vehicle comprising the steps of:

10 a) a processor unit in the vehicle detecting the presence of a mobile phone;

b) the processor unit enabling a function in the vehicle in response to said detection; and

c) repeating steps a) and b) and disabling the vehicle when the mobile phone ceases to be detected .

15

25. A method of enabling a vehicle as claimed in claim 24 further comprising the step of the processor unit communicating with an interface board; wherein

20 the processor unit enables the function in which the vehicle response to said detection.

26. A method of enabling a vehicle as claimed in claims 24 or 25 wherein the mobile phone is identified by the International Mobile Equipment Identification of the mobile phone.

27. A method of enabling a vehicle as claimed in any one of claims 24 to 26

further comprising the step of:

- 5 d) raising an alarm when the presence of the mobile device is not
detected in step a)

28. A method of enabling a vehicle as claimed in any one of claims 24 to 27

further comprising the step of:

- 10 e) the mobile phone receiving a first command initiated by the owner of
the vehicle to issue a second command to the processor unit to disable
the engine.

29. A method of enabling a vehicle as claimed in any one of claims 24 to 28

wherein the processor unit has an unarmed mode and an armed mode; and

- 15 when the processor unit is set to the unarmed mode, the vehicle
processor unit is not capable of disabling and/or enabling the operation of the
vehicle.

30. A method of enabling a vehicle as claimed in claim 29 wherein the vehicle

- 20 processor is arranged to be set to the unarmed mode by a physical
identification means.

31. A method of enabling a vehicle as claimed in claim 30 wherein physical

identification means is a smart card or magnetic strip card.

32. A remote vehicle communication system comprising:

a processor unit;

the processor unit being responsive to a signal from a mobile phone; and

5 the mobile phone being responsive to a signal from a network service provider; wherein

the network service provider is able to remotely instruct the processor unit to operate one or more functions.

10 33. A remote vehicle communication system as claimed in claim 32 wherein

the processor unit is arranged to be responsive to the signal from the mobile phone via an interface board.

34. A remote vehicle communication system as claimed in claims 32 to 33

15 wherein the one or more functions includes disabling the vehicle.

35. A remote vehicle communication system as claimed in any one of claims 32 to 34 wherein

the processor unit logs information about the vehicle; and

20 the one or more functions including sending the logged information to the network service provider via the mobile phone.

36. A remote vehicle communication system as claimed in any one of claims 32 to 35 wherein the network service provider remotely instructs the processor unit to operate the one or more functions for purpose of car maintenance.

5 37. A remote vehicle communication system as claimed in any one of claims 32 to 36 wherein the one or more functions includes sending the location of the vehicle the network service provider via the mobile phone.

10 38. A remote vehicle communication system as claimed in any one of claims 32 to 37 wherein
the processor unit has an unarmed mode and an armed mode; such that
when the processor unit is set to the unarmed mode, the vehicle
processor unit is not capable of disabling and/or enabling the operation of the
vehicle.

15

39. A remote vehicle communication system as claimed in any one of claims 32 to 38 wherein the vehicle processor is arranged to be set to the unarmed mode by a physical identification means.

20 40. A remote vehicle communication system as claimed in any one of claims 32 to 39 wherein physical identification means is a smart card or magnetic strip card.