

APPARATUS AND METHOD FOR SIGNALING ENHANCED SECURITY CONTEXT FOR SESSION ENCRYPTION AND INTEGRITY KEYS

BACKGROUND

Cross-Reference to Related Applications

- [0001] This application claims the benefit of U.S. Provisional Application No. 61/324,646, filed April 15, 2010, which application is incorporated herein by reference.

Field

- [0002] The present invention relates generally to an enhanced security context signaling for user equipment operating in a Universal Mobile Telecommunications Service (UMTS) and/or GSM Edge Radio Access Network (GERAN).

Background

- [0003] A successful AKA (Authentication and Key Agreement) authentication in a UMTS third generation (3G) radio access network or in a GERAN networks using 3G AKA authentication results in a pair of shared keys, a cipher key (CK) and an integrity key (IK), for securing communications between a user equipment (UE) and the network. The shared keys may be used directly to secure the traffic between the UE and the network as in the case of UTRAN (UMTS Terrestrial Radio Access Network), or may be used to statically derive keys, e.g. K_C or K_{C128} , in the case of GERAN (GSM Edge Radio Access Network).
- [0004] A compromised key may result in serious security problems until the keys are changed at a next AKA authentication. Typically, the AKA authentication is not run often due to the significant overhead required. Also, if both keys (CK and IK) are compromised, then the GERAN keys are compromised.
- [0005] In UMTS/HSPA (High Speed Packet Access) deployments, some or all of functionalities of a radio network controller (RNC) and a Node B may be collapsed together into one node at the edge of the network. The RNC needs the keys for functionalities such as user plane ciphering and signaling plane ciphering and integrity protection. However, the RNC functionality may be deployed in an exposed location

such as in a Home Node B in a UMTS Femtocell. Accordingly, RNC functionality deployed in possibly insecure locations providing access (including physical access) may allow the keys, CK and IK, to be compromised.

- [0006] Session keys (modified version of CK and IK) may be used to lower the security risks associated with exposed RNC functionality. Techniques for providing such session keys are disclosed in U.S. Patent Application Publication No. US 2007/0230707 A1.
- [0007] Unfortunately, the use of such session keys require upgrade modifications to the serving networks. However, networks operators are likely to upgrade serving networks in a staged manner.
- [0008] There is therefore a need for a technique for signaling enhanced security context support which is compatible with legacy serving networks.

SUMMARY

- [0009] An aspect of the present invention may reside in a method for establishing a first security context between a remote station and a serving network. The first security context has a security property that is not supported by a second security context. In the method, the remote station forwards a first message to the serving network, wherein the first message includes an information element signaling that the remote station supports the first security context. The remote station generates at least one session key, in accordance with the first security context, using the information element. The remote station receives, in response to the first message, a second message having an indication that the serving network supports the first security context. The remote station, in response to the second message, has wireless communications protected by the at least one session key.
- [0010] In more detailed aspects of the invention, the information element may comprise a count value updated for a session. Further, the indication that the serving network supports the first security context may comprise an authentication code generated based on a corresponding at least one session key generated by the serving network using the information element received from the remote station. Also, the remote station may comprise a mobile user equipment.
- [0011] In other more detailed aspects of the invention, the serving network may be a UMTS serving network. The first security context may be an enhanced UMTS security

context, and the second security context may be a legacy UTRAN security context. Alternatively, the serving network may be a GERAN serving network.

- [0012] Another aspect of the invention may reside in a remote station which may include means for forwarding a first message to a serving network, wherein the first message includes an information element signaling that the remote station supports a first security context, and wherein the first security context has a security property that is not supported by a second security context; means for generating at least one session key, in accordance with the first security context, using the information element; means for receiving, in response to the first message, a second message having an indication that the serving network supports the first security context; and means for having wireless communications, in response to the second message, protected by the at least one session key.
- [0013] Another aspect of the invention may reside in a remote station which may include a processor configured to: forward a first message to a serving network, wherein the first message includes an information element signaling that the remote station supports a first security context, and wherein the first security context has a security property that is not supported by a second security context; generate at least one session key, in accordance with the first security context, using the information element; receive, in response to the first message, a second message having an indication that the serving network supports the first security context; and have wireless communications, in response to the second message, protected by the at least one session key.
- [0014] Another aspect of the invention may reside in a computer program product, comprising computer-readable storage medium, comprising code for causing a computer to forward a first message to a serving network, wherein the first message includes an information element signaling that the computer supports a first security context, and wherein the first security context has a security property that is not supported by a second security context; code for causing a computer to generate at least one session key, in accordance with the first security context, using the information element; code for causing a computer to receive, in response to the first message, a second message having an indication that the serving network supports the first security context; and code for causing a computer to have wireless communications, in response to the second message, protected by the at least one session key.

BRIEF DESCRIPTION OF THE DRAWINGS

- [0015] FIG. 1 is a block diagram of an example of a wireless communication system.
- [0016] FIG. 2 is a block diagram of an example of a wireless communication system in accordance with a UMTS/UTRAN architecture.
- [0017] FIG. 3 is a block diagram of an example of a wireless communication system in accordance with a GERAN architecture.
- [0018] FIG. 4 is a flow diagram of a method for establishing an enhanced security context between a remote station and a serving network.
- [0019] FIG. 5 is a flow diagram of a method for establishing an enhanced security context between a remote station and a serving network based on an attach request message.
- [0020] FIG. 6 is a flow diagram of a method for establishing at least one session key from an enhanced security context between a remote station and a serving network based on a service request message.
- [0021] FIG. 7 is a flow diagram of a method for establishing at least one session key from an enhanced security context between a remote station and a serving network based on a routing area update request message.
- [0022] FIG. 8 is a block diagram of a computer including a processor and a memory.

DETAILED DESCRIPTION

- [0023] The word “exemplary” is used herein to mean “serving as an example, instance, or illustration.” Any embodiment described herein as “exemplary” is not necessarily to be construed as preferred or advantageous over other embodiments.
- [0024] With reference to FIGS. 2 through 4, an aspect of the present invention may reside in a method 400 for establishing an enhanced security context between a remote station 210 and a serving network 230. In the method, the remote station forwards a first message to the serving network (step 410), wherein the first message includes an information element signaling that the remote station supports an enhanced security context. The remote station generates at least one session key, CK_S and IK_S , in accordance with the enhanced security context, using the information element (step 420). The remote station receives, in response to the first message, a second message having an indication that the serving network supports the enhanced security context (step 430). The remote

station, in response to the second message, has wireless communications protected by the at least one session key (step 440).

- [0025] The information element may comprise a count. Further, the indication that the serving network supports the enhanced security context may comprise an authentication code (MAC) generated based on a corresponding at least one session key generated by the serving network 230 using the information element received from the remote station 210. Also, the remote station may comprise a mobile user equipment (UE) such as a wireless device.
- [0026] With further reference to FIG. 8, another aspect of the invention may reside in a remote station 210 which may include means (processor 810) for forwarding a first message to a serving network 230, wherein the first message includes an information element signaling that the remote station supports an enhanced security context; means for generating at least one session key, in accordance with the enhanced security context, using the information element; means for receiving, in response to the first message, a second message having an indication that the serving network supports the enhanced security context; and means for having wireless communications, in response to the second message, protected by at least one session key.
- [0027] Another aspect of the invention may reside in a remote station 210 which may include a processor 810 configured to: forward a first message to a serving network 230, wherein the first message includes an information element signaling that the remote station supports an enhanced security context; generate at least one session key, in accordance with the enhanced security context, using the information element; receive, in response to the first message, a second message having an indication that the serving network supports the enhanced security context; and have wireless communications, in response to the second message, protected by the at least one session key.
- [0028] Another aspect of the invention may reside in a computer program product, comprising computer-readable storage medium 820, comprising code for causing a computer 800 to forward a first message to a serving network 230, wherein the first message includes an information element signaling that the computer supports an enhanced security context; code for causing a computer to generate at least one session key, in accordance with the enhanced security context, using the information element; code for causing a computer to receive, in response to the first message, a second message having an indication that the serving network supports the enhanced security context; and code for causing a

computer to have wireless communications, in response to the second message, protected by the at least one session key.

- [0029] The serving core network 230 is connected to a serving RAN (Radio Access Network) 220 which provides wireless communications to the remote station 210. In a UMTS/UTRAN architecture, the serving RAN includes a Node B and a RNC (Radio Network Controller). In a GERAN architecture, the serving RAN includes a BTS (Base Transceiver Station) and a BSC (Base Station Controller). The serving core network includes an MSC/VLR (Mobile Switching Center/Visitor Location Register) for providing circuit-switched (CS) service, and an SGSN (Serving GPRS Support Node) for providing packet-switched (PS) services. The home network includes an HLR (Home Location Register) and an AuC (Authentication Center).
- [0030] The UE 210 and the serving core network 230 may be enhanced with new security properties to create an enhanced UMTS security context (ESC) using a COUNT (counter value). A 256-bit root key (K_{ASMEU}) for the ESC may be derived from the CK and IK when AKA authentication is performed. The root key may be set equal to $CK||IK$, or it may be derived using a more complex derivation resulting in additional useful security properties (e.g., CK and IK do not need to be kept). The COUNT may be a 16-bit counter value that is maintained between the UE and the serving core network. (Note: a legacy UTRAN security context consists of KSI (a 3-bit Key Set Identifier), CK (a 128-bit encryption key), and IK (a 128-bit integrity key)).
- [0031] With reference to FIG. 5, in a method 500 related to UMTS attach procedures, the UE 210 may signal that it supports ESC in a UMTS attach request message (step 510). The ESC is an example of the first security context. The support signal may be the presence of a new information element (IE) in the message. The IE may comprise the COUNT value. A serving network SN 230 that does not support ESC will ignore the new IE. Not supporting the ESC is an example of the second security context. Authentication data (RAND, XRES, CK, IK, AUTN) is obtained from the HLR/AuC 240 (step 515). The SN may indicate ESC support in the AKA challenge (Authentication Request) to the UE (step 520). The UE performs the authentication procedures (step 525) and returns a response RES to the SN (step 530). Upon successful authentication (step 530), the UE and SN derive the root key K_{ASMEU} and the session keys CK_S and IK_S (step 535). The SN forwards the session keys to the RAN 220 in an SMC (Security Mode

Command) message (step 540). The RAN generates a message authentication code (MAC) using the session key IK_S , which is forwarded to the UE in an SMC message (step 545). The UE checks the MAC (step 550) using the session key IK_S that the UE derived (step 535), and returns a complete indication to the RAN (step 555), which forwards it to the SN (step 560). The UE is then able to protect communications using the session keys (step 565).

[0032] With reference to FIG. 6, in a method 600 related to an Idle to Active Mode procedure 600, the UE 210 forwards a service request message which includes the COUNT value to the SN 230 (step 610). The UE and SN derive new the session keys CK_S and IK_S from the root key K_{ASMEU} (step 620). The SN forwards the session keys to the RAN 220 in an SMC message (step 630). The RAN generates a MAC, which is forwarded to the UE in an SMC message (step 640). The UE checks the MAC (step 650), and returns a complete indication to the RAN (step 660), which forwards it to the SN (step 670). The UE is then able to protect communications using the session keys (step 680).

[0033] With reference to FIG. 7, in a method 700 related to mobility management procedures 700 (such as a Routing Area Update (RAU) or Location Area Update (LAU)), the UE 210 forwards a RAU (or LAU) request message which includes the COUNT value to the SN 230 (step 710). Optionally, the UE and SN may derive new the session keys CK_S and IK_S from the root key K_{ASMEU} (step 720). The SN may forward the session keys to the RAN 220 in an SMC message (step 730). The RAN may generate a MAC, which may be forwarded to the UE in an SMC message (step 740). The UE may check the MAC (step 750), and may return a complete indication to the RAN (step 760), which forwards it to the SN (step 770). The SN then sends a RAU accept message to the UE (step 780). The UE is then able to protect communications using the session keys.

[0034] New access stratum (AS) keys may be generated for each transition from Idle to Active State. Similarly, keys may be generated at other events. The COUNT value may be sent in idle mobility messages and in initial layer 3 messages, e.g., Attaches, RAUs, LAUs, for idle, mobility, or service request. The SN may check that the sent COUNT value has not been used before, and updates the stored COUNT value in the process. If the COUNT value is new (e.g., received COUNT value > stored COUNT value), the UE and the SN proceed to calculate the new key CK_S and IK_S , using a Key Derivation

Function (KDF) such as HMAC-SHA256, from the root key K_{ASMEU} and the sent COUNT value. The KDF may include additional information, such as RAN node identity, for the new key calculation. If the check fails (the COUNT value is not new), the SN rejects the message. For GERAN usage, when K_C and K_{C128} are calculated from CK_S and IK_S , it may be done in the same manner as when calculated from CK and IK.

- [0035] The session keys (CK_S and IK_S) may have a lifetime such that the UE and the serving network keep and use the session keys until either it is no longer necessary to store the keys to send traffic securely between the UE and the network (UE moves to Idle mode), or a new context is created at a subsequent event (e.g., AKA authentication or a mobility event).
- [0036] The remote station 210 may comprise a computer 800 that includes a storage medium 820 such as memory, a display 830, and an input device 840 such as a keyboard. The apparatus may include a wireless connection 850.
- [0037] With reference to FIG. 1, a wireless remote station (RS) 102 (or UE) may communicate with one or more base stations (BS) 104 of a wireless communication system 100. The wireless communication system 100 may further include one or more base station controllers (BSC) 106, and a core network 108. Core network may be connected to an Internet 110 and a Public Switched Telephone Network (PSTN) 112 via suitable backhauls. A typical wireless mobile station may include a handheld phone, or a laptop computer. The wireless communication system 100 may employ any one of a number of multiple access techniques such as code division multiple access (CDMA), time division multiple access (TDMA), frequency division multiple access (FDMA), space division multiple access (SDMA), polarization division multiple access (PDMA), or other modulation techniques known in the art.
- [0038] A wireless device 102 may include various components that perform functions based on signals that are transmitted by or received at the wireless device. For example, a wireless headset may include a transducer adapted to provide an audio output based on a signal received via the receiver. A wireless watch may include a user interface adapted to provide an indication based on a signal received via the receiver. A wireless sensing device may include a sensor adapted to provide data to be transmitted to another device.

- [0039] A wireless device may communicate via one or more wireless communication links that are based on or otherwise support any suitable wireless communication technology. For example, in some aspects a wireless device may associate with a network. In some aspects the network may comprise a body area network or a personal area network (e.g., an ultra-wideband network). In some aspects the network may comprise a local area network or a wide area network. A wireless device may support or otherwise use one or more of a variety of wireless communication technologies, protocols, or standards such as, for example, CDMA, TDMA, OFDM, OFDMA, WiMAX, and Wi-Fi. Similarly, a wireless device may support or otherwise use one or more of a variety of corresponding modulation or multiplexing schemes. A wireless device may thus include appropriate components (e.g., air interfaces) to establish and communicate via one or more wireless communication links using the above or other wireless communication technologies. For example, a device may comprise a wireless transceiver with associated transmitter and receiver components (e.g., a transmitter and a receiver) that may include various components (e.g., signal generators and signal processors) that facilitate communication over a wireless medium.
- [0040] The teachings herein may be incorporated into (e.g., implemented within or performed by) a variety of apparatuses (e.g., devices). For example, one or more aspects taught herein may be incorporated into a phone (e.g., a cellular phone), a personal data assistant ("PDA"), an entertainment device (e.g., a music or video device), a headset (e.g., headphones, an earpiece, etc.), a microphone, a medical device (e.g., a biometric sensor, a heart rate monitor, a pedometer, an EKG device, etc.), a user I/O device (e.g., a watch, a remote control, a light switch, a keyboard, a mouse, etc.), a tire pressure monitor, a computer, a point-of-sale device, an entertainment device, a hearing aid, a set-top box, or any other suitable device.
- [0041] These devices may have different power and data requirements. In some aspects, the teachings herein may be adapted for use in low power applications (e.g., through the use of an impulse-based signaling scheme and low duty cycle modes) and may support a variety of data rates including relatively high data rates (e.g., through the use of high-bandwidth pulses).
- [0042] In some aspects a wireless device may comprise an access device (e.g., a Wi-Fi access point) for a communication system. Such an access device may provide, for example, connectivity to another network (e.g., a wide area network such as the Internet or a

cellular network) via a wired or wireless communication link. Accordingly, the access device may enable another device (e.g., a Wi-Fi station) to access the other network or some other functionality. In addition, it should be appreciated that one or both of the devices may be portable or, in some cases, relatively non-portable.

- [0043] Those of skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.
- [0044] Those of skill would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.
- [0045] The various illustrative logical blocks, modules, and circuits 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 device, 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 devices, 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.

- [0046] The steps of a method or algorithm 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. An exemplary storage medium is coupled to the processor such 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. The processor and the storage medium may reside in an ASIC. The ASIC may reside in a user terminal. In the alternative, the processor and the storage medium may reside as discrete components in a user terminal.
- [0047] In one or more exemplary embodiments, the functions described may be implemented in hardware, software, firmware, or any combination thereof. If implemented in software as a computer program product, the functions may be stored on or transmitted over as one or more instructions or code on a computer-readable medium. Computer-readable media includes both computer storage media and communication media including any medium that facilitates transfer of a computer program from one place to another. A storage media may be any available media that can be accessed by a computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium that can be used to carry or store desired program code in the form of instructions or data structures and that can be accessed by a computer. Also, any connection is properly termed a computer-readable medium. For example, if the software is transmitted from a website, server, or other remote source using a coaxial cable, fiber optic cable, twisted pair, digital subscriber line (DSL), or wireless technologies such as infrared, radio, and microwave, then the coaxial cable, fiber optic cable, twisted pair, DSL, or wireless technologies such as infrared, radio, and microwave are included in the definition of medium. Disk and disc, as used herein, includes compact disc (CD), laser disc, optical disc, digital versatile disc (DVD), floppy disk and blu-ray disc where disks usually reproduce data magnetically, while discs reproduce data optically with lasers. Combinations of the above should also be included within the scope of computer-readable media.

[0048] 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 widest scope consistent with the principles and novel features disclosed herein.

CLAIMS

1. A method for establishing a first security context between a remote station and a serving network, the first security context having a security property that is not supported by a second security context, the method comprising:

the remote station forwarding a first message to the serving network, wherein the first message includes an information element signaling that the remote station supports the first security context;

the remote station generating at least one session key, in accordance with the first security context, using the information element;

the remote station receiving, in response to the first message, a second message having an indication that the serving network supports the first security context; and

the remote station, in response to the second message, having wireless communications protected by the at least one session key.

2. A method for establishing a first security context as defined in claim 1, wherein the information element comprises a count value updated for a session.

3. A method for establishing a first security context as defined in claim 1, wherein the serving network is a UMTS serving network.

4. A method for establishing a first security context as defined in claim 3, wherein the first security context is an enhanced UMTS security context, and the second security context is a legacy UTRAN security context.

5. A method for establishing a first security context as defined in claim 1, wherein the serving network is a GERAN serving network.

6. A method for establishing a first security context as defined in claim 1, wherein the indication that the serving network supports the first security context comprises an authentication code generated based on a corresponding at least one session key generated by the serving network using the information element received from the remote station.

7. A method for establishing a first security context as defined in claim 1, wherein the remote station comprises a mobile user equipment.
8. A remote station, comprising:
 - means for forwarding a first message to a serving network, wherein the first message includes an information element signaling that the remote station supports a first security context, and wherein the first security context has a security property that is not supported by a second security context;
 - means for generating at least one session key, in accordance with the first security context, using the information element;
 - means for receiving, in response to the first message, a second message having an indication that the serving network supports the first security context; and
 - means for having wireless communications, in response to the second message, protected by the at least one session key.
9. A remote station as defined in claim 8, wherein the information element comprises a count value updated for a session.
10. A remote station as defined in claim 8, wherein the serving network is a UMTS serving network.
11. A remote station as defined in claim 10, wherein the first security context is an enhanced UMTS security context, and the second security context is a legacy UTRAN security context.
12. A remote station as defined in claim 8, wherein the serving network is a GERAN serving network.
13. A remote station as defined in claim 8, wherein the indication that the serving network supports the first security context comprises an authentication code generated based on a corresponding at least one session key generated by the serving network using the information element received from the remote station.

14. A remote station as defined in claim 8, wherein the remote station comprises a mobile user equipment.

15. A remote station, comprising:
a processor configured to:

forward a first message to a serving network, wherein the first message includes an information element signaling that the remote station supports a first security context, and wherein the first security context has a security property that is not supported by a second security context;

generate at least one session key, in accordance with the first security context, using the information element;

receive, in response to the first message, a second message having an indication that the serving network supports the first security context; and

have wireless communications, in response to the second message, protected by the at least one session key.

16. A remote station as defined in claim 15, wherein the information element comprises a count value updated for a session.

17. A remote station as defined in claim 15, wherein the serving network is a UMTS serving network.

18. A remote station as defined in claim 17, wherein the first security context is an enhanced UMTS security context, and the second security context is a legacy UTRAN security context.

19. A remote station as defined in claim 15, wherein the serving network is a GERAN serving network.

20. A remote station as defined in claim 15, wherein the indication that the serving network supports the first security context comprises an authentication code generated based on a corresponding at least one session key generated by the serving network using the information element received from the remote station.

21. A remote station as defined in claim 15, wherein the remote station comprises a mobile user equipment.

22. A computer program product, comprising:

computer-readable storage medium, comprising:

code for causing a computer to forward a first message to a serving network, wherein the first message includes an information element signaling that the computer supports a first security context, and wherein the first security context has a security property that is not supported by a second security context;

code for causing a computer to generate at least one session key, in accordance with the first security context, using the information element;

code for causing a computer to receive, in response to the first message, a second message having an indication that the serving network supports the first security context; and

code for causing a computer to have wireless communications, in response to the second message, protected by the at least one session key.

23. A computer program product as defined in claim 22, wherein the information element comprises a count value updated for a session.

24. A computer program product as defined in claim 22, wherein the serving network is a UMTS serving network.

25. A computer program product as defined in claim 24, wherein the first security context is an enhanced UMTS security context, and the second security context is a legacy UTRAN security context.

26. A computer program product as defined in claim 22, wherein the serving network is a GERAN serving network.

27. A computer program product as defined in claim 22, wherein the indication that the serving network supports the first security context comprises an authentication code generated based on a corresponding at least one session key generated by the serving network using the received information element.