

Electronic system for securely retransmitting messages, associated retransmission method and computer program product

The present invention relates to an electronic retransmission system for securely retransmitting messages that have previously been received by the system.

The invention also relates to a secure retransmission method for securely retransmitting messages that have previously been received by an electronic system.

The invention also relates, in addition, to a computer program product containing software instructions which upon being executed by a computer operationally implements such a retransmission method.

The invention is applicable to the field of securing of real-time information exchange, and relates in particular to the field of cyber-defence.

Currently, solutions for declassification of information/data, that is to say, exchanges of information from a domain having a given privilege level to a domain having a lower privilege level, are for the most part based on mechanisms for signing and labelling of messages. Such mechanisms, at this level of inspection of the data, require human intervention in the continuous and ongoing processing of contentious messages in order to validate that which may be sent to the domain having a lower privilege level.

However, such intervention by a human, who must read, understand, potentially modify the data or information and give their permission for each message is not compatible with the number of messages to be processed per second, or with the stringent constraints of timelines for delivery of messages, for example for the establishment of air situations or the exchange of situations by means of tactical data links.

With regard to solutions for feedback of information, that is to say, exchanges of data and information from a domain having a given privilege level to a domain having a higher privilege level, the problem related to the privilege level to be processed does not arise. The existing data/information feedback solutions are limited to preventing the reverse flow of data to be processed. In order to do this such solutions often make use of uni-directional data transfer links, such as data security diodes, that make it possible to direct the flows of data and thus prevent the reverse flow of data in a physical manner.

However, such data/information feedback solutions do not analyze the content of the messages to be exchanged and therefore do not provide protection against any possible injections of data by hackers.

There is therefore a need for the implementation of an electronic system that provides the ability to filter and exchange data in a secure manner between privilege

domains, which could possibly be different, and is configurable on the basis of the said privilege domains.

To this end, the subject matter of the invention relates to an electronic retransmission system for securely retransmitting messages that have previously been received by the said system, each message containing the data and a transport envelope for transporting of these data, the system including:

- a first module configured in order to select, from among the data from the messages received, the data belonging to a first list of reception allowable data;
- a second module configured in order to select, from among the data selected by the first module, the data belonging to a second list of transmission allowable data; and
- a transmission module configured in order to transmit the data selected by the second module.

According to other beneficial aspects of the invention, the electronic system includes one or more of the following characteristic features, taken into consideration in isolation or in accordance with all technically possible combinations:

- the first list of reception allowable data is different from the second list of transmission allowable data.
- the messages that are received by the electronic system are in compliance with the All Purpose STructured Eurocontrol SuRveillance Information EXchange (ASTERIX) standard, with each of the first and second lists being configured so as to allow the categories of messages defined in accordance with the ASTERIX standard.
- the first module is configured in order to convert the data received from the initial format to an intermediate format, and the second module is configured in order to convert the data selected by the said second module from the intermediate format to a final format, the intermediate format comprising a first field that contains an indication of the data to be maintained and a second field that contains the data.
- the intermediate format also includes a third field that contains an identifier for the said data.
- the first module is configured in order to convert the data received from the initial format to the intermediate format, and then to select, from among the data from the second field corresponding to the indication in the first field, the data belonging to the first list of reception allowable data.
- the second module is configured in order to select, from among the data from the second field selected by the first module and corresponding to the indication in the first field, the data belonging to the second list of transmission allowable data and in order to

convert the data selected by the said second module from the intermediate format to the final format.

- the system includes in addition, upstream from the first module, a deletion module for deleting of the transport envelope from each message, and downstream from the second module, an addition module for adding of the transport envelope relating to each message.

- the modules are implemented via virtual machines connected to each other by means of uni-directional data transfer links.

- the electronic system includes a hypervisor comprising the said virtual machines.

- the system includes in addition, a supervision module connected to at least one module of the electronic system, the supervision module being configured in order to receive one or more parameters originating from the said module and to correlate these parameters between themselves so as to obtain one or more supervision related indicators.

- the supervision module is capable of sending the indicators calculated to external systems.

The invention in addition relates to a secure retransmission method for securely retransmitting messages that have previously been received by an electronic system as defined above, with each message containing the data and a transport envelope for transporting these data, the method including:

- the selection, from among the data from the messages, the data belonging to the first list of reception allowable data;

- the selection, from among the data selected by the first module, of the data belonging to the second list of transmission allowable data; and

- the retransmission of the data selected by the second module.

The invention also relates to a computer program product containing software instructions which upon being executed by a computer operationally implements the retransmission method as defined above.

Other characteristic features and advantages of the invention will become apparent upon reading the description that follows of embodiments of the invention, given only by way of non-limiting example and with reference being made to the annexed drawings, in which:

- Figure 1 is a schematic representation of a secure electronic retransmission system for securely retransmitting messages according to the invention; and

- Figure 2 is a flow chart of a secure electronic retransmission method for securely retransmitting messages by making use of the electronic system shown in Figure 1.

In Figure 1, an electronic system 10 makes it possible to transfer data between different domains having potentially different levels of privilege. A privilege level groups together a specific category of data and information. The privilege levels are generally selected from a group consisting of: top secret, secret, confidential, restricted and non-classified. Classified information is sensitive or privileged information access to which is restricted by a law or regulation to a specific group of persons. The domains are, for example, systems for the development and elaboration of a spatial-, aerial-, terrestrial-, maritime-, or cyber situation, or even governmental organizations, regardless of their level of privilege.

In particular, the electronic system 10 makes it possible to declassify in real-time the data transmitted from a domain having a given privilege level to a domain having a lower privilege level. For example, the electronic system 10 makes it possible to declassify messages from a "secret-defence" level domain to a "confidential-defence" level domain, from a "confidential-defence" level domain to a "restricted distribution" level domain, or even from a "restricted distribution" level domain to a "non classified" level domain.

The electronic system 10, in particular, makes possible the declassification of data in real time in the case of bi-directional exchanges between military domains having different levels of privilege or between military and civilian domains, in particular.

In addition, the electronic system 10 also provides the ability to filter data transmitted from simulation and training domains to operational domains, so as to ensure that simulated situations are prevented from interfering with real-world based situations.

In the event of a feedback of information from a domain having a given privilege level to a domain having a higher privilege level, or exchanges of information between domains of identical privilege level, the electronic system 10 ensures the security and protection of the data exchanged.

As shown in Figure 1, the electronic system 10 is configured in order to receive as input the messages M_1 originating from installations having a first level of privilege and to retransmit as output the messages M_2 being forwarded to the installations having a second level of privilege. The messages M_2 correspond to the messages M_1 after they have been processed by the electronic system 10.

In the case of a declassification of information, the first level of privilege is higher than the second level of privilege.

In the case of a feedback of information, the first level of privilege is lower than the second level of privilege.

By way of a further variant, in the case of protection of data and information by means of transcoding, the first level of privilege and the second level of privilege are identical.

In particular, messages that are received by the electronic system 10 are being sent from and/or forwarded to a chosen installation or facility among the group consisting of: an aircraft, a radar, a control center, a governmental organization such as NATO (acronym for *North Atlantic Treaty Organization*), a military installation, a civilian installation, a simulation software program, a satellite, a naval vessel, a submarine, a space shuttle, and more generally any type of information system installed within a center, a vehicle or a personal equipment unit.

The messages M_1 that are received by the electronic system 10 include the data and a transport envelope for transporting of these data. The transport envelope includes, for example various different fields containing, respectively, the sender and the recipient of the data and the date of sending of the data. The envelope for transporting data is, for example, an IP (acronym for the English term *Internet Protocol*) envelope. The data are, for example, orders for control and command of an aircraft, orders for firing, or even location related data.

Similarly, the messages M_2 being output from the electronic system 10 include the data and a transport envelope for transporting of these data.

The electronic system 10 includes a sequence of modules connected in series, in particular: a deletion module 14 for deleting of the transport envelope of each message M_1 , a first conversion and selection module 16 for converting and selecting, a second conversion and selection module 18, a transport envelope addition module 20 for adding of a transport envelope related to each message M_1 , and a message sending module 21 for sending the messages M_2 . In the embodiment illustrated in Figure 1, the electronic system 10 also includes at least one protection module 22, 24, a data storage module 25, a supervision module 26 and a transmission module 27.

In the embodiment illustrated in Figure 1, the output of the deletion module 14 is connected to the input of the first module 16, preferably by means of a first protection module 22. The output of the first module 16 is connected to the input of the second module 18, preferably by means of the data storage module 25. The output of the second module 18 is connected to the input of the addition module 20, preferably by means of a second protection module 24. The output of the second module 18 is connected to the input of the transmission module 21 which retransmits as output the messages M_2 . In addition, the modules 14, 16, 18, 20, 21, 22, 24, 25 are each connected, independently of

each other, to the supervision module 26. In addition, the supervision module 26 is connected to the transmission module 27.

The modules 14, 16, 18, 20, 21, 22, 24, 25, 26, 27 of the electronic system 10 are operationally implemented via virtual machines, known per se, which are connected to each other by uni-directional data transfer links 28. The electronic system 10 then includes an information processing unit for processing information, not represented, constituted for example, by a processor and a memory storage unit associated with the processor. The processor is then configured so as to run the virtual machines, the latter being in the form of one or more software applications stored in the memory unit.

The use of virtual machines provides the ability to ensure the spatial and temporal separation of the processing operations performed by each module 14, 16, 18, 20, 21, 22, 24, 25, 26, 27.

In a preferred embodiment, illustrated in Figure 1, the first module 16, the second module 18, and the data storage module 25 are operationally implemented on a same given virtual machine.

The uni-directional data transfer links 28, for example, are compliant with a wired standard. The wired standard is for example, the IEEE (Institute of Electrical and Electronics Engineers) 802.3 standard or the PCI Express (Peripheral Component Interconnect Express) standard. By way of variants, even other types of links including wired, optical or electrical links may be considered.

The links 28 are configured so as to isolate the different virtual machines and to thus ensure the non-reversibility of the flow of data. Ensuring non-reversibility of the flow path of the data consists in blocking the flow back of the data in the direction opposite to that of the processing operations, that is to say, from the output to the input of the electronic system 10.

In the embodiment shown in Figure 1, the direction of the flow-path of the data, also known as the critical path corresponds to the direction going from the deletion module 14 towards the transmission module 21, and passing through the first protection module 22, the first module 16, the data storage module 25, the second module 18, the second protection module 24, and then the addition module 20. Thus, the deletion module 14 and the first protection module 22 are located upstream from both the first module 16 and the second module 18 in relation to the direction of flow of the data within the electronic system 10. The second protection module 24, the addition module 20, and the transmission module 21 are located downstream from the first module 16 and the second module 18 in relation to the direction of flow of the data within the electronic system 10.

The uni-directional data transfer links 28 thus allow for the transfer of data in the direction of flow of data and the blocking of data in the reverses direction. Thus, the leakage of sensitive data in particular during a declassification of information gets blocked due to the unidirectional nature of the links 28.

Preferably, the electronic system 10 includes, a hypervisor 30 comprising the virtual machines that operationally implement the modules, 14, 16, 18, 20, 21, 22, 24, 25, 26, 27. A hypervisor is a virtualization platform that makes it possible for multiple operating systems to work on the same given physical machine at the same time. The operating system of the hypervisor is, for example, PikeOS® or PolyXen®.

The deletion module 14 is configured, on the one hand, so as to receive the messages M_1 arriving over the electronic system 10, and on the other hand, to delete the transport envelope of each message M_1 received by the electronic system 10. Thus, at the output of the deletion module 14, only the data from the said messages M_1 are transmitted onward to the first module 16. The transport envelope is, in fact, more prone to be hacked with greater ease than the data in and of themselves, given that hackers are able to for example modify them, in particular change the recipient or the sender of the message. The data and information contained in the transport envelope are deleted from the electronic system 10. The data and information in the transport envelopes are, for example, known and invariable. Such data and information are for example "hard written", that is to say, integrated in an unalterable manner into the electronic system 10 during its manufacture.

The deletion module 14 thus provides the ability to counter possible attacks hidden in the message transport envelope by directly deleting these transport envelopes. One instance of such deletion of the transport envelope is a protocol break, that is to say, a change in protocol that makes it possible to ensure protection from attacks by overload, protocol flaw, hidden channel, or through injection of data.

By way of an additional safety measure, the deletion module 14 is preferably not provided with any operating system. In general, a module that is devoid of an operating system is a module that is devoid of the means that may be used for connection by external operators. Typically, for a module that is devoid of any operating system, a device driver for a network card is integrated solely in the virtual machine of the module, without the integration of any means that may be used for connection by external operators.

By way of a variant, the function of receiving of messages and the function of deletion of the transport envelope are carried out by two distinct and separate modules, connected to one another by a uni-directional data transfer link 28.

The first module 16 is configured in order to convert the data received by the electronic system 10 from an initial format to an intermediate format. Such a conversion of data is a break down in the messaging system, that is to say, a change in the format of the data originating from a messaging system, in order to protect against cyber attacks, in particular from attacks by overload, protocol flaw, hidden channel, or through injection of data.

The initial format of the data is, for example, the binary format.

The intermediate format of the data includes a first field that contains an indication of the data to be maintained and a second field that contains the data. The intermediate format includes, preferably, a third field that contains an identifier for the said data. The indication contained in the first field is, for example, the length of the data to be maintained and their position, for example, the N first bits of data to be maintained or even the N last bits of data to be maintained, N being an integer.

The intermediate format is, for example, the format KLV (Acronym for the English term *Key-Length-Value*) in accordance with the standard SMPTE 336 M-2007 (by the Society of Motion Picture and Television Engineers) in which the letter 'K' refers to the third field, the letter "L" refers to the first field and the letter 'V' refers to the second field, the indication contained in the first field then being the length of the data to be maintained with, for example, the convention according to which the first bits of data are maintained.

For example, the data contained in the message M_1 include the name, "Air France", of an airline in the binary format. The first module 16 provides the ability in this example to convert the binary format of the message to the KLV format in accordance with the standard SMPTE 336 M-2007. In the KLV format, the indication in the first field is the number of characters in the data, that is to say, ten for "Air France", the content of the second field is the data "Air France", and identifier in the third field is the data type, that is to say, the "name of an airline.

Then, once the conversion of data from the initial format to the intermediate format has been carried out, the first module 16 is configured in order to select from among the data in the second field corresponding to the indication in the first field, the data belonging to a first list of reception allowable data.

The selection by the first module 16 of data, from the data in the second field that are in accordance with the indication in the first field, make it possible to prevent the transfer of any possible additional data that could be added by a hacker in the second field. Again considering the previous example, even if a hacker were to add some additional data immediately following the data "Air France" in the second field, these additional data would not be taken into account since the first field indicates that the data

in the second field comprise only ten characters. In this example, only the ten characters corresponding to the data «Air France» shall therefore be taken into account by the first module 16.

The first list of reception allowable data is a white list, that is to say, a list that describes the data in such manner that only the data described in this list are allowed, with the other data being excluded and blocked.

For example, the messages that are received by the electronic system 10 are compliant with the ASTERIX standard and the first list of data is configured so as to allow the categories of messages defined in accordance with the ASTERIX standard.

The ASTERIX (acronym for the English term *All purpose structured Eurocontrol surveillance information exchange*) standard describes in particular a format used for the transmission of data sent from surveillance sensors. The ASTERIX standard defines different categories of data ranging from 0 to 255. For example, the categories from 0 to 127 group together the data originating from standard civilian and military applications, the categories ranging from 128 to 240 group together the data originating from special applications for the military domain and the categories from 241 to 255 group together the data originating from non-standard civilian and military applications.

The second module 18 is configured in order to select, from among the data in the second field that have been selected by the first module 16 and correspond to the indication in the first field, the data belonging to a second list of transmission allowable data.

The second list of transmission allowable data is a white list. In the last example, the second data list is configured so as to allow the categories of messages defined in accordance with the ASTERIX standard.

And then, once the selection has been carried out, the said second module 18 is configured in order to convert the data selected by the said second module 18 from the intermediate format to a final format. The final format is for example the initial format for the messages, in particular the binary format.

For example, the messages that are received by the electronic system 10 belong to three categories of messages defined in accordance with the ASTERIX standard: a first category of messages known as primary, a second category of messages known as secondary, and a third category of messages describing information pertaining to electronic warfare. The first category and the second category correspond, for example, to the category 48 of the ASTERIX standard. The third category corresponds, for example, to the category 34 of the ASTERIX standard. Such messages are for example, sent from radars.

The first list of reception allowable data is then configured so as to allow each of the three categories mentioned. The second list of transmission allowable data is configured so as to allow the data belonging to the first and the second category, but instead to block the data belonging to the third category. In this example, the first list provides the ability to filter the messages that belong to other categories apart from the three categories mentioned and which would for example have been added by a hacker.

In this example, the first data list thus ensures the protection of the integrity of the data passing through the electronic system 10. The second list provides the ability to filter the data that will be retransmitted by the electronic system 10 by deleting the data belonging to the third category. Such a filtering process is envisaged for example when sending data from a military installation to a civil installation to which the electronic warfare related information should not be communicated. In this example, the second data list thus ensures the declassification of data between installations having different privilege levels.

Thus, in the case of a declassification of information, the first list of reception allowable data is different from the second list of transmission allowable data.

In the case of a feedback of information, the first list of transmission allowable data is identical to the first list of reception allowable data. In this case, the first and second lists ensure only the protection of the integrity of the data passing through the electronic system 10.

The same holds true in the case of information exchanges between installations having identical levels of privilege, except when a specific filtering of certain categories of data is required.

The addition module 20 is configured so as to add the transport envelope related to each message, with this transport envelope having been previously configured in the factory in the electronic system 10.

Thus, the message M_2 being output from the electronic system 10 includes the data and a transport envelope for transporting of these data.

By way of an additional safety measure, the addition module 20 is preferably not provided with any operating system.

The transmission module 21 is configured so as to transmit the data selected by the second module 18 after the passage thereof through the addition module 20. The transmission module 21 is configured so as to transmit the data to a defined installation: an installation having a lower level of privilege in the case of a declassification of information, an installation having a higher level of privilege in the case of a feedback of

information, and an installation having an identical level of privilege in the case of protection of information, for example.

By way of an additional safety measure, the transmission module 21 is preferably not provided with any operating system.

By way of a variant, the functions of the addition module 20 and the transmission module 21 are grouped together in the same single module.

The protection modules 22 and 24 are selected from the group consisting of: a router, a firewall, an intrusion detection system, and an anti-virus system. A router is an intermediate element in an IT network that ensures the routing of data packets, that is to say, the transit of packets from one network interface to another in accordance with a set of rules. A firewall is a software program and/or an electronic equipment unit that makes it possible to enforce compliance with the security policy of the network. A network security policy for the network defines the communications allowed over an IT network. An intrusion detection system is a mechanism designed to identify abnormal or suspicious activities on a target that is analyzed, thus making it possible to be informed of successful and unsuccessful intrusion attempts. An anti-virus system, is preferably a software system, designed in order to identify, neutralize and eliminate malicious software programs.

In the embodiment illustrated in Figure 1, the electronic system 10 includes two protection modules: the first protection module 22 is situated upstream from both the first module 16 and the second module 18, and the second protection module 24 is situated downstream from both the first module 16 and the second module 18, in relation to the direction of flow of the data in the electronic system 10.

The first protection module 22 is capable of carrying out a first series of analyses of the data in order to verify that transported data have not been corrupted.

In similar fashion, the second protection module 24 is configured so as to carry out a second series of analyses of the data in order to verify that the data have not been corrupted in the electronic system 10.

The data storage module 25 is configured so as to store in a memory storage unit, the messages selected by the first module 16. The messages selected by the second module 18 are in this case selected from the messages stored in the said memory storage unit. The data storage module 25 thus provides the ability to relay the data between the first module 16 and the second module 18. In other words, the data storage module 25 forms a buffer memory.

The supervision module 26 is connected to each module 18, 20, 21, 22, 24, 25 of the electronic system 10 via uni-directional links 28 in such manner that each uni-

directional link 28 connects the supervision module 26 to a respective single module 18, 20, 21, 22, 24, 25. The supervision module 26 is also connected to the transmission module 27 via a uni-directional link 28 in such manner that the transfer of data between these two modules 26, 27 takes place only from the supervision module 26 to the transmission module 27.

The supervision module 26 is configured in order to receive the parameters originating from each module 14, 16, 18, 20, 21, 22, 24, 25, and to correlate these parameters between each other in a manner such as to calculate one or more supervision related indicators. The supervision module 26 is capable of sending the indicators calculated to the external systems. The parameters are, for example, the utilization rate of the processor of the module, start-up history of the module, or the number of stop and restart cycles of the module. The rate of utilization of the processor, also known as processor load rate, is relative to the operational level of the processor. The start-up history of a module, also known as the "log" as per the accepted English terminology, is a file containing data and information relative to the start-up of the module. The correlation consists of cross-reconciling the various different parameters received in accordance with rules that are predetermined and known per se. The indicators are syntheses of the correlations obtained, possibly converted into an external format that is readable by the receiving external system. The indicators are for example alerts. The external systems are, for example, a network administrator, a device for securing the information systems, or even a cyber-defense device. The external formats are for example the format IDMEF (acronym for the English term *Intrusion Detection Message Exchange Format*), the format associated with the SYSLOG Protocol, for example in accordance with the standard RFC 5424 (Request for Comments), or even the format associated with the SNMP protocol (acronym for the English term *Simple Network Management Protocol*).

By way of example, the parameters are the number of stop and restart cycles of each module 18, 20, 21, 22, 24, 25. Each module 18, 20, 21, 22, 24, 25 informs the supervision module 26 upon each new restart of the said module 18, 20, 21, 22, 24, 25. When the number of cycles of a module 18, 20, 21, 22, 24, 25 is greater than a threshold value, the supervision module 26 sends an indicator in the form of an alert and transmits this indicator in the IDMEF format to a network administrator. In this case, the supervision module 26 provides the means to explain the subevents, here the number of cycles of stops and restarts of the modules, that cause the sending of an alert.

Thus, the supervision module 26 provides the means to monitor the proper internal functioning of the different modules 18, 20, 21, 22, 24, 25 of the electronic system 10 and thus makes it possible for the electronic system 10 to protect itself. In addition, the

supervision module 26 is interoperable, that is to say, that it works no matter what kind of external system there is and does so without restriction with respect to access or implementation. The interoperability of the supervision system 26 is in particular due to the possibility of converting the indicators into an external format.

The transmission module 27 is configured so as to add a transport envelope to the data originating from the supervision module 26. Thus, the groups of data originating from the supervision module 26 and the transport envelope added to the data groups form the supervision related messages S_1 . The data and information in the transport envelopes are, for example, known and invariable, and are "hard written" into the electronic system 10. Such data and information for example contain the addresses of the external systems that are recipients of the supervision related messages S_1 .

The transmission module 27 is also configured so as to send the supervision related messages S_1 to the external systems in accordance with the information contained in the transport envelopes added. In practice, the transmission module 27 is capable of sending the supervision related messages to the logical interfaces, which are external to the electronic system 10. Such logical interfaces redistribute the supervision related messages to the external systems in particular on the basis of the external format of the data of the supervision related messages S_1 and the formats of data that are readable by the external systems. The logical interfaces are, for example, the SNMP interfaces, the SYSLOG interfaces, and the IDMEF interfaces.

By way of an additional safety measure, the transmission module 27 is preferably not provided with any operating system.

Such an electronic system 10 is suitable to be integrated in an installation or facility selected from among: an aircraft, a radar, a control center, a governmental organization, a military installation, a civilian installation, a simulation software program, a satellite, a naval vessel, a submarine, a space shuttle.

The secure retransmission method for securely retransmitting messages that have previously been received by the electronic system 10 mentioned above will now be described with reference being made to Figure 2.

Initially, the method includes a reception step 100, for receiving of the messages M_1 , each message M_1 containing the data and a transport envelope for transporting of these data. Such messages M_1 are in the case of a declassification of information originating from an installation having a given level of privilege and are being sent to an installation having a lower level of privilege. In the case of a feedback of information, the messages that are received by the electronic system 10 are originating from an installation having a given level of privilege and are being sent to an installation having a

higher level of privilege. In the case of protection of information, without feedback or filtering of information, the messages that are received by the electronic system 10 are originating from an installation having a given level of privilege and are being sent to an installation having an equivalent level of privilege.

The messages M_1 that are received by the electronic system 10 are routed to the deletion module 14 via a corresponding uni-directional link 28.

The method then includes a deletion step 110 for deleting of the transport envelope of each message M_1 by the deletion module 14. The data are then routed from the deletion module 14 to the first protection module 22 via a uni-directional link 28.

The method then includes an analysis step 120 for analyzing of the messages by the first protection module 22. Subsequently, the data are forwarded from the first protection module 22 to the first module of 16 via a corresponding uni-directional link 28.

The method then includes a conversion step 130 for converting of the data from the initial format to the intermediate format by the first module 16.

Subsequently, during a step of selection 140, the first module 16 selects, from among the data in the second field corresponding to the indication in the first field, the data belonging to the first list of reception allowable data.

Then, during a step of recording and storing in the memory unit 150, the data selected by the first module of 16 are recorded and stored in the memory unit by the data storage module 25.

After the step of recording and storing in the memory unit 150, the method includes a selection step 160 for selecting, by the second module 18 and, from among the data in the second field selected by the first module 16 and corresponding to the indication in the first field, of the data belonging to the second list of transmission allowable data.

Then, during a conversion step 170, the second module 18 converts the data selected by said second module 18 from the intermediate format to the final format. The data are routed from the second module 18 to the second protection module 24 via a corresponding uni-directional link 28.

The method subsequently includes an analysis step 180 for analyzing of the messages by the second protection module 24. Then, the data are routed from the second protection module 24 to the addition module 20 via a corresponding uni-directional link 28.

During an addition step 190, the addition module 20 adds to each message a transport envelope related to the said message. Then the messages are routed from the addition module 20 to the transmission module 21 via a corresponding uni-directional link 28.

Finally, during a step of re transmission 200, the transmission module 21 retransmits the messages to the receiving installation.

In addition, during the various different steps 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, of the method, the modules 18, 20, 21, 22, 24, 25 transmit their parameters to the supervision module 26. The supervision module 26 correlates and analyzes these parameters with a view to obtaining the indicators that are then sent to the transmission module 27.

The transmission module 27 adds to each data item or group of data originating from the supervision module 26 one transport envelope and sends the supervision related messages S_1 obtained to the external systems on the basis of the information contained in the transport envelope.

By way of a variant, the deletion module 14 is capable of recording and storing the data and information contained in the transport envelope of the message. Then, the deletion module 14 is capable of transferring the information items related to the transport envelope to the addition module 20 via a particular transfer path, which is different from the critical transfer path for transferring data from the messages. As may be necessary, a processing operation similar to the one applied to the data is applied to the transport envelope related information over the particular path. Such a processing operation makes it possible in particular to ensure protection from attacks by overload, protocol flaw, hidden channel, or even through injection of data. The addition module 20 is configured so as to add to the corresponding message the transport envelope that has been stored and appropriately processed.

Thus, the electronic system 10 makes it possible to filter and exchange data in a secure manner between networks having privilege levels that are possibly different. In general, the protection of data is ensured by application of one or more different successive breaks: a first protocol break that is brought about by the deletion module 14, a double breach of the messaging system that is brought about by the first and second modules 16, 18 and a last protocol break that is brought about by the addition module 20.

The use of virtual machines and uni-directional links between these virtual machines makes it possible to isolate the data transiting over the system 10 and to thus ensure non-reversibility of the direction of the flow-path of these data.

In particular, the electronic system 10 provides for the declassification of information and the feedback of information in a secure manner. In addition, in the case of a declassification of information, the electronic system 10 also provides for, in addition to the filtering of data, the degradation of the said data. For example, a position given to a precision of within one meter originating from a given installation, in particular a military

installation, is degraded into a position that is precise to within 10 meters after its passing through the electronic system 10, in order to be sent to an installation having a lower level of privilege, such as a civilian installation. Such degradation of the data is also known as "laundering" of data.

The electronic system 10 introduces, in addition, protection mechanisms that provide the ability to prevent intrusions, to detect them, as well as to block them, with this being possible due to the protection modules 22, 24, the deletion module 14, the addition module 20, the first module 16, and the second module 18.

The electronic system 10 provides the ability to perform all of these processing operations in real time, it is therefore appropriate to data link placed under heavy constraints related to routing and delivery times, such as the links used for the establishment of air situations or tactical data links.

The overall architecture of the electronic system 10 is predefined, in particular the assembly of the different modules of the system 10, and the sequence of steps for processing operations implemented by these modules are generic.

However, depending on the type of messages received, and the standard with which the messages are compliant, the first and second lists are configurable. Thus, it is possible to define the first and second lists specifically for an application of information declassification or for an application of information feedback, for example. The adaptability of the system 10 is therefore ensured on account of the possible configuration of the first and second lists. Thus, the electronic system 10 is configurable in accordance with the domains of privilege that are exchanging the messages, with this being without changing the overall architecture of the electronic system 10.

The electronic system 10 ensures execution of a double function namely, on the one hand, a function of protection of the data received, and then re-transmitted and, on the other hand, a function of filtering of the data based on the predefined configuration, in particular of the data allowable by the first and second lists.

Quite obviously, the person skilled in the art will understand that the invention is not limited to the arrangement of the modules described in Figure 1. For example, on an optional additional basis, the protection modules are added upstream from the deletion module 14 and downstream from the addition module 21, according to the direction of the flow path of the data in the electronic system 10.

CLAIMS

1. - An electronic retransmission system for securely retransmitting messages that have previously been received by the system, each message containing the data and a transport envelope for transporting of these data, the system including:

- a first module configured in order to select, from among the data from the messages received, the data belonging to a first list of reception allowable data;
- a second module configured in order to select, from among the data selected by the first module, the data belonging to a second list of transmission allowable data; and
- a transmission module configured in order to transmit the data selected by the second module.

2. - An electronic system according to claim 1, wherein the first list of reception allowable data is different from the second list of transmission allowable data.

3. - An electronic system according to claim 1 or 2, wherein the messages that are received by the electronic system are in compliance with the All Purpose STructured Eurocontrol SuRveillance Information EXchange (ASTERIX) standard, with each of the first and second lists being configured so as to allow the categories of messages defined in accordance with the ASTERIX standard.

4. - An electronic system according to any one of claims 1 to 3, wherein the first module is configured in order to convert the data received from the initial format to an intermediate format, and the second module is configured in order to convert the data selected by the said second module from the intermediate format to a final format, the intermediate format comprising a first field that contains an indication of the data to be maintained and a second field that contains the data.

5. - An electronic system according to claim 4, wherein the intermediate format also includes a third field that contains an identifier for the said data.

6. - An electronic system according to claim 4 or 5, wherein the first module is configured in order to convert the data received from the initial format to the intermediate format, and then to select, from among the data from the second field corresponding to the indication in the first field, the data belonging to the first list of reception allowable data.

7. - An electronic system according to any one of claims 4 to 6, wherein the second module is configured in order to select, from among the data from the second field selected by the first module and corresponding to the indication in the first field, the data belonging to the second list of transmission allowable data and in order to convert the data selected by the said second module from the intermediate format to the final format.

8. - An electronic system according to any one of claims 1 to 7, wherein the system includes in addition, upstream from the first module, a deletion module for deleting of the transport envelope from each message and, downstream from the second module, an addition module for adding of the transport envelope relating to each message.

9. - An electronic system according to any one of claims 1 to 8, wherein the modules are implemented via virtual machines connected to each other by means of uni-directional data transfer links.

10. - An electronic system according to claim 9, wherein the electronic system includes a hypervisor comprising the said virtual machines.

11. - An electronic system according to any one of claims 1 to 10, wherein the system includes in addition, a supervision module connected to at least one module of the electronic system, the supervision module being configured in order to receive one or more parameters originating from the said module and to correlate these parameters between themselves so as to obtain one or more supervision related indicators.

12. - An electronic system according to claim 11, wherein the supervision module is capable of sending the indicators calculated to external systems.

13. - A secure retransmission method for securely retransmitting messages that have previously been received by an electronic system according to any one of claims 1 to 12, with each message containing the data and one transport envelope for transporting these data, the method including:

- the selection, from among the data from the messages, the data belonging to the first list of reception allowable data;
- the selection, from among the data selected by the first module, of the data belonging to the second list of transmission allowable data; and

- the retransmission of the data selected by the second module.

14. - A computer program product containing software instructions which upon being executed by a computer operationally implements the retransmission method as claimed in claim 13.