

System for detecting intrusions by reconfiguration

The present invention relates to a system for detecting intrusions, the system comprising:

- 5 - at least one mesh surface, each mesh surface comprising at least two cells, each cell comprising a pattern, a pattern being a portion of continuous electrical circuit,
- at least one interconnection surface comprising a plurality of connectors, the connectors being suitable for connecting cells of the mesh surface(s) to each other according to a first configuration of the interconnection surface for forming groups of
- 10 electrically connected cells, the patterns of the cells of each group forming a continuous electrical circuit of patterns,
- a detection module capable of detecting a modification of an impedance which is characteristic of each group of electrically connected cells.

15 The present invention also relates to an associated method for detecting intrusions.

 In the field of computer security, one issue consists of protecting the equipment through which sensitive information passes. Such equipment in particular includes printed circuits or integrated circuits. A printed circuit, also called printed circuit board, is a support making it possible to maintain a set of electronic components and electrically connect

20 them to one another. An integrated circuit, also called electronic chip, is a set of electronic components reproducing one or several electronic functions and generally integrating several types of basic electronic components in a small space.

 The tracks of a printed circuit and the connections of the electronic components connected on such a printed circuit may be subject to physical attacks. Such physical

25 attacks in particular consist of approaching probes or connecting electrodes on the tracks of the printed circuit or on the connections of components connected on the printed circuit so as to capture the signals traveling over the tracks or the connections or to inject signals. The captured signals are next used by the attackers to collect sensitive data. The injected signals are used to disrupt the exchanged signals or to cause a malfunction of the

30 equipment.

 Similar attacks may be carried out on integrated circuits.

 As a result, physical protection systems are used to protect the printed circuits and integrated circuits of such equipment from intrusions. The protection systems for example

35 comprise two- or three-dimensional protective meshes. The meshes are in particular formed from separate electrical circuits forming patterns and the continuity, or alteration, of which is verified by circulating a control current and detecting the current losses, due to

a break of the circuit, or the modification of one of the electrical characteristics of the current, due to an alteration of the circuit. The meshes are for example positioned above and/or below components of the equipment to be protected, such as the tracks and connections of a printed circuit or the layers of silicon of an integrated circuit. The meshes in particular comprise a structure and patterns chosen so as to allow the detection of intrusion attempts. When an intrusion attempt is detected, reactive actions are triggered by the protection systems for example consisting of erasing the sensitive data from the equipment.

Yet attacks being increasingly sophisticated, the structure and patterns designed for the meshes are increasingly complex, which increases the development time and cost of the meshes.

Furthermore, the protection provided by such meshes may be bypassed by attackers after a reverse engineering phase. Reverse engineering, also called reverse design, is an activity consisting of studying an object to determine its inner workings or manufacturing method.

After reverse engineering, the attacker knows the positions and properties of the different electrical circuits of the mesh. The attacker is then able to shunt some of these electrical circuits and therefore section them to free an access space to the equipment to be protected, without the protection system detecting the intrusion. The term "shunt" refers to short-circuiting an electrical circuit.

There is therefore a need for a system making it possible on the one hand to respond to sophisticated attacks without increasing the complexity of the protective meshes, therefore their development cost and production cost; and on the other hand, to make it ineffective for an attacker to short-circuit one or more electrical circuits of a mesh after reverse engineering.

To that end, the invention relates to a system for detecting intrusions of the aforementioned type, in which the system further comprises a module for configuring interconnections of the connectors, the configuration module being able to modify, over time, the first configuration to obtain at least one second configuration of the interconnection surface.

According to specific embodiments, the intrusion detection system comprises one or more of the following features, considered alone or according to any technically possible combinations:

- the configuration module is able to determine, randomly, the second configuration from among a plurality of configurations of the interconnection

surface and to reconfigure the set of interconnections of the connectors according to the second configuration.

5 - when a break in the electrical continuity of at least one continuous circuit is detected over an area of a mesh surface, the configuration module is able to modify the configuration of the interconnection surface so as to increase the number of groups of connected cells present in that area.

10 - the system comprises at least two mesh surfaces and a module for measuring variations in a property between two of the mesh surfaces, the property being chosen from among an impedance, a resistance, a capacitance and an inductance.

- at least one electrical circuit is formed by the connection, which is not reconfigurable by the configuration module, of at least two adjacent cells of a mesh surface via a component previously statically configured.

15 - the configuration module is able to move over time, over one or over each mesh surface, a zone of the mesh surface having the highest number of groups of connected cells.

- the system comprises a member capable of activating, at randomly or pseudo-randomly chosen moments, the configuration module and/or the detection module.

20 - the interconnection surface comprises a programmable component, the configuration module and the detection module being software applications integrated into the programmable component.

- the interconnection surface comprises a micro-electromechanical system piloted by actuators, the configuration module being able to actuate the actuators.

25 - the mesh surface and the interconnection surface form a physical protective barrier for the configuration module and the detection module.

- after a break has been detected in the electrical continuity of a group of connected cells, the detection module is able to apply a security policy, the security policy comprising erasing sensitive data, carrying out integrity tests and/or reconfiguring interconnections of the connectors of the interconnection surface.

30 - the detection module includes several methods for detecting a break or alteration of each group of electrically connected cells and is able to use them in a combined manner with a defined temporal interleaving, which may be pseudo-random or random.

35 The invention also relates to a method for detecting intrusions, comprising the following steps:

- providing a system for detecting intrusions as previously described,

- determining, using the configuration module, a first configuration of the interconnection surface,
- configuring, using the configuration module, interconnections of the connectors of the interconnection surface according to the first determined configuration,
- 5 - activating the detection module to detect a modification of an impedance which is characteristic of each group of electrically connected cells,
- optionally detecting, via the detection module, a modification of an impedance which is characteristic of a group of electrically connected cells, and
- 10 - modifying the first configuration of the interconnection surface, using the configuration module, to interconnect the connectors of the interconnection surface according to a second configuration.

Other features and advantages of the invention will appear upon reading the following description of embodiments of the invention, provided as an example only and in reference to the drawings, which are:

- 15 - figure 1, a schematic sectional view of one example of an intrusion detection system showing, in section, a detection film formed by an interconnection surface, mesh surfaces and a configuration module, a detection module and a reaction module,
- figure 2, a schematic top view of a first mesh surface of the system of figure 1,
- 20 - figure 3, a schematic top view of the interconnection surface of the system of figure 1,
- figure 4, a schematic top view of a second mesh surface of the system of figure 1,
- figure 5, a schematic top view of an example pattern of a cell of a mesh surface of figure 1,
- 25 - figure 6, a flowchart of an example method for detecting intrusions using a dynamic configuration of the interconnections, and
- figure 7, a flowchart of another example method for detecting intrusions using a dynamic configuration and a static configuration of the interconnections.

30 An intrusion detection system 1 is illustrated in figure 1.

The system 1 is intended to protect a piece of equipment through which sensitive information passes. The equipment for example comprises a printed circuit or an integrated circuit. The equipment is for example an encryption device or transmission equipment through which encrypted data, such as banking data, passes.

35 The system 1 is able to detect intrusion attempts coming from outside the system 1. The intrusion attempts are in particular physical attacks consisting of approaching

probes or connecting electrodes on a printed circuit of the equipment protected by the system 1.

The system 1 comprises a detection film 1A able to completely envelop the equipment to be protected or at least to cover all or some of the printed circuits and integrated circuits of the equipment. The film 1A is limited to a flat surface of the equipment and thus extends only in two dimensions or extends over at least two angularly offset surfaces and thus forms a three-dimensional surface.

The film 1A comprises at least one mesh surface 2, each mesh surface 2 comprising at least two cells 3. The film 1A further comprises at least one interconnection surface 4 of the cells 3 of each mesh surface 2.

The system 1 also comprises a module 6 for configuring, over time, interconnections of the connectors 24 of the interconnection surface 4. The system 1 also comprises a module 8 for detecting intrusions and a module 10 for reacting to intrusion attempts detected by the detection module 8.

Optionally, the system 1 also comprises a member such as a timer configured to activate the configuration module 6 and/or the detection module 8.

In the example of figure 1, the film 1A comprises two mesh surfaces 2 and an interconnection surface 4.

As illustrated in figures 2 and 4, each mesh surface 2 comprises thirty-five cells 3. The cells 3 for example have an identical surface area equal to 54 square millimeters (mm^2). Alternatively, the cells 3 have different sizes.

The cells 3 are continuous segments of conductive tracks each comprising a geometric pattern 20 covering the entire surface of the cell 3, as illustrated in figure 5. Placing the patterns 20 end to end via the interconnections of the connectors 24 forms a mesh.

Each pattern 20 is a continuous, curved electrical track, without intersections and the breaking or alteration of an electrical characteristic of which makes it possible to detect an intrusion attempt in the system 1. The patterns 20 for example have boustrophedon shapes, as shown in figure 5, or more complex shapes, for example spiral or labyrinthine.

The interconnection surface 4 is configured to connect cells 3 of a same mesh surface 2 or cells 3 of different mesh surfaces 2 in order to form a more or less complex mesh.

In the example illustrated in figure 3, the interconnection surface 4 comprises a programmable component 23 and a plurality of connectors 24.

The programmable component 23 is for example an FPGA (Field-Programmable Gate Array).

The programmable component 23 is able to activate the configuration module 6, the detection module 8, the reaction module 10, and optionally, the timer.

5 The programmable component 23 is also configured to determine the interconnections of the connectors 24 on the interconnection surface 4 and to interconnect the connectors 24 according to the determined interconnections. The programmable component for example executes an evolution function of the interconnections able to cause the interconnections of the connectors 24 to evolve over time for each group of
10 connected cells 3.

 The connectors 24 are on the one hand connected to the ends of the patterns 20 of the cells 3. The connectors 24 are on the other hand interconnected by the programmable component 23 to connect, in series, cells 3 of the mesh surfaces 2 in a first configuration, to form groups of connected cells. Such groups of cells connected in series
15 are also called "equipotential". There may be several equipotentials in parallel, each corresponding to a group of cells.

 Alternatively, the interconnection surface 4 comprises several programmable components 23.

 Alternatively, the interconnection surface 4 comprises a micro-electromechanical
20 system piloted by actuators. A micro-electrochemical system, also called MEMS, is a microsystem comprising one or more mechanical elements, using electricity as a power source, in order to perform a sensor and/or actuator function, with at least one structure having micrometric dimensions.

 The patterns 20 of the cells 3 of each group of connected cells form a continuous
25 electrical circuit of patterns. For example, figures 2 and 4 illustrate different continuous electrical circuits of patterns, the cells 3 of a same electrical circuit being represented by a same type of crosshatching or dots.

 The configuration module 6 is able to configure the interconnections of the connectors 24 according to the first configuration of the interconnection surface 4.

30 The configuration module 6 is able to configure, over time, the interconnections of the connectors 24 according to a new configuration of the interconnection surface 4. The configuration module 6 is therefore able to modify, over time, the current configuration of the interconnection surface 4 in order to obtain a new configuration of the interconnection surface 4 and to reconfigure all of the interconnections of the connectors 24 according to
35 the second configuration.

The configuration module 6 is able to determine, randomly, each configuration from among a plurality of configurations of the interconnection surface 4.

Preferably, each configuration is chosen from among a plurality of factory tested and validated configurations to avoid configuration errors or nonoptimal configurations. In this case, the determination of each configuration is pseudo-random, i.e., although the possible configurations are known, the multiplicity of the configurations does not make it possible to anticipate which configuration will be chosen by the configuration module 6.

The configuration module 6 is further able to modify the configuration of the interconnection surface 4 when an intrusion attempt is detected by the detection module 8.

In this case, the configuration module 6 is for example able to modify the configuration of the interconnection surface 4 so as to increase the number of groups of cells connected in the zone of the mesh surface 2 where an intrusion attempt has been detected. Such an increase in the number of groups of cells and therefore of continuous electrical circuits in an area is called "tightening of the mesh" in the zone. Tightening the mesh in a zone makes it possible to make the use of shunts even more complex to free an access area to the zone to be protected.

Alternatively, the configuration module 6 is able to increase or decrease the number of cells of a group over part of the interconnection surface 4 based on a predefined rule, a state or an event.

Alternatively and/or additionally, the configuration module 6 is activated at moments chosen randomly, pseudo-randomly or periodically by the timer of the system 1, which makes it more difficult for an attacker to anticipate the configuration of the interconnection surface 4.

Alternatively and/or additionally, the configuration module 6 is able to modify the configuration of the interconnection surface 4 so as to move, over time, over one or each mesh surface 2, the zone of the mesh surface 2 having the highest number of groups of connected cells. A zone dense with groups of cells and therefore electrical circuits in fact makes it possible to detect an intrusion more easily. Conversely, such a zone uses more resources to operate. The movement of such a zone therefore makes it possible to strike a compromise between detection fineness of an intrusion and consumption of the system 1.

When the interconnection surface 4 comprises the programmable component 23, the configuration module 6 is for example a software application integrated into the programmable component 23.

When the interconnection surface 4 comprises a micro-electromechanical system piloted by actuators, the configuration module 6 is able to actuate the actuators.

5 The detection module 8 is capable of detecting a modification of an impedance which is characteristic of each group of electrically connected cells, and in particular a break in continuity or an alteration of the continuous circuits formed by connected groups of cells along the interconnection surface 4. An intrusion being characterized by a break or alteration, the detection module 8 is therefore able to detect intrusions. For example, the detection module 8 is able to detect a power outage by dry loop, transmission-reception of a signal, latency measurement or any other method making it possible to detect the alteration of a circuit formed by a group of interconnected cells.

10 The detection module 8 is configured to apply a security policy following the detection of a break in the continuity of a group of connected cells. The security policy for example comprises erasing sensitive data from the equipment protected by the system 1, activating additional tests, such as integrity tests for the mesh surfaces 2 or reconfiguring interconnections of the connectors 24 following a new configuration of the interconnection surface 4 in order to provide additional detection.

Typically, the detection module 8 is configured to emit electrical signals periodically on each electrical circuit, then to verify the proper reception thereof. In case of incorrect reception of an electrical signal, the detection module 8 is able to detect a physical alteration of one or several electrical circuits. In this example, the configuration module 6 slaves the detection module 8 so that the detection module 8 knows the signals it is meant to receive.

20 Alternatively and/or additionally, the detection module 8 includes several methods for detecting a break or alteration of a circuit and uses them in a combined manner with a defined temporal interleaving, which may be pseudo-random or random.

The detection module 8 is configured to be activated at a regular frequency, at least equal to the reconfiguration frequency, by the configuration module 6, of the interconnections of the connectors 24 of the interconnection surface 4.

25 Alternatively, the detection module 8 is activated at moments chosen randomly or pseudo-randomly by the timer of the system 1.

When the interconnection surface 4 comprises the programmable component 23, the detection module 8 is for example a software application integrated into the programmable component.

The reaction module 10 is connected to the detection module 8.

30 The reaction module 10 makes it possible to trigger a reaction action in response to an intrusion attempt in the system 1 detected by the detection module 8. For example,

the reaction module 10 is configured to erase the sensitive data present in the equipment protected by the system 1, to activate additional tests and/or to initiate a reconfiguration of the interconnections of the connectors 24.

5 When the interconnection surface 4 comprises the programmable component 23, the reaction module 10 is for example a software application integrated into the programmable component.

10 The timer is advantageously a low-consumption timer. In order for the overall consumption to remain low, the ratio between the awake and sleep periods of the configuration module 6 and/or the detection module 8 activated by the timer is for example about 1 per 1000, i.e., 1000 microseconds awake for one second of sleep, nevertheless with very small deviations between the awakenings relative to the time to implement an attack.

An intrusion detection method from the intrusion detection system 1 of figure 1 will now be described.

15 Initially, the intrusion detection method comprises a step 100 for providing the intrusion detection system 1 as previously described.

Next, the intrusion detection method comprises a step 110 for determining, using the configuration module 6, a first configuration of the interconnection surface 4.

20 Then, during the following step 120, the configuration module 6 configures the interconnections of the connectors 24 of the interconnection surface 4 according to the first configuration of the interconnection surface 4 previously determined during step 110.

25 Next, during the following step 130, the detection module 8 is activated in order to detect any break in the electrical continuity on each group of cells 3 electrically interconnected by the connectors 24 according to the first configuration of the interconnection surface 4. The detection module 8 is for example activated at a moment chosen randomly by the timer.

30 When the detection module 8 detects a break in the continuity of a continuous circuit, the detection module 8 communicates, during a step 140, with the reaction module 10. The reaction module 10 then takes protective actions on the equipment protected by the system 1.

Next, steps 110 to 140 are repeated over time. The configuration module 6 is for example activated at moments chosen randomly by the timer. The configuration of the interconnection of the connectors 24 done by the configuration module 6 during step 110 alternatively for example depends on the state of the system or a detected event.

Thus, the interconnections between the connectors 24 are reconfigured over time, which makes it possible to obtain new configurations of the interconnection surface 4 and to detect any shunts of several different equipotential cells.

5 Alternatively, the detection module 8 is activated several times between two configurations, by the configuration module 6, of the interconnections of the connectors 24 of the interconnection surface 4. The activation of the configuration module 6 is in fact independent of the activation of the detection module 8.

10 Thus, the system 1 allows effective protection of equipment against physical attacks with a simple and inexpensive mesh format that does not make the development and manufacturing phases of the system 1 more complex. The interconnection surface 4 is programmed to renew itself as a function of time, which provides a considerable gain for the protection level of the mesh.

15 In particular, the reconfiguration over time of the interconnections of the connectors 24 between the cells 3 of the mesh surfaces 2 makes it possible to limit attacks by reverse engineering and to thus make the use of shunts ineffective to short-circuit the electrical circuits of the mesh. Furthermore, the knowledge acquired by an attacker regarding the system is only partially reusable to develop an attack on another system.

20 Furthermore, the mesh surface 2 and the interconnection surface 4 form a physical protective barrier for the equipment protected by the system 1, the configuration module 6 and the detection module 8.

Additionally, the tightening function of the mesh in zones susceptible to attack makes it possible to reinforce the protection of the equipment to be protected.

25 Moreover, the tightening of the mesh at a zone of interest is particularly useful in case of optimized management of the number of available resources, i.e., optimization of the number of inputs and outputs of the interconnection surface 4.

30 The system 1 therefore resolves the problem of increasing the complexity of the meshes of the state of the art by reconfiguring interconnections of the connectors 24 of the interconnection surface 4 over time. The geometry of the mesh is thus specific to a piece of equipment to be protected and varies over time.

The frequency of the reconfigurations, by the configuration module 6, of the interconnections of the connectors 24 of the interconnection surface 4 is also adaptable based on the level of protection desired for the equipment or the estimated attack risks.

35 The system 1 also makes it possible to keep the energy consumption at an acceptable level and to make the protection lasting, even when the equipment of the system 1 is powered by a backup power source for a long period.

One skilled in the art will understand that the invention is not limited to the described embodiments, or to the specific examples of the description.

For example, additionally, the system 1 comprises a module for measuring a variation of a property between at least two of the mesh surfaces 2 of the system 1. The property is for example chosen from among an impedance, a resistance, a capacitance and an inductance. The variations in the property make it possible to detect intrusion attempts and then trigger the configuration module 6 and/or the reaction module 10.

In another example, the system 1 further comprises at least one shielding surface positioned around the mesh surface(s) 2. The shielding surface for example makes it possible to protect the equipment from chemical or electromagnetic attacks.

In still another example, at least one electrical circuit is formed by the connection, which is not reconfigurable by the configuration module 6, of at least two adjacent cells 3 of a mesh surface 2 via a component previously statically configured in the factory. A component previously statically configured is a component unalterably integrated into the system 1 during its manufacture. Each group of cells connected to each other by a component previously statically configured forms a macrocell. The macrocells have the advantage of limiting the number of interconnections of the connectors 24 of the interconnection surface 4. In this case, as illustrated in figure 7, the method for detecting intrusions further comprises a step 150 for building, in the factory, non-reconfigurable interconnections forming the macrocells.

In this last example, the interconnections of the connectors 24 of the interconnection surface 4 are defined statically in part for certain groups of cells and dynamically for others.

12
CLAIMS

1.- An intrusion detection system (1), the system (1) comprising:

5 - at least one mesh surface (2), each mesh surface (2) comprising at least two cells (3), each cell (3) comprising a pattern (20), a pattern (20) being a portion of continuous electrical circuit,

10 - at least one interconnection surface (4) comprising a plurality of connectors (24), the connectors (24) being suitable for connecting cells (3) of the mesh surface(s) (2) to each other according to a first configuration of the interconnection surface (4) for forming groups of electrically connected cells (3), the patterns (20) of the cells (3) of each group forming a continuous electrical circuit of patterns (20),

 - a detection module (8) able to detect a modification of an impedance which is characteristic of each group of electrically connected cells,

15 characterized in that the system (1) further comprises a configuration module (6) for configuring interconnections of the connectors (24), the configuration module (6) being able to modify, over time, the first configuration to obtain at least one second configuration of the interconnection surface (4), and the configuration module (6) being able to modify the configuration of the interconnection surface (1) when an intrusion attempt is detected by the detection module (8).

20 2.- The system (1) according to claim 1, wherein the configuration module (6) is able to determine, randomly, the second configuration from among a plurality of configurations of the interconnection surface (4) and to reconfigure the set of interconnections of the connectors (24) according to the second configuration.

25 3.- The system (1) according to any one of claims 1 to 2, wherein when a break in the electrical continuity of at least one continuous circuit is detected over an area of a mesh surface (2), the configuration module (6) is able to modify the configuration of the interconnection surface (4) so as to increase the number of groups of connected cells present in that area.

30 4.- The system (1) according to any one of claims 1 to 3, wherein the system (1) comprises at least two mesh surfaces (2) and a module for measuring variations in a property between two of the mesh surfaces (2), the property being chosen from among an impedance, a resistance, a capacitance and an inductance.

35

5.- The system (1) according to any one of claims 1 to 4, wherein at least one electrical circuit is formed by the connection, which is not reconfigurable by the configuration module (6), of at least two adjacent cells (3) of a mesh surface (2) via a component previously statically configured.

5

6.- The system (1) according to any one of claims 1 to 5, wherein the configuration module (6) is able to move over time, over one or over each mesh surface (2), a zone of the mesh surface (2) having the highest number of groups of connected cells.

10

7.- The system (1) according to any one of claims 1 to 6, wherein the system (1) comprises a member able to activate, at randomly or pseudo-randomly chosen moments, the configuration module (6) and/or the detection module (8).

15

8.- The system (1) according to any one of claims 1 to 7, wherein the interconnection surface (4) comprises a programmable component, the configuration module (6) and the detection module (8) being software applications integrated into the programmable component.

20

9.- The system (1) according to any one of claims 1 to 8, wherein the interconnection surface (4) comprises a micro-electromechanical system piloted by actuators, the configuration module (6) being able to actuate the actuators.

25

10.- The system (1) according to any one of claims 1 to 9, wherein the mesh surface (2) and the interconnection surface (4) form a physical protective barrier for the configuration module (6) and the detection module (8).

30

11.- The system (1) according to any one of claims 1 to 10, wherein, after a break has been detected in the electrical continuity of a group of connected cells, the detection module (8) is able to apply a security policy, the security policy comprising erasing sensitive data, carrying out integrity tests and/or reconfiguring interconnections of the connectors (24) of the interconnection surface (4).

35

12.- The system (1) according to any one of claims 1 to 11, wherein the detection module (8) includes several methods for detecting a break or alteration of each group of electrically connected cells and is able to use them in a combined manner with a defined temporal interleaving, which may be pseudo-random or random.

13.- An intrusion detection method, the method comprising the following steps:

- providing (100) a system (1) for detecting intrusions according to any one of claims 1 to 12,

5 - determining (110), using the configuration module (6), a first configuration of the interconnection surface (4),

- configuring (120), using the configuration module (6), interconnections of the connectors (24) of the interconnection surface (4) according to the first determined configuration,

10 - activating (130) the detection module (8) to detect a modification of an impedance which is characteristic of each group of electrically connected cells,

- optionally detecting (140), via the detection module (8), a modification of an impedance which is characteristic of a group of electrically connected cells, and

15 - modifying the first configuration of the interconnection surface (4), using the configuration module (6), to interconnect the connectors (24) of the interconnection surface (4) according to a second configuration.