SYSTEM AND METHOD FOR SECURE DATA ENTRY

This invention describes a secure data entry system that works on most computers without the need to install any software driver.

Background

Online electronic transactions are getting more popular on the Internet.

One of the problems of using electronic transaction is the threat of viruses, Trojan horses and malicious programs capturing the user's password and information and altering the content of an electronic transaction.

Secure key pads are used to encrypt and authenticate electronic transactions. One of the problems with the deployment of a secure key pad is the extensive user support required for the installation of its software driver.

Summary of Invention

This invention describes a secure data entry system consisting of:

a. secure data entry device which consist of secure data entry software on electronic devices for entering data entries, optionally adding a unique session number to the data entries with the device's ID, optionally signing the serialized data entries, encrypting the signed, serialized data entries and sending the secure data entries to the keyboard buffers of the requesting computers.

b. Requesting programs or requesting web pages / form that request for the secure data entries, receive the secure data entries from the keyboard buffers and forward the secure data entries to the processing servers.

c. Processing servers then decrypts the secure data entries, verifying the digital signature of the data entries, verifying that the serial session number is newer then the one stored in the database, updating the session serial number in the database and processing the data entries.

Detailed Description of Invention

An embodiment of the Invention will now be described, by way of example, with reference to the accompanying drawings in which;

Figure 1 is a block diagram of the invention for a particular example;

Figure 2 is a flow chart of the secure data entry software;

Figure 3 is a flow chart of the usage of the secure data entry system;

Figure 4 is a snap shot of the display of a secure data entry requesting program or web page / form:

Figure 1 is a block diagram of the invention. The secure data entry system consist of: a secure data entry device 1 1 which consist of secure data entry software installed in electronic devices, a cryptographic storage and/or engine 18 may be used to store and perform the cryptographic function on the secure data entry device 11. The secure data entry device 11 is linked to a computer 12 with link 19. Link 19 may be a connection to the computer's keyboard or USB port with the secure data entry device 11 emulating a keyboard. Link 19 may also be a connection to the computer's serial, parallel, PCMCIA, IRDA and other I/0 port, with a driver 13 installed on the computer 12 to communicate with the secure data entry device, capture the secure data entries from the secure data entry device and to store the secure data entries to the computer's keyboard buffer 14; the secure data entries in the keyboard buffer 14 is read by the browser (displaying the requesting web page / form) or requesting

program 15. The requesting programs or requesting web pages / form 15 will then transmit the secure data entries to the processing server 17 via a Network.

Figure 2 is a flow chart of the secure data entry software; the ITEM COUNTER is incremented by 1 and displayed (22), the secure data entry software will prompt the user to enter one or multiple data entries into the secure data entry devices cache (23), the secure data entry software will check if the user has indicated he has finished entering the data entries (24), when he indicates he has finished by pressing a FINISH button on the secure data entry device, the secure data entry software will add a device ID and a session serial number stored in the secure data entry device or the cryptographic storage or engine to the data entries stored in the secure data entry device's cache and increment the serial number (25). The secure data entry software then optionally sign and encrypt the data entries (26), and output the secure data entries in the secure data entry device's cache to the linked computer (27).

Figure 3 is a flow chart of the usage of the secure data entry system; users will start the requesting program or browse a requesting web page / form and the requesting program or requesting web page /form will request the user to enter the required data entries into the secure data entry device (31), the user press a START button on the secure data entry device and input each entry sequentially with each entry separated by an ENTER key, the user will finish the entry by pressing a FINISHED key on the secure data entry device, and the secure data entry software will send the secure data entries to the computer (32), the requesting program or requesting web page / form

will receive the secure data entries (33), the secure data entry software will forward the secure data entry to the processing server (34), the processing server will decrypted the secure data entries, verify if the data entries are correctly signed and serialized and process the data entries (35).

Figure 4 is a snap shot of the display of a secure data entry requesting program or web page / form 4 1, the user is requested to begin by pressing a START button 42 on the secure data entry device, each data entry is itemized with a running ITEM NUMBER 45, each data entry is described with a DESCRIPTION 43, the user is prompted to complete the data entry by pressing the FINISH button on the secure data entry device 44, the secure data entries from the secure data entry device will be read into a secure data entry area 46 in the requesting program or web page / form and displayed on the display of the computer.

The secure data entry system consists of

a. secure data entry devices which consist of secure data entry software in electronic devices.
b. requesting programs or requesting web pages / form and.
c. processing servers.

The secure data entry devices' functions are

a. entering one or multiple data entries.
b. optionally serializing the data entry session with a unique session number

   with the device's ID,
c. optionally signing the serialized data entries,
d. encrypting the signed serialized data entries and

e. sending the encrypted signed serialized data entries to the keyboard buffer of the requesting computer.

The requesting programs or requesting web pages / forms:

a. request for secure data entries.

b. receive the secure data entries from the keyboard buffer and

c. forward the secure data entries to processing servers.

The processing servers functions are:

a. serving the web pages / forms,

b. decrypting the secure data entries,

c. verifying the digital signature of the data entries,

d. verifying that the serial session number is newer then the one stored in the database,

e. updating the session serial number in the database and

f. processing the data entries.

The secure date entry devices may be another computer notebook, Personal Digital Assistant, hand phone, key pad or other electronic devices.

The secure data entry software may capture data entries from the secure data entry device's input device.

The secure data entry software may serialize the data entry by adding a session serial number to the data entries, this serial number is incremented each time the secure data entries software is used. This serial number counter may be stored in the secure data entry device's non volatile memory or in a cryptographic storage attached to the secure data entry device.

The secure data entry software may add the device's ID to the data entries.

The secure data entry software may digital sign the serialized data entries with a

private key unique to the user, this private key may be stored in the secure data entry device's non volatile memory or in a cryptographic storage attached to the secure data entry device

The secure data entry software may use symmetrical or asymmetrical encryption; the encryption key may be stored in the secure data entry device's non volatile memory or in a cryptographic storage attached to the secure data entry device.

The secure data entry device with the secure data entry software can send the secure data entries to the computer via the keyboard port of the computer.

The secure data entry device with the secure data entry software can send the secure data entries to the computer via the USB port on the computer with the secure data entry device emulating a USB keyboard.

The secure data entry device with the secure data entry software can send the secure data entries to the computer via any of the I/O port on the computer with a device driver installed on the computer, the device driver retrieve the data from the secure data entry device and send the data to the keyboard buffer on the computer.

The requesting programs request for secure data entries by prompting the user to enter a number of data entries shown on the computers display with the secure data entry device.

The requesting web pages / form request for secure data entries by prompting the user to enter a number of data entries shown by a browser with the secure data entry device.

The requesting programs receive secure data entries by reading the keyboard buffer on the requesting computer.

The requesting web pages / form receive secure data entries by the browser reading the keyboard buffer on the requesting computer and putting these secure data entries into a text field on the web page / form.

The requesting programs can send the secure data entries to the processing server using a Network.

The requesting web pages / form can send the secure data entries to the processing server by submitting the web page or form reply using a Network.

The processing servers may be used for serving the requesting web pages / form.

The processing servers decrypts the secure data entries using it's decryption key.

The processing servers may verify the authenticity of the data entries if the data entries are signed by the secure data entry software.

The processing servers may verify that the secure data entry session serial number is larger then that store in the processing server's database.

The processing servers will update its database with the latest secure data entry session serial number.

The processing servers will process the data entries

CLAIMS

1. A secure data entry system consisting of:
   a. secure data entry devices which consist of secure data entry software in electronic devices for users to enter data entries, optionally serializing the data entries with a unique session number, optionally adding the device's ID, optionally signing the serialized data entries, encrypting the signed serialized data entries and sending the secure data entries to the keyboard buffer of the requesting computer,
   b. requesting programs or requesting web pages / forms that request for secure data entries, receive secure data entries from the keyboard buffer and forwarding the secure data entries to processing servers,
   c. processing server for serving the requesting web pages / forms, receiving the secure data entries, decrypting the secure data entries, verifying the digital signature of the data entries, verifying that the serial session number is newer then the one stored in the database, updating the session serial number in the database and processing the data entries.
2. As claimed in Claim 1 the secure data entry system consists a secure data entry software in electronic devices for:
   a. entering one or multiple data entries,
   b. optionally serializing the data entry session with a unique session number,
   c. optionally adding the device's ID to the data entries,
   d. optionally signing the serialized data entries,
   e. encrypting the signed serialized data entries,

f. sending the encrypted signed serialized data entries to the keyboard buffer of the requesting computer.

3. As claimed in Claim 1 the secure data entry system includes requesting programs or requesting web pages / forms that:

a. request for secure data entries,

b. receive the secure data entries from the keyboard buffer and

c. forward the secure data entries to processing servers.

4. As claimed in Claim 1 the secure data entry system includes processing servers for:

a. serving the web pages / forms,

b. decrypting the secure data entries,

c. verifying the digital signature of the data entries,

d. verifying that the serial session number is newer then the one stored in the database,

e. updating the session serial number in the database and

f. processing the data entries.

5. As claimed in Claim 1 and Claim 2 the secure data entry devices may be another computer, notebook, Personal Digital Assistant, hand phone, key pad or other electronic devices.

6. As claimed in Claim 1 and Claim 2 the secure data entry software may capture data entries from the secure data entry device's input device.

7. As claimed in Claim 1 and Claim 2 the secure data entry software may serialize

the data entry by adding a session serial number to the data entries, this serial number is incremented each time the secure data entries software is used. This serial number counter may be stored in the secure data entry devices non volatile memory or in a cryptographic storage attached to the secure data entry device.

8. As claimed in Claim 1 and Claim 2 the secure data entry software may add the device's ID to the data entries.

9. As claimed in Claim 1 and Claim 2 the secure data entry software may digitally sign the serialized data entries with a private key unique to the user, this private key may be stored in the secure data entry device's non volatile memory or in a cryptographic storage attached to the secure data entry device.

10. As claimed in Claim 1 and Claim 2 the secure data entry software may use symmetrical or asymmetrical encryption; the encryption key may be stored in the secure data entry device's non volatile memory or in a cryptographic storage attached to the secure data entry device.

11. As claimed in Claim 1 or Claim 2 the secure data entry, device with the secure data entry software can send the secure data entries to the computer via the keyboard port of the computer.

12. As claimed in Claim 1 or Claim 2 the secure data entry device with the secure data entry software can send the secure data entries to the computer via the USB port on the computer with the secure data entry device emulating a USB keyboard.

13. As claimed in Claim 1 or Claim 2 the secure data entry device with the secure data entry software can send the secure data entries to the computer via any of the I/O port on the computer with a device driver installed on the computer, the device driver retrieve the data from the secure data entry device and send the data to the keyboard buffer on the computer.

14. As claimed in Claim 1 or Claim 3 the requesting programs request for secure data entries by prompting the user to enter a number of data entries shown on the computers display with the secure data entry device.
15. As claimed in Claim 1 or Claim 3 the requesting web pages / forms request for secure data entries by prompting the user to enter a number of data entries shown by a browser with the secure data entry device.
16. As claimed in Claim 1 or Claim 3 the requesting programs receive secure data entries by reading the keyboard buffer on the requesting computer.
17. As claimed in Claim 1 or Claim 3 the requesting web pages / forms receive secure data entries by the browser reading the keyboard buffer on the requesting computer and putting these secure data entries into a text field on the web page / form.
18. As claimed in Claim 1 or Claim 3 the requesting programs can send the secure data entries to the processing server using a Network.
19. As claimed in Claim 1 or Claim 3 the requesting web pages / forms can send the secure data entries to the processing server by submitting the web page / form reply using a Network.
20. As claimed in Claim 1 and Claim 4 the processing servers may be used for serving the requesting web pages / forms.
21. As claimed in Claim 1 and Claim 4 the processing servers decrypts the secure data entries using its decryption key.
22. As claimed in Claim 1 and Claim 4 the processing servers may verify the authenticity of the data entries if the data entries are signed by the secure data entry software.
23. As claimed in Claim 1 and Claim 4 the processing servers may verify that the secure data entry session serial number is larger then that store in the

processing server's database.

24. As claimed in Claim 1 and Claim 4 the processing servers will update its database with the latest secure data entry session serial number.

25. As claimed in Claim 1 and Claim 4 the processing servers will process the data entries