

AN AUTHENTICATION DEVICE

Field of Invention

The present invention relates to an information security device. In particular, the present invention relates to a device for authenticating a user accessing information on computer-based systems.

Background

The need for heightened information security is intensifying as repeated security breaches on information networks, identity theft and phishing attacks have made consumers and enterprises conscious of the danger posed by weak and insecure static password-based information security systems. Consequently, consumers and enterprises alike are more willing to invest in and employ cost-effective, reliable, and user-friendly software and hardware authentication solutions that offer secure forms of identification and enhance overall network security. As a result, the use of authentication products is slowly moving towards the mainstream.

Authentication solutions can be subdivided into three different categories: hardware tokens, software tokens, and biometrics. Hardware tokens include smart cards and readers, Universal Serial Bus (USB) tokens, one-time password-generating tokens and the like. These devices provide a higher level of authentication by requiring users to present a physical object that can validate a user's identity. Another less obtrusive and relatively less expensive solution is the utilization of software tokens, which reside on a local hard drive, for ensuring that network access is restricted to certain terminals. Finally, biometrics technology is becoming increasingly popular as prices fall and accuracy improves. Biometrics authentication is one of the most secure means of authenticating individuals using bio-identifiers, for example, face images, hand images, fingerprints, iris images, retina images, signature, voice pattern or keystroke dynamics.

Authentication devices such as hardware tokens are the most commonly deployed authentication solutions today as the authentication keys are normally stored on portable hardware tokens and are in the secure possession of the users. These devices further enhance network security by providing a two-level authentication, serving as the users'

digital identity organizer and managing the users' varied credentials regardless of whether these are encryption keys or passwords, on a single device. Different authentication devices adopt different types of connection interfaces. Some authentication devices are standalone devices that do not need an input connection device. On the other hand, other authentication devices require connection devices or interfaces such as using PC-cards, Bluetooth devices or USB connectors. However, it is observed that the majority of existing authentication device solutions use the USB connector as an input interface type primarily because the USB connector is already a widely adopted interface in computers today.

A USB-based authentication device plugs directly into a computer's USB ports, using strong encryption to communicate with security software on the computer. Once the USB-based authentication device is recognized, the USB-based authentication device either provides a pre-stored, encrypted authentication key to the security software for authentication or requests a user to enter a password in order to gain access to the computer. A related application for the former authentication method is a hardware token required by certain computer programs to allow access to a software. The hardware token is plugged into the computer's USB ports to enable the software to access the hardware token for authorizing usage of the software.

Good security systems should always be designed to be difficult to breach. A problem with the current authentication devices utilising authentication keys is that the authentication keys can be intercepted and easily cracked. Even though the authentication keys are encrypted, rapid advancement in computer processor technology means it is becoming easier for hackers to intercept and crack the authentication keys. Cracking of the authentication keys is accomplished by exhausting every possible encryption key in a sequence space. For example, an authentication key of 40 bits key-strength requires a computer system to take 2^{40} steps to find a corresponding encryption key. This kind of computing power is easily available in most universities and even small companies today. The predictability in the data format of the authentication keys during a key transfer phase also contributes to the problem. Hence, it is unwise to employ only encryption as the only form of security measure to protect the integrity of the authentication keys since encryption too is fallible.

There is therefore a need for an authentication device that preferably further obfuscate the authentication key in an unpredictable format to thereby increase the difficulty of intercepting and cracking the authentication key which is required for information access on computer-based systems for addressing the problems faced by current implementations of authentication devices.

Summary

The present embodiment of the invention disclosed herein provides an authentication device. By multiplexing the authentication key with a chaos signal before transmitting the authentication key, the authentication device increases the difficulty of the authentication key being successfully intercepted and cracked by computer hackers.

In accordance with a first aspect of the invention, there is disclosed an authentication device comprising means for providing an authentication key, a chaotic signal generator and a multiplexer. The authentication key is unique. The chaotic signal generator is for generating a chaotic signal. The multiplexer further multiplexes the authentication key and the chaotic signal together by embedding the authentication key into the chaotic signal and generating an authentication signal therefrom. The generated authentication signal possesses a chaotic signal property. Finally, the generated authentication signal is providable to a computer-based system for authenticating the authentication key.

In accordance with a second aspect of the invention, there is disclosed an authentication method comprising the steps of: providing an authentication key by means for providing the authentication key, the authentication key being unique; generating a chaotic signal by a chaotic signal generator; and multiplexing the authentication key and the chaotic signal by a multiplexer by embedding the authentication key into the chaotic signal and generating an authentication signal therefrom, the authentication signal for provision to a computer-based system for authenticating the authentication key, the authentication signal having a chaotic signal property. The means for providing the authentication key, the chaotic signal generator and the multiplexer forms an authentication device.

Brief Description Of The Drawings

Embodiment of the invention are disclosed hereinafter with reference to the drawings, in which:

- 5 FIG. 1 shows a block diagram of the usage of an authentication device in conjunction with a sound card installed in a computer-based system;

FIG. 2 shows a block diagram of sub-components of the authentication device according to an embodiment of the invention;

10

FIG. 3 shows a data frame structure of a data frame assembled by a micro-controller for embedding an authentication key provided by a memory unit, the micro-controller and the memory unit being sub-components of the authentication device of FIG. 2;

- 15 FIG. 4 shows a Chua's circuit diagram for chaotic signals generation for use with the authentication device of FIG. 2;

FIG. 5 shows a graph illustrating a negative resistance characteristic of an operational amplifier for use in the Chua's circuit of FIG. 4 for generating chaotic signals.

20

FIG. 6 shows graphs of the temporal waveforms of state variables described by state equations of the Chua's circuit of FIG. 4;

- FIG. 7 shows a Hysteresis Chaos Generator circuit for chaotic signals generation for use with the authentication device of FIG. 2, the Hysteresis Chaos Generator circuit being a Resistor Capacitor-Operational Transconductance Amplifier (RC-OTA) implementation;

25

FIG. 8 shows a graph illustrating a hysteresis property of the Hysteresis Chaos Generator circuit of FIG. 7;

30

FIG. 9 shows graphs of the temporal waveforms of state variables described by state equations of the Hysteresis Chaos Generator circuit of FIG. 7;

FIG. 10 shows a block diagram illustrating the interaction between chaotic signal generators, a multiplexer and the micro-controller, wherein the chaotic signal generators and the multiplexer are sub-components of the authentication device of FIG. 2; and

- 5 FIG. 11 shows a flowchart illustrating a process for the detection of the chaotic signals from the authentication signal provided by the authentication device of FIG. 2 to the sound card installed in the computer-based system and the decryption of an authentication key recovered from the chaotic signals.

10 Detailed Description

An authentication device for providing authentication means to a computer-based system by supplying an authentication key is described hereinafter for addressing the foregoing problems. The authentication device, according to an embodiment of the invention, multiplexes the authentication key with chaos signals to generate an authentication signal
15 before transmitting the authentication signal through an audio connector to thereby increase the difficulty of enabling computer hackers to intercept and crack the authentication key.

For purposes of brevity and clarity, the description of the invention is limited hereinafter
20 for use in devices for providing an authentication key-based authentication means to computer-based systems. This however does not preclude various embodiments of the invention from other applications that require similar operating performance as authentication key-based systems for providing authentication means to computer-based systems. The operational and functional principles fundamental to one embodiment of the
25 invention are common throughout other embodiments.

An embodiment of the invention is described hereinafter in accordance with FIGs. 1 to 11 of the drawings, in which like elements are numbered with like reference numerals.

- 30 With reference to FIG. 1, which is a block diagram illustrating usage of an authentication device 102 used in conjunction with a computer-based system 104, a user (not shown) in possession of the authentication device 102 first inserts the authentication device 102 into a sound input port of a sound card 106 installed on the computer-based system 104 for

performing user authentication on the computer-based system 104. The user authentication is performed by an authentication software (not shown) pre-installed on the computer-based system 104. The authentication device 102 then transmits an authentication signal (not shown), generated internally by the authentication device 102, to the computer-based system 104 via the sound card 106. The sound card 106 is preferably an independent add-on card type that plugs into an empty card slot on a main board 108 or a sound module type that is pre-integrated onboard the main board 108 together with the related sound output interfaces. The sound card 106 then performs digitization on the authentication signal after which the authentication signal in digitized form is passed to a Central Processing Unit (CPU) installed on the main board 108 for further processing. The processing of the authentication signal includes recognizing the type of authentication signal and decrypting a pre-encrypted authentication key embedded within the authentication signal. The authentication software then presents the authentication results obtained from the processing of the authentication signal to the user on a monitor 110. The monitor 110 is connected to the main board 108 via a video output port (not shown) located on the main board 108.

FIG. 2 shows a system block diagram of sub-components of the authentication device 102. The authentication device 102 comprises a key module 202 wherein the key module 202 further comprises a memory unit 204 and a micro-controller 206. Additionally the authentication device 102 comprises a first chaotic signal generator 208a, a second chaotic signal generator 208b, a multiplexer 210, a battery unit 212 and an audio connector 214.

The memory unit 204 stores an authentication key which is pre-encrypted during manufacture of the authentication device 102. The authentication key stored in each authentication device 102 is unique to provide an authentication identity for differentiating between authentication devices 102 authenticating with the computer-based system 104. The encryption algorithm used for the encryption of the authentication key is preferably one of symmetric key algorithm (private-key cryptography) and asymmetric key algorithm (public-key cryptography). The encrypted authentication key is then stored into the memory unit 204. The memory unit 204 is preferably of type static RAM. The micro-controller 206 then coordinates the transfer of the encrypted authentication key stored in

the memory unit 204 to other sub-components of the authentication device 102 whenever an external request for the authentication key is received.

5 The first chaotic signal generator 208a and the second chaotic signal generator 208b generate chaotic signals for obfuscating the authentication key through the presentation of the authentication key in an unfamiliar and difficult-to-decipher data format. The obfuscation of the authentication key in this manner thus provides increased resiliency against key snooping and key cracking by computer hackers in addition to encryption that is already applied to the authentication key during the manufacture of the authentication
10 device 102. The first chaotic signal generator 208a and the second chaotic signal generator 208b generate different types of chaotic signals through use of different chaotic signal generating circuits.

The multiplexer 210 then selects a chaotic signal from the chaotic signals received from
15 the first chaotic signal generator 208a and the second chaotic signal generator 208b based on a configuration pre-determined during the manufacture of the authentication device 102. Although only two chaotic signal generators for connecting to the multiplexer 210 are described, more than two chaotic signal generators can be configured for connection to the multiplexer 210 to provide a plurality of chaotic signals. The multiplexer 210 then
20 multiplexes the authentication key received from the key module 202 together with the selected chaotic signal for generating an authentication signal (not shown) therefrom. The authentication signal is then transmitted from the audio connector 214 to the computer-based system 104 via a sound card installed on the computer-based system 104. The audio connector 214 is preferably of type stereo 3.5 mm jack plug.

25

The battery unit 212 is included into the authentication device 102 for providing power needed for operating the key module 202, the first chaotic signal generator 208a, the second chaotic signal generator 208b and the multiplexer 210. As the authentication device 102 does not adopt the USB as a connection interface, the authentication device 102
30 is thus not able to draw power via the USB interface for powering the various sub-components in the authentication device 102. Hence, the inclusion of the battery unit 212 then enables the authentication device 102 to function independently without the need for

an additional external power source. The battery unit 212 preferably uses flat-cell batteries.

FIG. 3 shows a data frame structure of a data frame 300 assembled by the micro-controller 206 for embedding the authentication key provided by the memory unit 204. The data frame 300 comprises four data fields. The four data fields are a preamble 302, a time value 304, a specific key value 306 and an error bit checker 308. The length of the preamble 302 is preferably 48 bits for primarily serving as an identification header for the data frame 300. The time value 304 that follows after the preamble 302 is preferably 40 bits long. The time value 304 contains a value of time that is generated by a clock of the micro-controller 206. The value stored in the time value 304 is preferably defined in a Day (DD), Month (MM), Year (YY), Hour (HH) and Minute (MM) format. The time value 304 is synchronized to a time value obtained from a system clock of the computer-based system 104 whenever the authentication device 102 is inserted into the sound input port of the sound card 106 to provide authentication. Hence, the time value 304 is the only data field in the data frame 300 that changes. In addition, the time value 304 as extracted from the transmitted data frame 300 received by the computer-based system 104 must match with a time value as obtained from the system clock of the computer-based system 104 by the authentication software for ensuring that the data frame 300 has not been tampered with.

The specific key value 306 is preferably 64 bits long and contains a device serial number (not shown) pre-assigned by the manufacturer during the manufacture of the authentication device 102. The device serial number stored in the specific key value 306 uniquely identifies each authentication device 102. Lastly, the error bit checker 308 serves as an error-checking field for the data frame 300. The error bit checker 308 stores a checksum value calculated using a pre-defined error-check function, which uses an input parameter calculated by summing a total number of bits obtained from the time value 304 and the specific key value 306. Alternatively, the error bit checker 308 preferably contains a value calculated by summing a total number of bits obtained from the time value 304 and the specific key value 306.

To perform error checking, the authentication software computes a value by summing up the bit values from the decrypted time value 304 and the decrypted specific key value 306

of the data frame 300 as received by the computer-based system 104. The authentication software computes a checksum using the same pre-defined error-check function. The computed checksum is then compared against the value obtained from the error bit checker 308. If the two values match, the data integrity of the transmitted data frame 300 is then
5 assumed to be intact. However, if the two values do not match, the data integrity of the transmitted data frame 300 is compromised and the transmitted data frame 300 is thus discarded.

The generation of chaotic signals for use with the authentication device 102 can be accomplished using many various types of chaotic signal generation circuits available.
10 One of the more commonly used chaotic signals generation circuit is a Chua's circuit 400 as shown in FIG. 4. The first chaotic signal generator 208a preferably uses the Chua's circuit 400 for generating chaotic signals. A further details on the Chua's circuit 400 can be obtained in "R. N. Madan (Ed.), Chua's Circuit - A Paradigm for Chaos, World Scientific 1993" (hereinafter referred to as Reference 1). The content of Reference 1 is
15 hereby incorporated by way of reference.

The Chua's circuit 400 uses an operational amplifier (not shown) that has a negative resistance for imparting chaotic characteristics to the generated signals. FIG. 5 shows a graph illustrating a negative resistance characteristic of the operational amplifier used in
20 the Chua's circuit 400 for generating chaotic signals. Additionally, the Chua's circuit 400 is described by a group of state equations according to Reference 1. Generated graphs of the temporal waveforms of the state variables described by the group of state equations of the Chua's circuit 400 are as shown in FIG. 6.

Similarly, the generation of chaotic signals for use with the authentication device 102 can also be accomplished using a Hysteresis Chaos Generator circuit 700 as shown in FIG. 7. FIG. 7 shows a Resistor Capacitor-Operational Transconductance Amplifier (RC-OTA) implementation of the Hysteresis Chaos Generator circuit 700. The RC-OTA implementation of the Hysteresis Chaos Generator circuit 700 is preferably used by the
30 second chaotic signal generator 208b for generating chaotic signals.

Further details on the Hysteresis Chaos Generator circuit 700 can be found in "S.Nakagawa and T.Saito, An RC OTA Hysteresis Chaos Generator, IEEE Trans. Circuit

Syst. I, 43, 12, pp.1019-1021 (1996)” (hereinafter referred to as Reference 2). The content of reference 2 is hereby incorporated by way of reference. FIG. 8 further shows a graph illustrating a hysteresis property of the Hysteresis Chaos Generator circuit 700. In addition, Reference 2 describes that a group of state equations is definable for describing the operational characteristics of the Hysteresis Chaos Generator circuit 700. Generated graphs of the temporal waveforms of the state variables described by the group of state equations of the Hysteresis Chaos Generator circuit 700 are as shown in FIG. 9.

Preferably, each of the Chua’s circuit 400 and the Hysteresis Chaos Generator circuit 700 is implementable using a Field-Programmable Gate Array (FPGA).

As described above, FIG. 2 illustrates the use of two chaotic signal generators with the multiplexer 210, the first chaotic signal generator 208a and the second chaotic signal generator 208b. However, when more than two chaotic signal generators are needed for the obfuscation of the authentication key, an Undetermined-Chaotic-Signal-Generator (UCSG) 1002 is preferably added to provide another additional source of chaotic signal. FIG. 10 is a system block diagram showing use of a plurality of chaotic signal generators, specifically including the UCSG 1002, with the multiplexer 210 and the key module 202 for obfuscating the authentication key.

When more chaotic signals are used for the obfuscation of the authentication key, the authentication signal thus produced becomes more complex and unpredictable. The UCSG 1002 functions as another chaotic signal generator that generates chaotic signal of different characteristics from the first chaotic signal generator 208a and the second chaotic signal generator 208b.

More than one of the UCSG 1002 can be configured and utilised in tandem when required for generating chaotic signals with different characteristics. The multiplexer 210 preferably functions as a switch for selecting a chaotic signal from the plurality of chaotic signals received from the first chaotic signal generator 208a, the second chaotic signal generator 208b and the UCSG 1002. Alternatively, the multiplexer 210 functions as a multiplexer for multiplexing the plurality of chaotic signals received from the first chaotic signal generator 208a, the second chaotic signal generator 208b and the UCSG 100 to

thereby obtain a resulting chaotic signal. The multiplexer 210 then further multiplexes the resulting chaotic signal with the authentication key received from the key module 202 for generating the authentication signal therefrom.

- 5 User authentication is carried out by the authentication software pre-installed on the computer-based system 104 using the authentication signal provided by the authentication device 102 as shown in FIG. 1. FIG. 11 shows a flowchart illustrating a process for detecting the chaotic signals from the authentication signal provided by the authentication device 102 to the sound card installed in the computer-based system 104. The flowchart of
10 Fig. 11 further illustrates decryption of the authentication key recovered from the chaotic signals. Referring to Fig. 11, when the authentication software receives the authentication signal, the authentication signal is inspected for determining the value of the Lyapunov exponent in a step 1102. The Lyapunov exponent is defined according to the equation:

15
$$\lambda = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} \ln \left| \frac{df(x_0)}{dx_n} \right|$$

- wherein λ is the Lyapunov exponent, N is the number of iterations, n defines an n -dimensional phase space, and x_0 is the starting point. A positive Lyapunov exponent indicates that the authentication signal is chaotic in nature. A decision is then made in a
20 step 1104 for determining if the Lyapunov exponent is positive in value. If the value of the Lyapunov exponent is found to be negative, the authentication signal is then discarded in a step 1106. On the contrary, if the value of the Lyapunov exponent is positive, the authentication signal is chaotic in nature and is hence accepted by the authentication software as a valid authentication signal.

25

- The authentication software then finds the preamble 302 of the data frame 300 that marks the beginning of the data frame 300 in a step 1108. When the preamble 302 is found, the authentication signal checks and decrypts a sequence code (not shown) located after the preamble 302 of the data frame 300 in a step 1110. The sequence code comprises both the
30 time value 304 and the specific key value 306 in encrypted form.

In a step 1112, the authentication software performs a checksum calculation for the sequence code using the pre-defined error-check function to obtain a checksum value. The checksum value is then compared against the value obtained from the error bit checker 308 of the data frame 300 and a decision is taken in a step 1114. If the checksum value does not match the value obtained from the error bit checker 308, the data integrity of the sequence code is compromised and the sequence code is subsequently discarded in a step 1116. However, if the checksum value matches the value obtained from the error bit checker 308, the authentication software extracts the time value 304 and the specific key value 306 in a step 1118. The time value 304 and the specific key value 306 are then checked for correctness and another decision is further taken in a step 1120. If the values are determined to be incorrect, the values are discarded in the step 1116. However, if the values are determined to be correct, the identification and authentication of the user is then completed in a step 1122.

15 In the foregoing manner, an authentication device for providing an authentication key-based authentication means to a computer-based system is described according to an embodiment of the invention for addressing the foregoing disadvantages of implementation approaches adopted by existing authentication devices. Although only one embodiment of the invention are disclosed, it will be apparent to one skilled in the art in view of this disclosure that numerous changes and/or modification can be made without departing from the scope and spirit of the invention.

20

Claims

1. An authentication device comprising:

means for providing an authentication key, the authentication key being unique;

5 a chaotic signal generator for generating a chaotic signal; and

a multiplexer for multiplexing the authentication key and the chaotic signal by embedding the authentication key into the chaotic signal and generating an authentication signal therefrom, the authentication signal having a chaotic signal property,

10 wherein the authentication signal is providable to a computer-based system for authenticating the authentication key.

2. The authentication device as in claim 1, the chaotic signal generator comprising one of a Chua's circuit and a Hysteresis Chaos circuit.

15

3. The authentication device as in claim 2, the Chua's circuit and the Hysteresis Chaos circuit being implemented using Field-Programmable Gate Array (FPGA).

4. The authentication device as in claim 1, the chaotic signal generated by the chaotic signal generator having a positive Lyapunov exponent, the Lyapunov exponent being defined according to the equation:

20

$$\lambda = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} \ln \left| \frac{df(x_0)}{dx_n} \right|$$

wherein λ is the Lyapunov exponent, N is the number of iterations, n defines an n -dimensional phase space, and x_0 is the starting point.

25

5. The authentication device as in claim 1, the means for providing the authentication key comprising a memory unit and a micro-controller, the memory unit for storing the authentication key and the micro-controller for coordinating the processing of the authentication key by the multiplexer.

30

6. The authentication device as in claim 1, the authentication device further comprising:

an output interface being removably couplable to an input interface of a sound circuit of the computer-based system for providing the authentication signal to the sound circuit, the authentication key being retrievable by the computer-based system from the authentication signal received by the sound circuit.

5

7. The authentication device as in claim 6, the output interface being an audio connector.

10

8. The authentication device as in claim 1, further comprising of a battery unit for powering at least one of the chaotic signal generator, the means for providing the authentication key and the multiplexer.

9. The authentication device as in claim 1, the authentication key being pre-encrypted and pre-stored onto the means for providing the authentication key.

15

10. An authentication method comprising the steps of:

providing an authentication key by means for providing the authentication key, the authentication key being unique;

generating a chaotic signal by a chaotic signal generator; and

20

multiplexing the authentication key and the chaotic signal by a multiplexer by embedding the authentication key into the chaotic signal and generating an authentication signal therefrom, the authentication signal for provision to a computer-based system for authenticating the authentication key, the authentication signal having a chaotic signal property,

25

wherein the means for providing the authentication key, the chaotic signal generator and the multiplexer forms an authentication device.

11. The authentication method as in claim 10, the step of generating the chaotic signal by the chaotic signal generator further comprising the step of:

30

the chaotic signal generator being one of a Chua's circuit and a Hysteresis Chaos circuit.

12. The authentication method as in claim 11, the step of the chaotic signal generator being one of the Chua's circuit and the Hysteresis Chaos circuit further comprising the step of:

implementing the Chua's circuit and the Hysteresis Chaos circuit using
Field-Programmable Gate Array (FPGA).

13. The authentication method as in claim 10, the step of generating the chaotic signal by the chaotic signal generator comprising the step of:

generating the chaotic signal by the chaotic signal generator having a
positive Lyapunov exponent, the Lyapunov exponent being defined according to
the equation:

$$\lambda = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} \ln \left| \frac{df(x_0)}{dx_n} \right|$$

wherein λ is the Lyapunov exponent, N is the number of iterations, n defines an n -dimensional phase space, and x_0 is the starting point.

14. The authentication method as in claim 10, the step of providing the authentication key by the means for providing an authentication key further comprising the step of:

providing the means for providing the authentication key with a memory
unit and a micro-controller, the memory unit for storing the authentication key and
the micro-controller for coordinating the processing of the authentication key by the
multiplexer.

15. The authentication method as in claim 10, further comprising the step of:

providing the authentication signal to an input interface of a sound circuit of
the computer-based system by an output interface being removably couplable to the
input interface of the sound circuit, the authentication key being retrievable by the
computer-based system from the authentication signal received by the sound circuit.

16. The authentication method as in claim 15, the step of providing the authentication signal to the input interface of the sound circuit of the computer-based system by the output interface further comprising the step of the output interface being an audio connector.

17. The authentication method as in claim 10, further comprising the step of:
providing a battery unit for powering at least one of the chaotic signal
generator, the key module and the multiplexer.

5 18. The authentication method as in claim 10, the step of providing the authentication
key by the key module comprising the step of:
pre-encrypting and pre-storing the authentication key onto the key module.

10 19. An authentication key retrieval method comprising the steps of:
receiving an authentication signal by a computer-based system, the
authentication signal being provided by an authentication device;
detecting a chaotic signal property from the authentication signal received
by the computer-based system; and
extracting the authentication key from the authentication signal using a
15 chaotic signal when the chaotic signal property is detected,
wherein the authentication key is providable to the computer-based system
for authentication thereof.

20 20. The authentication key retrieval method as in claim 19, the step of detecting the
chaotic property from the authentication signal comprising the step of:
checking the authentication signal for a positive Lyapunov exponent, the
Lyapunov exponent being defined according to the equation:

$$\lambda = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} \ln \left| \frac{df(x_0)}{dx_n} \right|$$

25 wherein λ is the Lyapunov exponent, N is the number of iterations, n defines an n -
dimensional phase space, and x_0 is the starting point.

21. The authentication key retrieval method as in claim 19, the step of extracting the
authentication key from the authentication signal using the chaotic signal comprising
the step of:
30 locating a preamble for detecting a data frame, the preamble being
representative of the header data field of the data frame.

AMENDED CLAIMS**received by the International Bureau on 11 December 2007 (11.12.2007)**

1. An authentication device comprising:
 - a storage module for providing an authentication key, the authentication key being unique and pre-stored onto the storage module;
 - a chaotic signal generator for generating a chaotic signal; and
 - a multiplexer for combining the authentication key and the chaotic signal by embedding the authentication key into the chaotic signal and generating an authentication signal therefrom, the authentication signal having a chaotic signal property,
 wherein the authentication signal is for provision to a computer-based system for authenticating the authentication key.
2. The authentication device as in claim 1, the chaotic signal generator comprising one of a Chua's circuit and a Hysteresis Chaos circuit.
3. The authentication device as in claim 2, the Chua's circuit and the Hysteresis Chaos circuit being implemented using Field-Programmable Gate Array (FPGA).
4. The authentication device as in claim 1, the chaotic signal generated by the chaotic signal generator having a positive Lyapunov exponent, the Lyapunov exponent being defined according to the equation:

$$\lambda = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} \ln \left| \frac{df(x_0)}{dx_n} \right|$$
 wherein λ is the Lyapunov exponent, N is the number of iterations, n defines an n -dimensional phase space, and x_0 is the starting point.
5. The authentication device as in claim 1, the storage module comprising a memory unit and a micro-controller, the memory unit for storing the authentication key and the micro-controller for coordinating the processing of the authentication key by the multiplexer.

6. The authentication device as in claim 1, the authentication device further comprising:
an output interface being removably couplable to an input interface of a sound circuit of the computer-based system for providing the authentication signal to the sound circuit, the authentication key being retrievable by the computer-based system from the authentication signal received by the sound circuit.
7. The authentication device as in claim 6, the output interface being an audio connector.
8. The authentication device as in claim 1, further comprising of a battery unit for powering at least one of the chaotic signal generator, the storage module and the multiplexer.
9. The authentication device as in claim 1, the authentication key pre-stored onto the storage module being pre-encrypted.
10. An authentication method comprising the steps of:
providing an authentication key by a storage module, the authentication key being unique and pre-stored onto the storage module;
generating a chaotic signal by a chaotic signal generator; and
combining the authentication key and the chaotic signal by a multiplexer by embedding the authentication key into the chaotic signal and generating an authentication signal therefrom, the authentication signal for provision to a computer-based system for authenticating the authentication key, the authentication signal having a chaotic signal property,
wherein the storage module, the chaotic signal generator and the multiplexer forms an authentication device.
11. The authentication method as in claim 10, the step of generating the chaotic signal by the chaotic signal generator further comprising the step of:
the chaotic signal generator being one of a Chua's circuit and a Hysteresis Chaos circuit.

12. The authentication method as in claim 11, the step of the chaotic signal generator being one of the Chua's circuit and the Hysteresis Chaos circuit further comprising the step of:

implementing the Chua's circuit and the Hysteresis Chaos circuit using Field-Programmable Gate Array (FPGA).

13. The authentication method as in claim 10, the step of generating the chaotic signal by the chaotic signal generator comprising the step of:

generating the chaotic signal by the chaotic signal generator having a positive Lyapunov exponent, the Lyapunov exponent being defined according to the equation:

$$\lambda = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} \ln \left| \frac{df(x_0)}{dx_n} \right|$$

wherein λ is the Lyapunov exponent, N is the number of iterations, n defines an n -dimensional phase space, and x_0 is the starting point.

14. The authentication method as in claim 10, the step of providing the authentication key by the storage module further comprising the step of:

providing the storage module with a memory unit and a micro-controller, the memory unit for storing the authentication key and the micro-controller for coordinating the processing of the authentication key by the multiplexer.

15. The authentication method as in claim 10, further comprising the step of:

providing the authentication signal to an input interface of a sound circuit of the computer-based system by an output interface being removably couplable to the input interface of the sound circuit, the authentication key being retrievable by the computer-based system from the authentication signal received by the sound circuit.

16. The authentication method as in claim 15, the step of providing the authentication signal to the input interface of the sound circuit of the computer-based system by the

output interface further comprising the step of the output interface being an audio connector.

17. The authentication method as in claim 10, further comprising the step of:
 - providing a battery unit for powering at least one of the chaotic signal generator, the storage module and the multiplexer.
18. The authentication method as in claim 10, the step of providing the authentication key by the storage module comprising the step of:
 - pre-encrypting the authentication key being pre-stored onto the storage module.
19. An authentication key retrieval method comprising the steps of:
 - receiving an authentication signal by a computer-based system, the authentication signal being provided by an authentication device;
 - detecting a chaotic signal property from the authentication signal received by the computer-based system; and
 - extracting the authentication key from the authentication signal using a chaotic signal when the chaotic signal property is detected,
 - wherein the authentication key is providable to the computer-based system for authentication thereof.
20. The authentication key retrieval method as in claim 19, the step of detecting the chaotic property from the authentication signal comprising the step of:
 - checking the authentication signal for a positive Lyapunov exponent, the Lyapunov exponent being defined according to the equation:

$$\lambda = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} \ln \left| \frac{df(x_0)}{dx_n} \right|$$

wherein λ is the Lyapunov exponent, N is the number of iterations, n defines an n -dimensional phase space, and x_0 is the starting point.

21. The authentication key retrieval method as in claim 19, the step of extracting the authentication key from the authentication signal using the chaotic signal comprising the step of:
 - locating a preamble for detecting a data frame, the preamble being representative of the header data field of the data frame.
22. A computer implemented method comprising:
 - providing an authentication key by a storage module, the authentication key being unique and pre-stored onto the storage module;
 - generating a chaotic signal by a chaotic signal generator; and
 - combining the authentication key and the chaotic signal by a multiplexer by embedding the authentication key into the chaotic signal and generating an authentication signal therefrom, the authentication signal for provision to a computer-based system for authenticating the authentication key, the authentication signal having a chaotic signal property,
 - wherein the storage module, the chaotic signal generator and the multiplexer form an authentication device.
23. A machine readable medium having stored therein a plurality of programming instructions, which when execute, the instructions cause the machine to:
 - provide an authentication key by a storage module, the authentication key being unique and pre-stored onto the storage module;
 - generate a chaotic signal by a chaotic signal generator; and
 - combine the authentication key and the chaotic signal by a multiplexer by embedding the authentication key into the chaotic signal and generating an authentication signal therefrom, the authentication signal for provision to a computer-based system for authenticating the authentication key, the authentication signal having a chaotic signal property,
 - wherein the storage module, the chaotic signal generator and the multiplexer form an authentication device.

24. An apparatus comprising:

a machine readable medium having stored therein a plurality of programming instructions, which when executed, the instructions cause the machine to:

provide an authentication key by a storage module, the authentication key being unique and pre-stored onto the storage module;

generate a chaotic signal by a chaotic signal generator;

combine the authentication key and the chaotic signal by a multiplexer by embedding the authentication key into the chaotic signal and generating an authentication signal therefrom, the authentication signal for provision to a computer-based system for authenticating the authentication key, the authentication signal having a chaotic signal property; and

a processor coupled to the machine readable medium to execute the programming instructions,

wherein the storage module, the chaotic signal generator and the multiplexer form an authentication device.