EFFICIENT TRANSMISSION OF CRYPTOGRAPHIC INFORMATION IN SECURE REAL TIME PROTOCOL

CROSS REFERENCE

[0001] This present application claims priority to Provisional Application No. 60/554,311 entitled "Efficient Transmission of Cryptographic Information in Secure Real Time Protocol," filed March 18, 2004, the contents of which is expressly incorporated herein by reference as though fully set forth in full.

BACKGROUND

FIELD

[0002] The present disclosure relates generally to security in data processing systems, and more particularly, efficient transmission of cryptographic information in secure real time protocol.

BACKGROUND

[0003] Real Time Protocol (RTP) is an Internet protocol standard for real time transmission of multimedia data. Today, RTP supports numerous multimedia applications including, by way of example, multicast and unicast network services. Multicast network services are usually associated with a multimedia transmission from a content provider to any number of distributed subscribers. Unicast network services are usually associated with a multimedia transmission from a content provider to a single subscriber. In either case, the subscriber can view the multimedia data in real time, or download the data for later viewing.

[0004] As the demand for multimedia applications continues to grow, the need for secured transport of multimedia content becomes more apparent. A new standard, called Secure Real Time Protocol (SRTP), has recently emerged in the telecommunications industry to address this need. SRTP can provide confidentiality, message authentication, and data integrity for RTP traffic. SRTP can also protect against active attacks such as replay attack and the like.

[0005] In SRPT, traffic is transported in packets. Namely, data to be transmitted is broken into packets. Each packet includes a header and payload. Using a same session key, the payload is encrypted at the transmitting end and decrypted at the receiving end.

The session key is a short term key that is changed periodically, typically multiple times during a single multimedia broadcast. A master key is used to derive the session key in a cryptographically secure way. More particularly, a short term random number (SK_RAND), generated by the transmitting end and sent to the receiving end, is applied to a key derivation function at both ends using the master key to produce the session key. The master key is typically a long term key that remains valid for the subscription period of the multimedia subscriber.

[0006] The SRTP also includes an optional field called a Master Key Identifier (MKI). This field may be included in the SRPT header. The MKI may be used to identify the master key from which the session key(s) were derived and may be used for other key management. In multicast network services, such as broadcast systems, the SK-RAND and other information is carried by the MKI.

[0007] However, SRTP requires that the MKI information be sent with every packet, or none of the packets, thereby wasting valuable bandwidth. Accordingly, there is a need for a more efficient and/or effective way to send the MKI in SRTP.

SUMMARY

[0008] A method of transmitting Master Key Identifier (MKI) information using secure real time protocol is disclosed. The method includes dividing MKI information into a plurality of portions, attaching a portion of the MKI information to a data packet, and transmitting the data packet with the attached portion of the MKI information.

[0009] A method of receiving Master Key Identifier (MKI) information using secure real time protocol is disclosed. The method includes receiving a plurality of data packets, each being attached to a different portion of the MKI information, and recovering the MKI information from the received portions of the MKI information.

[0010] An apparatus with secure real time protocol capability is disclosed. The apparatus includes means for dividing MKI information into a plurality of portions, means for attaching a portion of the MKI information to a data packet, and means for transmitting the data packet with the attached portion of the MKI information.

[0011] Another apparatus with secure real time protocol capability is disclosed. The apparatus includes means for receiving a plurality of data packets, each being attached to a different portion of the MKI information, and means for recovering the MKI information from the received portions of the MKI information.

[0012] It is understood that other embodiments of the present invention will become readily apparent to those skilled in the art from the following detailed description, wherein various embodiments of the invention are shown and described by way of illustration. As will be realized, the invention is capable of other and different embodiments and its several details are capable of modification in various other respects, all without departing from the spirit and scope of the present invention. Accordingly, the drawings and detailed description are to be regarded as illustrative in nature and not as restrictive.

BRIEF DESCRIPTION OF DRAWINGS

[0013] FIG. 1 is a functional block diagram illustrating an example of a transmitting and receiving terminal in a communications system;

[0014] FIG. 2 is a more detailed functional block diagram illustrating an example of a transmitting and receiving terminal in a communications system;

[0015] FIG. 3 is a flow diagram illustrating the operation of an encryption module;

[0016] FIG. 4 is a flow diagram illustrating the operation of a decryption module;

[0017] FIG. 5 is a flow diagram illustrating a method of transmitting MKI information using secure real time protocol; and

[0018] FIG. 6 is a flow diagram illustrating a method of receiving MKI information using secure real time protocol.

DETAILED DESCRIPTION

[0019] The detailed description set forth below in connection with the appended drawings is intended as a description of various embodiments of the present invention and is not intended to represent the only embodiments in which the present invention may be practiced. The detailed description includes specific details for the purpose of providing a thorough understanding of the present invention. However, it will be apparent to those skilled in the art that the present invention may be practiced without these specific details. In some instances, well known structures and components are shown in block diagram form in order to avoid obscuring the concepts of the present invention.

[0020] FIG. 1 is a functional block diagram illustrating an example of a transmitting and receiving terminal in a communications system. The transmitting and receiving

terminals 102, 104 may be any suitable devices capable of supporting SRTP multimedia applications including, wired and wireless telephones, computers, laptops, personal digital assistants (PDA), broadcast equipment, video conferencing equipment, and the like. By way of example, the transmitting terminal 102 is a multimedia content provider, and the receiving terminal 104 is a subscriber of multimedia services entitling it to receive the multimedia content from the transmitting terminal 102.

[0021] The transmitting terminal 102 is shown with an encryption module 106 and the receiving terminal 104 is shown with a decryption module 108. The encryption module 106 may be used to generate SRTP packets. An SRTP packet includes an encrypted payload. A SRTP header may be attached to the SRTP packet. The SRTP header contains information such as the payload type, sequence number, time stamp, etc. An encryption function 110 may be used to encrypt the payload using a session key. The payload contains the data to be provided to the receiving terminal 108, e.g., multimedia content. An optional keyed hash function 113 may be applied to the SRTP packet and the SRTP header. The result of the hash function 113 produces a message authentication code (MAC) which may be appended to the end of the packet. The packet, along with the SRTP header and MAC, may then be transmitted over a communications link 114 to the receiving terminal 104 using an appropriate transmitter 115.

[0022] The communications link 114 may be any suitable wired or wireless link, or combination of the two. By way of example, one or both of the terminals 102, 104 may engage in wireless communications with a network access point using Code Division Multiple Access (CDMA) technology. CDMA is a modulation and multiple access scheme based on spread-spectrum communications and is well known in the art. The network access point may be a base station transceiver that serves a particular geographic area and provides access to a wired network, such as the Internet, through a gateway.

[0023] The SRTP packet, along with the SRTP header and MAC, is directed through the communications link 114 to a receiver 117 in the receiving terminal 104. The receiving terminal 104 may use the MAC to verify the authenticity and integrity of the SRTP packet. This may be achieved by applying the SRTP header and the encrypted payload to the same keyed hash function 116 used in the transmitting terminal 102. The

resulting MAC produced by the keyed hash function 116 may then be compared to the transmitted MAC via a comparator 118. The decryption function 120 may be used to recover the payload if the MAC produced by the keyed hash function 116 agrees with the transmitted one.

[0024] The encryption and decryption modules 106, 108 may be implemented as stand-alone components, or distributed across one or more components within their respective terminals. The encryption and decryption modules 106, 108 may be implemented as hardware, firmware, software, or any combination thereof. For the purposes of explanation, the encryption and decryption modules 106, 108 will be described in terms of their functionality. The manner in which they are implemented will depend on the particular application and the design constraints imposed on the overall system. Those skilled in the art will recognize the interchangeability of hardware, firmware, and software configurations under these circumstances, and how best to implement the described functionality for each particular application.

[0025] In two-way multicast communications, such as videoconferencing, teleconferencing, etc., each party transmits as well as receives. Each terminal would therefore require both an encryption and decryption module in these applications. In these applications, the encryption and decryption modules may be separate components, integrated into a single component, or distributed across multiple components in their respective terminals. In the detailed description to follow, the transmitting and receiving terminals 102, 104 will be described with an encryption module 106 at one end of the communications link 114 and a decryption module 108 at the other end. Those skilled in the art will readily recognize how to extend the concepts described throughout this disclosure to two-way communications.

[0026] FIG. 2 is a more detailed functional block diagram illustrating an example of a transmitting and receiving terminal in a communications system. The ability to engage in secured multimedia communications depends on a shared root key known by both the encryption and decryption modules 106, 108. The root key is initially set up as a configuration function. That is, the configuration manager or the network manager is responsible for distributing the root key to be loaded into memory on the various transmitting and receiving terminals 102, 104. This can be done manually or by using some form of secure key distribution scheme.

[0027] The root key may be used by the transmitting terminal 102 to distribute encrypted master keys to various receiving terminals. By way of example, a transmitting terminal that is a multimedia content provider may distribute encrypted master keys to subscribers of its services. The master key may be generated in the transmitting terminal 102 by a random number generator 202. A root key encryption function 204 may be applied to the master key before it is sent over the communications link 114 to the receiving terminal 104. The receiving terminal 104 can use its root key with a decryption function 206 to recover the master key.

[0028] The master key may be used by both the transmitting and receiving terminals 102, 104 to derive a session key for secured encrypted communications. A bit-stream generator 208 in the transmitting terminal may be used to generate a bit-stream, such as for example, a random number, which is often referred to in the art as a SK_RAND. A key derivation function 210 uses the bit-stream and the master key as inputs to generate the session key. The key derivation function 210 is a one-way encryption, such as a hash function or the like. The session key generated by the key derivation function 210 may then be used to encrypt the payload in a manner described in greater detail above.

[0029] The bit-stream may also be provided to a processing element 211 used to generate the header. By way of example, the processing element 211 may be used to generate information to be inserted in the MKI field of the SRTP header. Included in the information is the bit-stream. As explained in greater detail earlier, the SRTP header, along with the MAC, are attached to the SRTP packet, and sent across the communications link 114. At the receiving end, the bit-stream may be recovered from MKI field of the SRTP header and input with the master key to a key derivation function 214. The key derivation function 214 performs the same encryption function as the transmitting terminal 102. The result of the key derivation function 214 produces a session key that may be used by the decryption function 120 to recover the payload.

[0030] The processing element 211 may reduce the overhead associated with the SRTP header by sending the information in the MKI field in multiple packets. For example, the processing element 211 may be used to determine the number of packets (N) required to send the information by dividing the total bit length (L_i) of the information that needs to be sent by the minimum bit length (L_{mki}) of the MKI field allowed by the protocol. If the information that needs to be sent in the MKI field to the

receiving terminal 104 is 24-bits in length, i.e., $L_i = 24$, and the minimum bit length of the MKI field is 8 bits, i.e., $L_{mki} = 8$, (as is the case in SRTP), then three packets may be used to send the information to the receiving terminal 104. If the information is 20-bits in length, i.e., $L_i = 20$, then three packets may still be used, but the information will need to be padded with 4-bits before being split up into three packets. Alternatively, the information can be split between the three (3) packets first, and then the MKI field in one or more of the SRTP headers may be padded. In any event, the information is split up into N information portions, where N equals L_i divided by L_{mki} rounded up to the nearest integer. Each information portion is inserted in the MKI field of the SRTP header for one of the packets and transmitted with the encrypted payload and MAC across the communications link 114 to the receiving terminal 104.

[0031] At the receiving terminal 104, an assembler 215 may be used to recover the information from the MKI field of the N consecutive packets. If the information in the MKI field for one of the packets is padded, the padded segment is not used by the assembler 215 to recover the information from the MKI field of the N packets. Alternatively, if the recovered information is padded, the padded segment of the information may be discarded by the assembler 215. In any event, once the information is recovered, the bit-stream may be provided to the key derivation function 214 to generate the session key to decrypt the payload.

[0032] FIG. 3 is a flow diagram illustrating the operation of an encryption module. In step 302, the encryption module may generate a bit-stream. The bit-stream may be used to derive a session key in step 304, and the session key may be used to encrypt data in step 306. In step 308, the bit-stream may be included as part of the information that is transmitted in the MKI field of the SRTP header. Alternatively, the bit-stream may be included as part of any information that is transmitted in the SRTP header. In the latter case, padding may be added to the MKI field in step 308, if the length of the MKI information is not evenly dividable by the minimum length of the MKI field allowed by the protocol. In any event, a portion of the information may be attached to a data packet having the encrypted data in step 310. Padding may be added in step 310 if the length of the MKI information portion is less than the minimum length of the MKI field allowed by the protocol. The data packet with the attached portion of the information may be transmitted in step 312. Returning to step 310, once the portion of the information is attached to the data packet, addition data may be encrypted in step 306 in

preparation for the next data packet transmission. In some applications, the bit-stream may be the only information in the SRTP header that is divided and transmitted over multiple data packets.

[0033] FIG. 4 is a flow diagram illustrating the operation of a decryption module. In step 402, multiple data packets are received. A portion of the information is attached to each data packet. As explained above, the information may be from the MKI field of the SRTP header, or any other portion of the SRTP header. Alternatively, the information may consist solely of the bit-stream. In any event, the bit-stream may be recovered by assembling the information portions attached to the data packets in step 404. If a portion of the information attached to one of the data packets has been padded, the padded segment is not used when recovering the information. If the information, once recovered, is padded, then the padded segment of the information may be discarded. In step 406, bit-stream may be used to derive the session key, and in step 408, the session key may be used to decrypt the data in the data packets.

[0034] FIG. 5 is a flow diagram illustrating a method of transmitting MKI information using secure real time protocol. In step 502, the MKI information is divided into a plurality of portions. A portion of the MKI information is attached to a data packet in step 504, and the data packet, with the attached portion of the MKI information, is transmitted in step 506.

[0035] FIG. 6 is a flow diagram illustrating a method of receiving MKI information using secure real time protocol. In step 602, a plurality of data packets are received, with a different portion of the MKI information attached to each. In step 604, the MKI information is recovered from the received portions of the MKI information.

[0036] For example, assume that the MKI information is divided into smaller portions or chunks and transmitted in N packets. The MKI information may be recovered by gathering N consecutive MKIs and reassembling them into the information. Therefore, the MKI information can be processed in the same manner as it would have been if the information had been transmitted with every Nth packet. Also, it should be noted that the information may vary over time, but would remain the same for many data packets in a row.

[0037] By dividing and transmitting the information to be sent in the overhead into a plurality of portions, the overhead is, in effect, sent on every Nth packet rather than every packet. This significantly reduces the overhead of sending the MKI.

[0038] Although the flow diagrams describe the operation of the encryption and decryption modules as a sequential process, some of the operations can be performed in parallel or concurrently. In addition, the order of the operations may be rearranged. In some embodiments, certain steps may be omitted, or additional steps may be added depending on the particular application and the overall design constraints.

[0039] The various illustrative logical blocks, modules, circuits, elements, and/or components described in connection with the embodiments disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic component, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general-purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing components, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[0040] The methods or algorithms described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. A storage medium may be coupled to the processor such that the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor.

[0041] The previous description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without departing from

the spirit or scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein, but is to be accorded the full scope consistent with the claims, wherein reference to an element in the singular is not intended to mean "one and only one" unless specifically so stated, but rather "one or more." All structural and functional equivalents to the elements of the various embodiments described throughout this disclosure that are known or later come to be known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed by the claims. Moreover, nothing disclosed herein is intended to be dedicated to the public regardless of whether such disclosure is explicitly recited in the claims. No claim element is to be construed under the provisions of 35 U.S.C. §112, sixth paragraph, unless the element is expressly recited using the phrase "means for" or, in the case of a method claim, the element is recited using the phrase "step for."

WHAT IS CLAIMED IS:

CLAIMS

1. A method of transmitting Master Key Identifier (MKI) information using secure real time protocol, comprising:

dividing MKI information into a plurality of portions;

attaching a portion of the MKI information to a data packet; and

transmitting the data packet with the attached portion of the MKI information.

2. The method of claim 1 further comprising padding the portion of the MKI information attached to the data packet.

3. The method of claim 1 further comprising padding the MKI information.

4. The method of claim 1 wherein the MKI information includes a bit-stream used to derive a session key.

5. The method of claim 4 wherein the bit-stream includes a short term random number.

6. A method of communications using secure real time protocol, comprising:

deriving a session key from a bit-stream;

encrypting data with the session key;

diving information into a plurality of portions; and

transmitting a portion of the information attached to a data packet having the encrypted data, the information including the bit-stream.

7. A method of receiving Master Key Identifier (MKI) information using secure real time protocol, comprising:

receiving a plurality of data packets, each attaching a portion of MKI information; and

recovering the MKI information from the received portions of the MKI information.

8. The method of claim 7 wherein a segment of one of the portions of the MKI information is not used when recovering the MKI information.

9. The method of claim 8 further comprising discarding a segment of the recovered MKI information.

10. The method of claim 7 wherein the recovered MKI information includes a bit-stream used to derive a session key.

11. The method of claim 10 wherein the bit-stream includes a short term random number.

12. A method of communications using secure real time protocol, comprising:

receiving a plurality of data packets, each attaching a portion of information, the information including a bit-stream;

recovering the bit-stream from the received portions of the information; and

decrypting data from the data packets with a session key derived from the bit-stream.

13. Apparatus with secure real time protocol capability, comprising:

an encryption module configured to divide MKI information into a plurality of portions and attach a portion of the MKI information to a data packet; and

a transmitter configured to transmit the data packet with the attached portion of the MKI information.

14. An apparatus with secure real time protocol capability, comprising:

an encryption module having a key derivation function configured to derive a session key from a bit-stream, and an encryption function configured to encrypt data with the session key, the encryption module being further configured to divide information into a plurality of portions; and

a transmitter configured to transmit a portion of the information attached to a data packet having the encrypted data, the information including the bit-stream.

15. An apparatus with secure real time protocol capability, comprising:

a receiver configured to receive a plurality of data packets, each attaching a portion of MKI information; and

a decryption module configured to recover the MKI information from the received portions of the MKI information.

16. An apparatus with secure real time protocol capability, comprising:

a receiver configured to receive a plurality of data packets, each attaching a portion of information, the information including a bit-stream; and

a decryption module configured to recover the bit-stream from the received portions of the information, the decryption module comprising a key derivation function configured to derive a session key from the bit-stream and a decryption function configured to decrypt data from the data packets with the session key.

17. An apparatus with secure real time protocol, comprising:

means for dividing MKI information into a plurality of portions;

means for attaching a portion of the MKI information to a data packet; and

means for transmitting the data packet with the attached portion of the MKI information.

18. The apparatus of claim 17 further comprising means for padding the portion of the MKI information attached to the data packet.

19. The apparatus of claim 17 further comprising means for padding the MKI information.

20. An apparatus with secure real time protocol capability, comprising:

means for receiving a plurality of data packets, each being attached to a portion of the MKI information; and

means for recovering the MKI information from the received portions of the MKI information.

21. The apparatus of claim 20 wherein a segment of one of the portions of the MKI information is not used when recovering the MKI information.

22. The apparatus of claim 20 further comprising means for discarding a segment of the recovered MKI information.

23. Computer readable media embodying a program of instructions executable by a processor to perform a method of transmitting Master Key Identifier (MKI) information using secure real time protocol, the method comprising:

dividing MKI information into a plurality of portions;

attaching a portion of the MKI information to a data packet; and

transmitting the data packet with the attached portion of the MKI information.

24. The computer readable media of claim 23 wherein the method further comprises padding the portion of the MKI information attached to the data packet.

25. The computer readable media of claim 23 wherein the method further comprises padding the MKI information.

26. Computer readable media embodying a program of instructions executable by a processor to perform a method of communications, the method comprising:

deriving a session key from a bit-stream;

encrypting data with the session key;

dividing information into a plurality of portions; and

transmitting a portion of information attached to a data packet having the encrypted data, the information including the bit-stream.

27. The computer readable media of claim 26 wherein the data packet includes an unencrypted header having the portion of the information.

28. The computer readable media of claim 27 wherein an unencrypted header includes a Master Key Identifier (MKI) field having the portion of the information.

29. Computer readable media embodying a program of instructions executable by a processor to perform a method of receiving Master Key Identifier (MKI) information using secure real time protocol, comprising:

receiving a plurality of data packets, each attaching a portion of the MKI information; and

recovering the MKI information from the received portions of the MKI information.

30. The computer readable media of claim 29 wherein a segment of one of the MKI information portions is not used when recovering the MKI information.

31. The computer readable media of claim 29 further comprising discarding a segment of the recovered MKI information.

32. Computer readable media embodying a program of instructions executable by a processor to perform a method of communications using secure real time protocol, comprising:

receiving a plurality of data packets, each attaching a portion of information, the information including a bit-stream;

recovering the bit-stream from the received portions of the information;

decrypting data from the data packets with a session key derived from the bit-stream.

33. The computer readable media of claim 32 wherein each of the data packets includes an unencrypted header having one of the received portions of the information.

34. The computer readable media of claim 33 wherein each of the headers includes a Master Key Identifier (MKI) field having one of the received portions of the information.