The present invention relates to a security acceleration board for converting between encryption schemes in a wireless application protocol (wap) gateway.

The invention relates to the field of network security protocol conversion. In particular, the invention relates to the conversion between the Wireless Transport Layer Security and Secure Sockets Layer protocols.

2. Background Information and Description of Related Art

The Wireless Application Protocol (WAP) defines a set of protocols for wireless applications. The Wireless Transport Layer Security (WTLS) is the security layer of the WAP and provides privacy, data integrity, and authentication for WAP services.

WTLS is based on the Transport Layer Security (TLS), a security layer widely used in the Internet, with modifications to accommodate bandwidth, datagram connection, processing power, memory capacity, and cryptography limitations typical in wireless communications.

Secure Sockets Layer (SSL) is a protocol for transmitting private documents via the Internet. Currently, SSL is not directly compatible with WTLS. Hence, it is not possible to convert between WTLS encrypted data and SSL encrypted data without decrypting the data.

The common method of converting between SSL data and WTLS data uses software executing inside a WAP gateway. Wireless messages travel through the air to a carrier's receiver, where they are received and passed to the gateway. If the message is WTLS encrypted, the encrypted message is decrypted, then encrypted using SSL. If the message is SSL encrypted, the

encrypted message is decrypted, then encrypted using WTLS. Then, the encrypted message is transmitted out of the gateway.

The data is decrypted and stored in the memory of the WAP gateway temporarily, allowing a period of time when the message is unencrypted and unprotected in the WAP gateway. This creates a security vulnerability. Furthermore, since the conversion is done using software, a considerable amount of CPU resources are consumed and a latency in the response to a client request may be experienced.

BRIEF DESCRIPTION OF ACCOMPANYING DRAWINGS

The invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings in which like reference numerals refer to similar elements.

Figure 1 illustrates an embodiment of a system implementing the invention.

Figure 2 illustrates an example of a security procedure implemented with an embodiment of the method of the invention.

Figure 3 illustrates an embodiment of a board according to the invention.

Figure 4 illustrates an embodiment of the method of the invention.

DETAILED DESCRIPTION OF THE INVENTION

Embodiments of a system and method for accelerating the conversion process between encryption schemes are described. In the following description, numerous specific details are provided for a thorough understanding of embodiments of the invention. One skilled in the relevant art will recognize, however, that the invention can be practiced without one or more of the specific details, or with other methods, components, materials, etc. In other instances,

well-known structures, materials, or operations are not shown or described in detail to avoid obscuring aspects of the invention.

Reference throughout this specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, the appearances of the phrases "in one embodiment" or "in an embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures, or characteristics may be combined in any suitable manner in one or more embodiments.

Referring to Figure 1, a block diagram illustrates an embodiment of a system 100 implementing the invention. Those of ordinary skill in the art will appreciate that the system 100 may include more components than those shown in Figure 1. However, it is not necessary that all of these generally conventional components be shown in order to disclose an illustrative embodiment for practicing the invention. System 100 includes a service provider 102, a client 104, and a content provider 106. The client has a device 110. In one embodiment of the invention, the device 110 is a wireless device, which typically uses Wireless Application Protocol (WAP), a set of protocols for wireless applications. The content provider 106 has a server 112 to store content. The service provider 102 provides a gateway 108. The gateway 108 connects the client 104 to the content provider 106. The gateway 108 encrypts and decrypts data as necessary to provide compatibility between the different protocols used by the client and the content provider. For example, the client device 110 typically encrypts data

according Wireless Transport Layer Security Protocol (WTLS), a security layer for WAP that provides privacy, data integrity, and authentication for WAP services. Data on the Internet is typically encrypted according to Secure Sockets Layer Protocol (SSL). Therefore, the gateway will decrypt and encrypt the data from WTLS to SSL and vice versa if the client wants to access an Internet web page.

The gateway 108 contains a security acceleration board 114 for decrypting and encrypting data. In one embodiment of the invention, the board 114 is a plug and play device that fits into a Peripheral Component Interconnect (PCI) slot or a single or dual in-line memory module (SIMM or DIMM) slot.

The client uses the device 110 to send a request 116, which is encrypted according to an encryption scheme. For example, a client may use a cellular phone to send a request for an Internet web page. The request 116 is received in the gateway 108. The board 114 decrypts the request 116 and encrypts the request according to another encryption scheme. In one embodiment of the invention, the request is encrypted according to WTLS. The board 114 may decrypt the request and encrypt the request according SSL. The request 118 is sent to a content provider 106. The content provider accesses the requested content and sends a response 120, which is encrypted according to an encryption scheme. In one embodiment of the invention, the response is encrypted according to SSL. The response 120 is received in the gateway 108. The board 114 decrypts the response and encrypts the response according to another encryption scheme. In one embodiment of the invention, the board decrypts the response and encrypts the response according to WTLS. Then, the response 122 is sent to the client device 110.

Referring to Figure 2, an example of a security procedure implemented with an embodiment of the method of the invention is illustrated. At 200, there is a security protocol handshake between the client and the gateway. Then, at 202, the client provides the gateway with an indication of security parameters, including security protocol and cryptographic parameters. Then, at 204, the gateway receives data encrypted according to a first encryption scheme. Then, at 206, the data and security parameters are transmitted to the board. Then, at 208, the board decrypts the data and prevents access to the data from outside the board. Then, at 210, the gateway initiates a security protocol handshake with a server, and they both agree upon the required security parameters. Then, at 212, the board receives security parameters from the gateway. Then, at 214, the board encrypts the data according to a second encryption scheme and transmits the data to the gateway. Then, at 216, the gateway transmits the encrypted data to the server. A similar security procedure is used when data from the server is received by the gateway and transmitted to the client.

Figure 3 illustrates one embodiment of the security acceleration board 114 of the invention. The board includes a controller 300 and a hardware device 302. The controller receives data and security parameters from a bus 306. In one embodiment of the invention, the controller is a Field Programmable Gate Array (FPGA). The data is encrypted according to an encryption scheme. The controller 300 determines what conversion is needed and then transmits the data to the hardware device 302. In one embodiment of the invention, the hardware device 302 is a programmable hardware device. For example, the hardware device 302 may be a FPGA. In another embodiment of the invention, the hardware device 302 is a non-programmable hardware device. For example, the

hardware device 302 may be an Application Specific Integrated Circuit (ASIC). The hardware device 302 decrypts the data received from the controller and encrypts the data according to another encryption scheme.

In one embodiment of the invention, the data is stored in a memory 308 during the conversion process. The controller 300 controls the access of memory 308. In one embodiment, the controller 300 prevents access to the memory from outside the board 114. This prevents the gateway 108 and sources outside the gateway from accessing the memory. In one embodiment of the invention, there may be more than one memory used to store the data during the conversion process. After the data is converted from one encryption scheme to another encryption scheme, the data is transmitted to the controller 300 to forward out of the gateway 108.

In one embodiment of the invention, board 114 includes a second hardware device 304. In this embodiment, the hardware device 302 does the decryption and encryption of data according to one encryption scheme while the second hardware device 304 does the decryption and encryption of data according to another encryption scheme. For example, suppose that the board 114 is used to convert data from WTLS to SSL and from SSL to WTLS. The hardware device 302 may be configured for SSL encryption and decryption while the second hardware device 304 may be configured for WTLS encryption and decryption. Therefore, if the data received at the controller 300 is SSL encrypted, the controller will transmit the data to hardware device 302 to decrypt the data. Then, hardware device 302 will transmit the data to the second hardware device 304 to encrypt the data according to WTLS. The data is then transmitted to the controller for forwarding out of the gateway. Conversely, if the data received at the

controller is WTLS encrypted, the controller will transmit the data to the second hardware device 304 to decrypt the data. Then, the second hardware device 304 will transmit the data to the hardware device 302 to encrypt the data according to SSL.

In one embodiment of the invention, the second hardware device 304 is a programmable hardware device, for example, a FPGA. In another embodiment of the invention, the second hardware device 304 is a non-programmable hardware device, for example, an ASIC.

Figure 4 illustrates one embodiment of the method of the invention. At 400, data is received at a first hardware device encrypted according to a first encryption scheme. In one embodiment of the invention, the data is received from a controller. In one embodiment of the invention, data and security parameters are received at the first hardware device. Then, at 402, the data is decrypted at the first hardware device. In one embodiment of the invention, the data is then transmitted to a second hardware device. At 404, the data is encrypted according to a second encryption scheme. In one embodiment of the invention, the data is encrypted according to a second encryption scheme at the first hardware device. In another embodiment of the invention, the data is encrypted according to a second encryption scheme at the second hardware device. In one embodiment of the invention, the decrypted data is stored and retrieved during the conversion from the first encryption scheme to the second encryption scheme. The data may be stored in a memory. In one embodiment of the invention, access to the stored decrypted data from outside the board 114 is prevented. This prevents access to the stored decrypted data from the gateway 108 and any source outside the gateway. In one embodiment of the invention, access to the stored decrypted

data is prevented by the controller 300. In one embodiment of the invention, the data encrypted according to the second encryption scheme is transmitted to the controller to forward out of a gateway.

The above description of illustrated embodiments of the invention, including what is described in the Abstract, is not intended to be exhaustive or to limit the invention to the precise forms disclosed. While specific embodiments of, and examples for, the invention are described herein for illustrative purposes, various equivalent modifications are possible within the scope of the invention, as those skilled in the relevant art will recognize.

These modifications can be made to the invention in light of the above detailed description. The terms used in the following claims should not be construed to limit the invention to the specific embodiments disclosed in the specification and the claims. Rather, the scope of the invention is to be determined entirely by the following claims, which are to be construed in accordance with established doctrines of claim interpretation.