US 20150082052A1

(19) **United States**

(12) **Patent Application Publication**

Zilberstein et al.

(10) **Pub. No.: US 2015/0082052 A1**

(43) **Pub. Date: Mar. 19, 2015**

(54) **ENCRYPTION-ENABLED INTERFACES**

(71) Applicant: **Waterfall Security Solutions Ltd.**, Rosh Ha'ayin (IL)

(72) Inventors: **Amir Zilberstein**, Yad Rambam (IL); **Lior Frenkel**, Misgav Dov (IL)

(21) Appl. No.: **14/512,496**

(22) Filed: **Oct. 13, 2014**

Related U.S. Application Data

(63) Continuation of application No. 12/518,276, filed on Jun. 9, 2009, filed as application No. PCT/IL2007/001535 on Dec. 11, 2007.

(30) **Foreign Application Priority Data**

Dec. 12, 2006 (IL) 180020

Publication Classification

(51) **Int. Cl.**

G06F 21/62	(2006.01)
G06F 21/83	(2006.01)

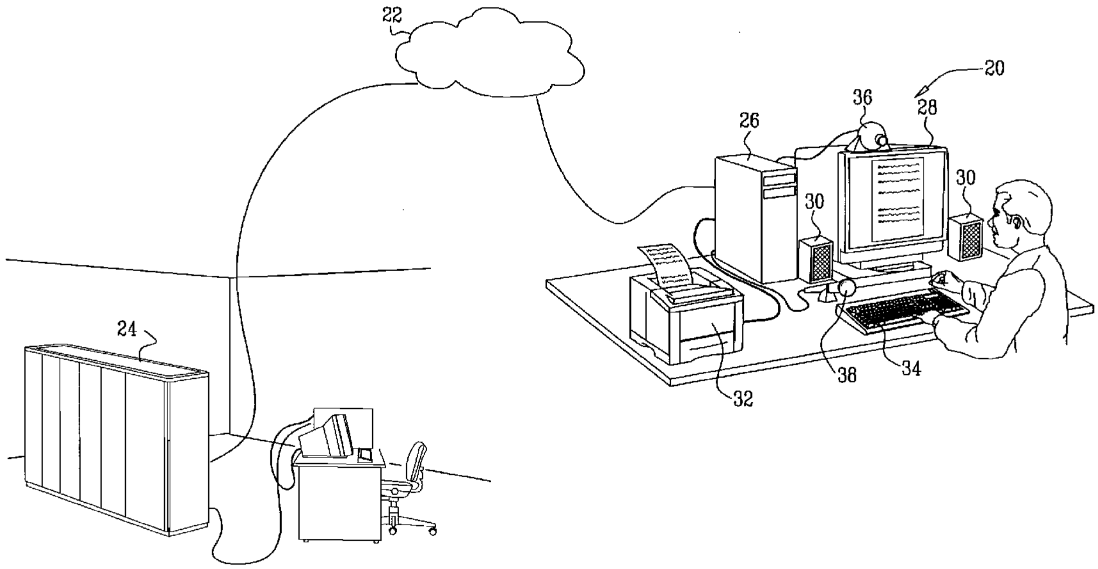
(52) **U.S. Cl.**

CPC ***G06F 21/62*** (2013.01); ***G06F 21/83*** (2013.01)

USPC **713/189**

(57) **ABSTRACT**

Decryption apparatus includes an input memory (**48**), which is coupled to receive encrypted data, and an output transducer (**28**), for presenting decrypted data to a user. A decryption processor (**50**) is coupled to read and decrypt the encrypted data from the input memory but is incapable of writing to the input memory, and is coupled to convey the decrypted data to the output transducer for presentation to the user.



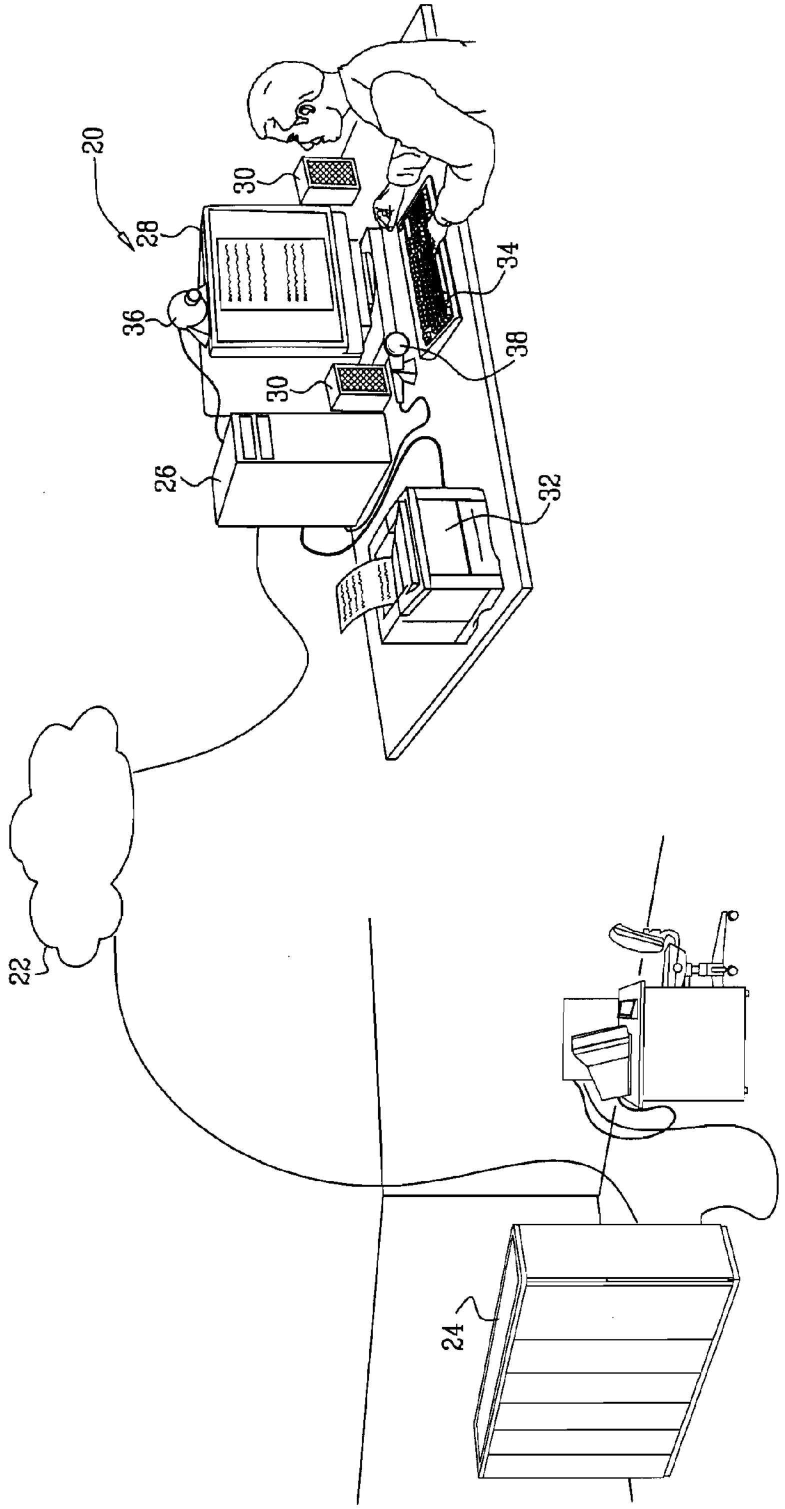


FIG. 1

FIG. 2

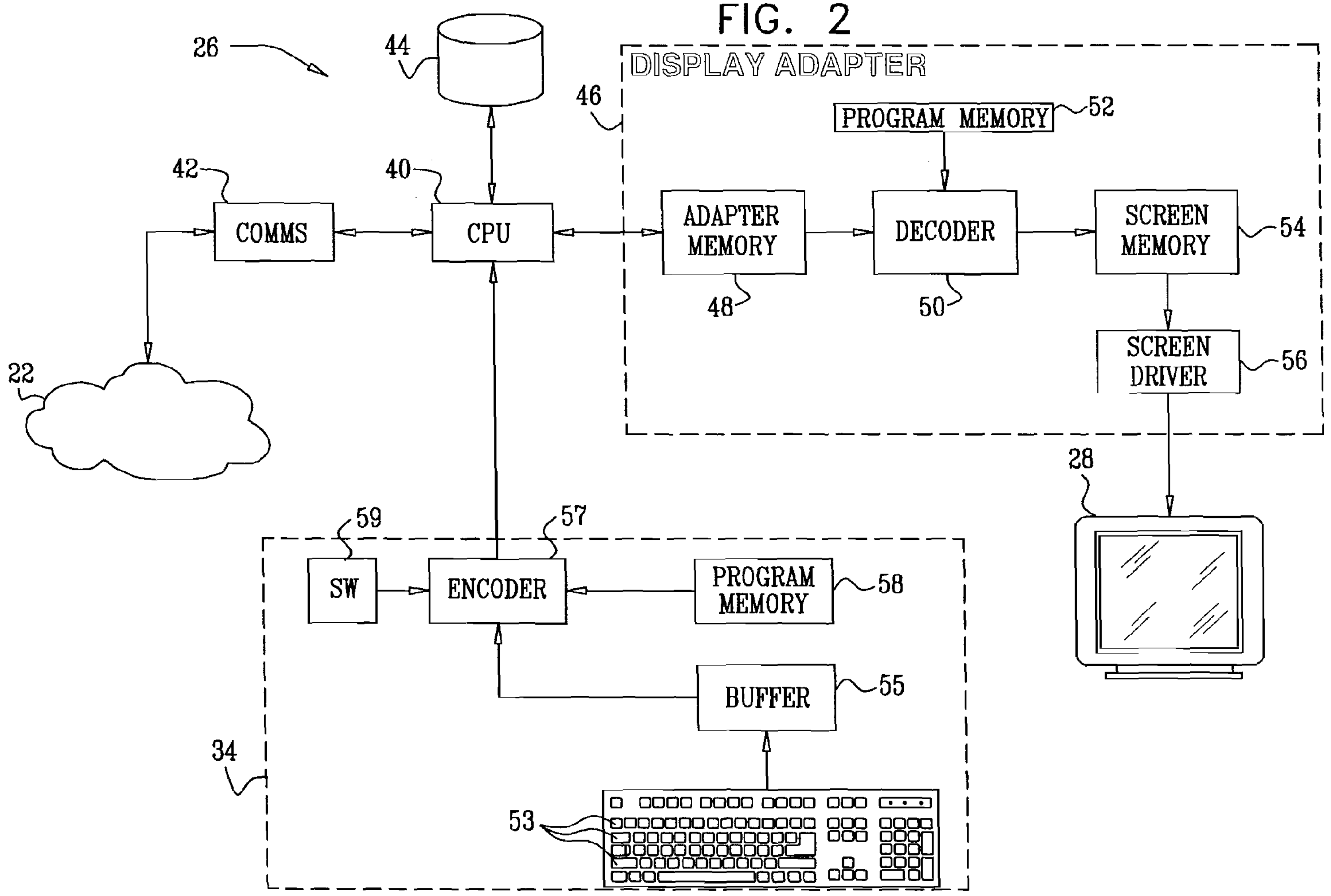
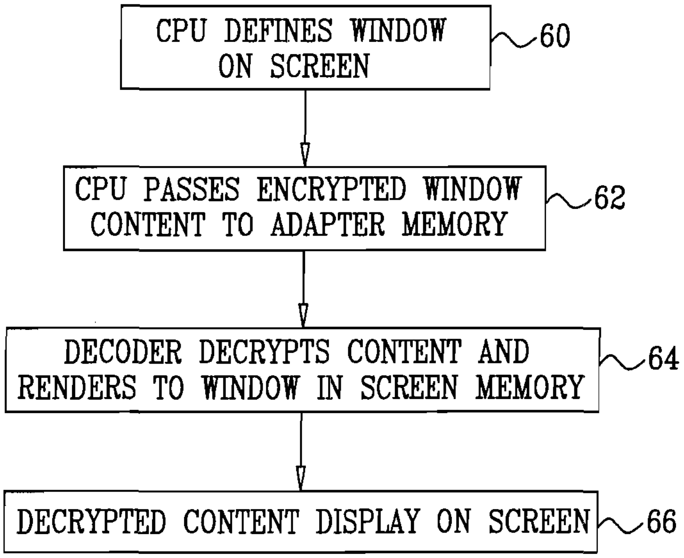

26
44
DISPLAY ADAPTER
46
PROGRAM MEMORY
52
42
COMMS
40
CPU
ADAPTER MEMORY
DECODER
SCREEN MEMORY
54
48
50
SCREEN DRIVER
56
22
28
59
SW
57
ENCODER
PROGRAM MEMORY
58
BUFFER
55
34
53

FIG. 3


CPU DEFINES WINDOW ON SCREEN
60
CPU PASSES ENCRYPTED WINDOW CONTENT TO ADAPTER MEMORY
62
DECODER DECRYPTS CONTENT AND RENDERS TO WINDOW IN SCREEN MEMORY
64
DECRYPTED CONTENT DISPLAY ON SCREEN
66

ENCRYPTION-ENABLED INTERFACES

FIELD OF THE INVENTION

[0001] The present invention relates generally to data decryption, and specifically to methods and devices for preventing unauthorized parties from accessing decrypted data.

BACKGROUND OF THE INVENTION

[0002] Data encryption is widely used in preventing unauthorized access to data. Various methods of data encryption are known in the art. In general, these methods use a key to convert data to a form that is unintelligible to a reader (human or machine), and require an appropriate key in order to decrypt the data. Symmetric encryption methods use the same key for both encryption and decryption. Such symmetric methods include the well-known DES (Data Encryption Standard) and AES (Advanced Encryption Standard) algorithms. In asymmetric encryption methods, such as the RSA (Rivest Shamir Adelman) algorithm, a computer that is to receive encrypted data generates complementary public and private keys and transmits the public key to the sender. After the sender has encrypted the data using the public key, only the holder of the private key can decrypt it.

SUMMARY OF THE INVENTION

[0003] Modern methods of encryption make it very difficult for a malicious party who intercepts an encrypted message to decrypt the message contents. On the other hand, once a computer that receives the message has decrypted it using the proper key and method, the message contents are typically held in clear (unencrypted) form on the receiving computer, at least temporarily. If a malicious party can gain access to the memory (RAM or disk) of the receiving computer (using a "Trojan horse" or other "spyware" program, for example), the malicious party will be able to read the message contents. Thus, the receiving computer itself becomes the weak link in the security chain over which encrypted messages are carried. A similar problem may occur with data that are input to the computer in clear form from an input device, before the computer has encrypted the data.

[0004] Embodiments of the present invention provide methods and apparatus for encryption and decryption that can be used to prevent unauthorized parties from accessing decrypted data on the receiving computer. In some embodiments, a decryption processor reads and decrypts encrypted data from an input memory that receives the encrypted data, but the decryption processor is incapable of writing to the input memory. Rather, the decryption processor is coupled to convey the decrypted data solely to an output transducer, such as a video display, printer, or audio speaker, for presentation to the user. Therefore, the decrypted data are never held on the receiving computer in a memory that could be accessed by unauthorized parties, and there is no link available over which the decryption processor could be made to transmit the decrypted data out of the computer other than directly to the output transducer.

[0005] In other embodiments, an encryption processor is coupled between an input transducer, such as a keyboard, microphone, touch screen or imaging device, and the computer. The encryption processor receives and encrypts input data signals from the input transducer, so that the data input to the computer are already encrypted. Typically, the computer is able to access the input transducer only via the encryption processor, so that an unauthorized party cannot gain access to the clear signals that are produced by the input transducer itself. The computer may then transmit and/or store the input data from the input transducer in encrypted form, without ever having to decrypt the data.

[0006] There is therefore provided, in accordance with an embodiment of the present invention, decryption apparatus, including:

[0007] an input memory, which is coupled to receive encrypted data;

[0008] an output transducer, for presenting decrypted data to a user; and

[0009] a decryption processor, which is coupled to read and decrypt the encrypted data from the input memory but is incapable of writing to the input memory, and which is coupled to convey the decrypted data to the output transducer for presentation to the user.

[0010] In one embodiment, the apparatus includes an output memory, which is coupled to receive the decrypted data from the decryption processor and to output the decrypted data to the output transducer, wherein the input memory is coupled to receive the encrypted data from a central processing unit (CPU) of a computer, and wherein the output memory is inaccessible to the CPU.

[0011] In some embodiments, the decryption processor has an output that is coupled to the output transducer, and the apparatus includes a central processing unit (CPU) and a communication interface, wherein the CPU is coupled to receive the encrypted data from the communication interface and to write the encrypted data to the input memory, and wherein the CPU is unable to access the output of the decryption processor. In one embodiment, the output transducer includes a video display, and the CPU is arranged to define a window on the video display for presentation of the decrypted data, and wherein the decryption processor is arranged to write the decrypted data to the window. Additionally or alternatively, the decryption processor is arranged to decrypt the encrypted data using a predetermined key, and the CPU is unable to access the predetermined key.

[0012] The output transducer may include a video display, an audio speaker, or a printer.

[0013] There is also provided, in accordance with an embodiment of the present invention, a method for decryption, including:

[0014] receiving encrypted data in an input memory;

[0015] reading and decrypting the encrypted data from the input memory using a decryption processor, which is incapable of writing to the input memory; and

[0016] conveying the decrypted data from the decryption processor to an output transducer for presentation to a user.

[0017] There is additionally provided, in accordance with an embodiment of the present invention, a computer input device for operation with a computer, including:

[0018] an input transducer, which is coupled to receive an input from a user and to generate a data signal responsively to the input;

[0019] an encryption processor, which is coupled to process the data signal so as to output data to the computer, and which has a first operational mode in which the encryption processor encrypts the data signal using an encryption key not accessible to the computer so that the data are unintelligible to the computer, and a second operational mode in which the data are intelligible to the computer; and

[0020] a mode switch, which is operable by a user so as to switch between the first and second operational modes of the encryption processor.

[0021] There is further provided, in accordance with an embodiment of the present invention, a method for inputting data to a computer, including:

[0022] receiving a data signal from an input transducer responsively to an input by a user;

[0023] processing the data signal so as to generate data for output to the computer using an encryption processor, which has a first operational mode in which the encryption processor encrypts the data signal using an encryption key not accessible to the computer so that the data are unintelligible to the computer, and a second operational mode in which the data are intelligible to the computer;

[0024] setting a mode switch so as to select one of the first and second operational modes; and

[0025] outputting the data to the computer in accordance with the selected one of the operational modes.

[0026] The present invention will be more fully understood from the following detailed description of the embodiments thereof, taken together with the drawings in which:

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] FIG. **1** is a schematic, pictorial illustration of a system for transmission, reception and processing of encrypted data, in accordance with an embodiment of the present invention;

[0028] FIG. **2** is a block diagram that schematically shows elements of a terminal for encrypting and decrypting data, in accordance with an embodiment of the present invention; and

[0029] FIG. **3** is a flow chart that schematically illustrates a method for decrypting and displaying encrypted data, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

[0030] FIG. **1** is a schematic, pictorial illustration of a system for transmission, reception and decryption of encrypted data, in accordance with an embodiment of the present invention. A source computer **24** transmits encrypted data over a network **22** to a receiving terminal **20**. The data may be encrypted in accordance with any suitable method of encryption that is known in the art, including both symmetric and asymmetric methods. Network **22** may comprise the Internet or substantially any other public or private computer network.

[0031] Terminal **20** comprises a computer console **26**, which is coupled to one or more output transducers for converting data in the console to a form in which a human user can receive and understand the data content. Examples of output transducers that are shown in FIG. **1** include a video display screen **28**, audio speakers **30** and a printer **32**. In the description that follows, display screen **28** is used as the target transducer for purposes of secure decryption of encrypted data received by terminal **20**. Alternatively, the audio speakers or printer may be used for this purpose, as may output transducers of other types (not shown in the figures).

[0032] Typically, terminal **20** also comprises one or more user input devices, which may comprise text, image capture and/or audio input transducers. Typically, the text input transducer comprises a keyboard **34**. Alternatively or additionally, the user input devices may comprise a camera **36**, or a microphone **38**, or a touch-sensitive screen, scanner or other types of input devices known in the art (not shown in the figures). In the description that follows, certain techniques for secure input of encrypted data to console **26** are described, by way of example, with reference to keyboard **34**. These techniques may similarly be applied, mutatis mutandis, to input devices of other types.

[0033] FIG. **2** is a block diagram that schematically shows details of console **26**, in accordance with an embodiment of the present invention. Console **26** may be a general-purpose computer with a specialized display adapter **46**, which performs secure data decryption functions. Alternatively, the decryption functions of adapter **46** may be performed by a decryption circuit that is integrated into the electronics of screen **28** (or similarly integrated into the electronics of another type of output transducer), rather than into the computer console. Additionally or alternatively, keyboard **34** is adapted, as described hereinbelow, to perform secure data encryption. Further alternatively, terminal **20** may comprise one or more dedicated, special-purpose devices that implement the principles of secure decryption and/or encryption that are described herein. Although for the sake of completeness, both secure decryption and secure encryption functions are illustrated in FIG. **2**, terminal may alternatively be configured with only secure decryption or only secure encryption capabilities.

[0034] Console **26** comprises a central processing unit (CPU) **40**, which performs general computing functions. CPU **40** is coupled via a communication interface **42** to transmit and receive data to and from network **22**. The console comprises a memory **44** (which may typically comprise both RAM and disk memory), which is accessed by the CPU in a conventional manner. Typically, upon receiving an encrypted data transmission, CPU **40** writes the encrypted data to memory **44**. In conventional scenarios, the key required to decrypt the data may also be held in the memory. The CPU would then decrypt the data using this key, and then would output the decrypted data to the user automatically or upon request. In the course of such a process, the CPU typically writes the decrypted data to memory **44**. As a result, if a malicious party is able to gain access to the memory through a software security breach, for example, that party may be able to read the decrypted data (generally by causing CPU **40** or another component of terminal **20** to transmit the decrypted data over network **22**), notwithstanding the strength of the encryption that was used in transmission of the data over the network.

[0035] To avoid this sort of scenario in the present embodiment, CPU **40** does not decrypt the encrypted data transmitted by source computer **24**. Rather, the CPU writes the encrypted data to an adapter memory **48** of display adapter **46**. Memory **48** serves as the input memory for decryption purposes. A decryption processor **50** in the display adapter then decodes the encrypted data using the appropriate key and program instructions stored in a program memory **52**. The decryption processor may comprise a programmable processing device, such as a microprocessor or field-programmable gate array (FPGA), or it may alternatively comprise a hard-coded logic device. (In the latter case, memory **52** may be unnecessary, or this memory may be used only to hold the decryption key and/or other basic operating data.)

[0036] Processor **50** writes the decrypted data to a screen memory **54**, typically in the form of either a bitmap or of characters and/or vectors for rendering to screen **28**. The screen memory thus serves as the output memory for the decryption process. A screen driver circuit **56** drives screen **28**

to display the contents of memory **54**. Alternatively, decryption processor **50** may feed the screen driver circuit directly, or the functions of the decryption processor and the screen driver may be integrated in a single integrated circuit.

[0037] As illustrated by the directions of the arrows in adapter **46**, decryption processor **50** is coupled to adapter memory **48** in a read-only configuration, i.e., the processor is able to read from the adapter, but not to write back to the adapter. This configuration may be implemented physically in hardware, by connecting the write output of processor **50** to screen memory **54**, but not to adapter memory **48**. Similarly, the screen memory may be configured so that processor **50** can overwrite the memory contents, but the contents of the memory may be read out only by screen driver circuit **56**. As a result, even if an unauthorized party is successful in gaining access, via a software breach, to CPU **40** and to memories **44** and **48**, it will be physically impossible for this party to access the decrypted data generated by processor **50**. Alternatively, decryption processor **50** may be configured in software to disable write access to memory **48** (and to other elements outside adapter **46**), but if so, it is desirable that the software be stored in a way that prevents unauthorized parties from accessing and changing it.

[0038] Adapter **46** may be configured as a plug-in card, which takes the place of a conventional display adapter in console **26**. In this case, terminal **20** may be a standard personal computer, which is enhanced for secure data decryption by installation of adapter **46**. Alternatively, some or all of the functions of adapter **46** may be integrated into the motherboard of console **26**. Further alternatively, as noted above, the secure decryption functions of adapter **46** may be integrated into the electronics of display screen **28**, in the form of suitable hardware components and/or embedded software. In this latter embodiment, console **26** outputs encrypted data to screen **28**, and the circuitry in the screen decrypts and displays the data. Although the elements of adapter **46** are shown in FIG. **2**, for the sake of clarity, as separate functional blocks, in practice some or all of these functional blocks may be combined into in or more integrated circuit chips.

[0039] As noted earlier, although the secure decryption functions of this embodiment are implemented in conjunction with display screen **28**, such functions may similarly be integrated with other types of output transducers. For example, a sound card with decryption capabilities may be coupled to drive speakers **30** to play decrypted messages, or a printer interface with decryption capabilities may drive printer **32** to print decrypted text and/or graphics. As in the case of screen **28**, the secure decryption capabilities in these example may be incorporated in console **26** or in the speakers or printer.

[0040] The secure encryption functions of terminal **20** are embodied in keyboard **34**. The keyboard comprises a set of keys **53**, which generate respective data signals when depressed by the user, as is known in the art. These data signals are digitized and, optionally, held in a buffer **55**. The digitized data signals are then encoded by an encryption processor **57**, using an appropriate key and program instructions stored in a program memory **58**. The encryption processor may comprise a programmable processing device, such as a microprocessor or field-programmable gate array (FPGA), or it may alternatively comprise a hard-coded logic device, as in the case of decryption processor **50**. In the embodiment shown in FIG. **2**, encryption processor **57** is integrated with keyboard **34**, typically within the keyboard package. Alternatively, the encryption processor may be packaged separately from the keyboard. Further alternatively or additionally, the functions of decryption processor **50** and encryption processor **57** may be integrated together in a single, secure input/output unit.

[0041] Typically, encryption processor **57** has two modes of operation:

[0042] 1. An encryption mode, in which the processor encrypts the data signal using an encryption key that is not accessible to CPU **40**; and

[0043] 2. A clear mode, in which the encryption function of processor **57** is turned off or bypassed, so that the output data from the keyboard are intelligible to the CPU, typically in the standard keyboard data output format.

A user-operable switch **59** permits the user to toggle between the two modes. The switch may simply be a manual switch on the keyboard package, so that even if a hacker gains access to console **26** via communication interface **42**, for example, the hacker will be unable to change the switch setting.

[0044] In normal operation, the user maintains switch **59** in the clear position, so that the user can interact with terminal via keyboard **34** in the conventional manner. From time to time, however, the user may toggle switch **59** to the encryption mode, whereupon encryption processor **57** will output encrypted data to CPU **40**. The CPU in this case is unable to decipher the encrypted data (and cannot access the unencrypted data signals in the keyboard), but rather stores the encrypted data in memory **44** or transmits the encrypted data via communication interface **42** in accordance with instructions that the CPU received previously.

[0045] For example, in a secure communication session between computer **24** and terminal **20**, computer **24** may prompt the user to flip switch **59** to the encryption mode position before inputting some particularly sensitive item of information. Software running on the terminal may prompt CPU **40** to generate a data packet for transmission to computer **24**, and to insert the encrypted data that are entered via keyboard **34** into the payload of the packet before transmission. Computer **24** holds the necessary key to decrypt the payload upon reception, but CPU **40** does not have access to the key. Therefore, even if a hacker were to gain control over the CPU and copy the data transmitted to computer **24**, the hacker will still have no way of deciphering the encrypted payload data.

[0046] FIG. **3** is a flow chart that schematically illustrates a method for decrypting and displaying encrypted data, in accordance with an embodiment of the present invention. The method is described, for the sake of clarity, with reference to the hardware configuration shown in FIG. **2**, but it may similarly be carried out, mutatis mutandis, in other configurations, such as those mentioned above. In the embodiment of FIG. **3**, it is assumed that terminal **20** functions is a personal computer, which runs a window-based operating system and carries out other sorts of computer applications, in addition to the secure decryption function of display adapter **46**. Therefore, the display adapter is capable of displaying both the decrypted data and other, non-secure application data on the same screen simultaneously. (Decryption processor **50** may be bypassed or operate in pass-through mode for displaying the non-secure data.) Alternatively, the method may be simplified, as will be apparent to those skilled in the art, if adapter **46** is limited to displaying decrypted data in full-screen mode.

[0047] To initiate decryption, CPU **40** opens a window on screen **28** in which the decrypted data are to be displayed, at a window definition step **60**. Typically, the CPU opens the decryption window in response to a command by the user of terminal **20** when the user wishes to read an encrypted message or other encrypted data. Alternatively, the CPU may open the window automatically upon receipt of encrypted data from source computer **24**.

[0048] The CPU then writes the encrypted data that are to be decrypted and displayed in the window to adapter memory **48**, at a data input step **62**. Together with the data, the CPU submits a header or other instructions to processor **50** indicating that the data should be decrypted (and possibly including decryption parameters, such as a key identifier), and defining the window in which the decrypted data should be displayed. Decryption processor **50** reads the instructions, decrypts the data, and writes the decrypted data to the appropriate address range in screen memory **54**, at a decryption step **64**. As noted above, the decrypted data may have the form of alphanumeric characters, a bitmap, or graphical vectors, depending on the type of data involved and the rendering capabilities of screen driver **56**. The screen driver reads the decrypted data from memory **54**, and displays the decrypted content in the appropriate window on screen **28**, at a display step **66**.

[0049] The method described above is suitable for displaying a single block of data (characters and/or graphics) of a predetermined size. After viewing one block, the user may prompt CPU **40** to return to step **62** and feed the next block of encrypted data to adapter **46**. Alternatively, for interactive applications, CPU **40** may load a file of data into adapter memory **48**, and decoder **50** may be configured to receive various user inputs so that the user can navigate through the file and change display parameters while viewing the file contents on screen **28**. For example, the decryption processor may be programmed to support a Web browser-type interface in the window assigned for display of decrypted data. In this case, CPU **40** may pass encrypted graphical and text objects, together with markup-language instructions (which may or may not be encrypted) to adapter **46**, which then displays the decrypted graphics and text in the browser interface. The decryption processor may similarly be programmed to support application interfaces of other types.

[0050] As noted above, terminal **20** may also be configured to receive user input, via keyboard **34**, for example, in response to the decrypted data that are displayed on screen **28**. The encryption function of processor **57** may be turned on when secure encryption of the user input is required. Alternatively, if the keyboard is not configured for secure encryption, the user input will reach CPU **40** in non-encrypted form, and may therefore be vulnerable to unauthorized access. Even so, application security is still enhanced, because the unauthorized party is unable to modify the contents of the display that has prompted the user input. For example, in an interactive banking application, a malicious party may attempt to spoof certain contents of the screen, in order to cause the user to approve a transfer of funds to a different account and/or in a different amount from the account and/or amount that are actually displayed on the screen. If the application uses secure decryption, as described above, the malicious party will be barred from access to the screen contents, and this sort of spoofing is prevented.

[0051] Although the description above relates to uses of embodiments of the present invention in preventing unauthorized access to decrypted data, the architecture and methods associated with these embodiments may also be useful in enhancing the efficiency and reliability of various encryption and decryption processes, as will be apparent to those skilled in the art. It will thus be appreciated that the embodiments described above are cited by way of example, and that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention includes both combinations and subcombinations of the various features described hereinabove, as well as variations and modifications thereof which would occur to persons skilled in the art upon reading the foregoing description and which are not disclosed in the prior art.

1-32. (canceled)

33. A computer terminal, comprising:

a communication interface, configured to be coupled to a network;

a secure input device, which comprises:

an input transducer, which is coupled to receive an input from a user and to generate a data signal responsively to the input;

an encryption processor, which is coupled to process the data signal so as to output data for transmission over the network, such that the data signal is not accessible outside the secure input device except in the data output by the encryption processor, and which has a secure operational mode in which the encryption processor generates the output data by encrypting the data signal using an encryption key not accessible to any elements of the computer terminal outside the secure input device so that the output data are unintelligible to such elements; and

a display configured to display non-secure data received from the network without decryption while the secure input device operates in the secure operational mode.

34. The terminal according to claim **33**, wherein the input transducer comprises a text input device.

35. The terminal according to claim **34**, wherein the text input transducer comprises a keyboard.

36. The terminal according to claim **33**, wherein the input transducer comprises an image capture device.

37. The terminal according to claim **33**, wherein the input transducer comprises an audio input device.

38. The terminal according to claim **33**, and comprising a central processing unit (CPU), which is coupled to receive the output data from the secure input device and to transmit the output data via the communication interface to the network,

wherein the encryption key is not accessible to the CPU, and the output data are unintelligible to the CPU.

39. A method for data communication, comprising:

in a secure input device of a computer terminal, receiving a data signal from an input transducer responsively to an input by a user;

processing the data signal using an encryption processor operating in the secure input device in a secure operational mode so as to generate data for output via a network, such that the data signal is not accessible outside the secure input device except in the data output by the encryption processor, which generates the output data in the secure operational mode by encrypting the data signal using an encryption key not accessible to any elements of the computer terminal outside the secure input device so that the output data are unintelligible to such elements;

transmitting the output data from the secure input device over a network to a computer; and while the secure input device operates in the secure operational mode, receiving over the network non-secure data from the computer and displaying the non-secure data on the terminal.

40. The method according to claim **39**, wherein the input transducer comprises a text input device.

41. The method according to claim **40**, wherein the text input transducer comprises a keyboard.

42. The method according to claim **39**, wherein the input transducer comprises an image capture device.

43. The method according to claim **39**, wherein the input transducer comprises an audio input device.

44. The method according to claim **39**, wherein transmitting the output data comprises receiving the output data in a central processing unit (CPU) of the computer terminal and passing the output data from the CPU to the network,

wherein the encryption key is not accessible to the CPU, and the output data are unintelligible to the CPU.

* * * * *