

## **PRIVACY PROTECTION IN COMMUNICATION SYSTEMS**

### **Claim of Priority under 35 U.S.C. §119**

[0001] The present Application for Patent claims priority to Provisional Application Serial No. 60/758,971, filed January 13, 2006, and Provisional Application Serial No. 60/762,771, filed January 27, 2006, both assigned to the assignee hereof, and the entire disclosures of which are hereby expressly incorporated by reference herein.

### **BACKGROUND**

#### **Field**

[0002] The present invention generally relates to communications, and more particularly, to protecting a user's privacy in communication systems.

#### **Background**

[0003] As modern devices become capable of communicating with arbitrary application servers, there is a need for such communications to be authenticated and secured. In asymmetric or public key systems, the device (or "user") may present a public key to an application server (or "application"), while keeping a separate private key confidential. In shared or symmetric key systems, the user may conduct communications with an application using a user identity, which might be "anonymous" in that the user identity may not reveal who the user actually is. Upon receiving this user identity, the application can then obtain a key linked to that user identity to engage in encrypted communications with the user. The key may be one previously known to the application, or it may be fetched from a key server, e.g., a third party that is trusted by both the user and the application.

[0004] There are certain ways in which user privacy might be compromised in these systems, even when an "anonymous" user identity is used. For example, if a user exchanges the same user identity with an application over multiple

sessions, the application might infer private information about the user by linking the user's sessions to each other. This is referred to as a "linkability attack." For example, in a wireless network, using one identity to access several base stations could lead to a user being tracked across the network.

Alternatively, if a user accesses several different applications using the same user identity, then a third party might ascertain which applications the user has accessed, and when the user has accessed them, by passively eavesdropping on the communication of user identity between the application and the key server. This potentially reveals private information about the user's preferences. The same information might be obtained by a third party directly querying the accessed applications.

## SUMMARY

[0005] One aspect of the present invention provides a method for protecting user privacy comprising generating a derived identity associated with a user based on a key and at least one parameter comprising a session variable; and sending said derived identity to an application.

[0006] Another aspect of the present invention provides a method for protecting user privacy during communications in a system having a key server, said method comprising receiving from a user a derived identity generated from a key and at least one parameter comprising a session variable; transmitting said derived identity to said key server; and receiving from said key server information associated with said user.

[0007] Yet another aspect of the present invention provides a method for protecting user privacy comprising receiving, from a user, a derived key identity generated from a key and at least one parameter comprising a session variable; and identifying said key from said derived key identity.

[0008] Yet another aspect of the present invention provides a method for protecting user privacy during communications in a system having a key server, said method comprising receiving from a requesting application a derived identity generated from a key and at least one parameter comprising a session variable; and identifying said user from said derived identity.

- [0009] Yet another aspect of the present invention provides an apparatus for protecting user privacy comprising a derived identity generator for generating a derived identity associated with a user based on a key and at least one parameter comprising a session variable; a transmitter for sending said derived identity to an application.
- [0010] Yet another aspect of the present invention provides an apparatus for protecting user privacy during communications in a system having a key server, said apparatus comprising a receiver for receiving from a user a derived identity generated from a key and at least one parameter comprising a session variable; and a transmitter for transmitting said derived user identity to said key server.
- [0011] Yet another aspect of the present invention provides an apparatus for protecting user privacy comprising a receiver for receiving, from a user, a derived key identity generated from a key and at least one parameter comprising a session variable; a processor for identifying said key from said derived key identity.
- [0012] Yet another aspect of the present invention provides An apparatus for protecting user privacy during communications in a system having a key server, said apparatus comprising a receiver for receiving from a requesting application a derived identity generated from a key and at least one parameter comprising a session variable; and a processor for identifying said user from said derived identity.
- [0013] Yet another aspect of the present invention provides an apparatus for protecting user privacy during communications with an application, said apparatus comprising a means for generating a derived identity; a means for sending said derived identity to an application.
- [0014] Yet another aspect of the present invention provides an apparatus for protecting user privacy during communications in a system having a key server, said apparatus comprising a receiver for receiving from a requesting application a derived identity generated from a key and at least one parameter comprising a session variable; a means for identifying said user from said derived identity; and a transmitter for transmitting information associated with said user to said requesting application.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0015] FIG. 1 shows an embodiment of the present invention in which a key server is used to facilitate encrypted communications between a user and an application.

[0016] FIG. 2 illustrates an embodiment of a process or method in which the user may establish secure communications with an application according to the embodiment shown in FIG. 1.

[0017] FIG. 3 shows an embodiment of a process or method in which the user can securely communicate with an application, without using a key server.

## DETAILED DESCRIPTION

[0018] To protect user privacy, there is a need for providing secure communications between a user and an application, without revealing the actual identity of the user to the application or to a third party eavesdropping on the communication, or otherwise allowing the application to determine that different sessions originate from the same user. The invention disclosed herein addresses this need.

[0019] Reference is now directed to FIG. 1, which shows an embodiment of a communication system 100 wherein a key server is used to facilitate encrypted communications between a user and an application.

[0020] The communication system 100 can be any voice, data or multimedia system, for example, operating under a communications standard and/or protocol, such as the WCDMA (Wideband Code Division Multiple Access), cdma2000, or IP (Internet Protocol) standard, or any other suitable standard or protocol. The embodiment may be utilized, for example, as an enhancement to the Generic Bootstrapping Architecture as specified in various communications standards. (See, e.g., “Generic Authentication Architecture (GAA): Generic bootstrapping architecture,” 3GPP TS 33.220, and “Generic Bootstrapping Architecture (GBA) Framework,” 3GPP2 S.S0109-0 Version 1.)

[0021] As illustrated in FIG. 1, a user 114 (also referred to as a user equipment) may access an application 116 in the system 100. The application 116 may be a dedicated server in the network serving a specific application, e.g., VoIP (Voice over Internet Protocol), or a network element itself. The application 116 may also be a software application stored in servers or other devices on the network. In an embodiment (not shown), the application 116 could reside on the same physical device as a key server 126. Each application may have its own dedicated transmitter / receiver circuit (not shown) for communicating with the user 114 and/or the key server 126, or several applications may share a common transmitter / receiver circuit. It may be noted that an application may include several physical entities, e.g., the application may be an entire mobile network comprising multiple base stations.

[0022] In one embodiment, the user 114 may pre-store a key 102 in its memory. Both the key 102, and the fact that it is stored in user 114, are known to the key server 126. The key 102 may be unique to user 114, or to a group of users that includes user 114. The key 102 may be used permanently, or only during a specific time period. In an embodiment, the key 102 is known only to authorized parties such as the key server 126 and the user 114.

[0023] In one embodiment, both the user 114 and the key server 126 can generate a temp\_ID 108 (also referred to as a derived identity) using a common formula, as follows:

$$temp\_id = F(key, m) \quad \text{Eq (1)}$$

In Eq (1), F is a predetermined algorithmic function such as a cryptographic hash function. Alternatively, F can be a function that serially concatenates one or more parameters with the output of one or more hash functions. F can also be a function that performs a hash on the combination of a number of parameters with the output of one or more other hash functions. In an embodiment, the predetermined algorithmic function can be the Secure Hash Algorithm SHA-1. (See Federal Information Processing Standard Publication 180-1 (1995).)

[0024] Also in Equation (1), m denotes a parameter set which may include, for example, a user identity, one or more session-dependent variables, and/or other

parameters. A session may denote a set of communications between a user and an application in which the same temp\_ID is used. In an embodiment, m generally includes at least one session variable that may change each time a temp\_ID is exchanged with an application. Such a variable may be a digitally incremented use counter, a time stamp, or output of a pseudorandom number generator. It will be understood that larger session variables may be used for greater security, at the cost of greater implementational complexity. In an embodiment, the session variable can be a 16-bit counter value.

[0025] Referring again to FIG. 1, both F and m are known to the user 114 and key server 126. In one embodiment, the key server 126 may pre-calculate and store the values of temp\_ID based on a given key 102 and all possible values of the parameter m, so that, given a temp\_ID, the key 102 used to generate it may be quickly identified.

[0026] FIG. 2 illustrates an embodiment of a process or method 200 in which user 114 may establish secure communications with application 116 according to the embodiment shown in FIG. 1. First, in step 201, user 114 calculates temp\_ID 108 from the key and the parameter set m, and sends the temp\_ID 108 to the application 116.

[0027] In step 202, once it has received the temp\_ID 108 sent by user 114, application 116 sends the temp\_ID 108 to the key server 126.

[0028] As described earlier, in one embodiment, the key server 126 has pre-stored a set of temp\_IDs and keys in its memory. In step 203, the key server 126 uses the temp\_ID 108 received from the application 116 to identify key 102. As mentioned previously, each key can correspond to a unique user. In this example, key 102 corresponds to user 114. The key server 126 can therefore match temp\_ID 108 with user 114, as shown in step 203.

[0029] In step 203, the key server 126 may further generate a sub\_key 238 (also called traffic key herein) based on key 102. This generation of a sub-key may use another algorithmic function and involve parameters known only to the user 114 and key server 126. In one embodiment, the value of temp\_ID 108 itself may be used in generating the associated sub-keys. In an alternative embodiment, any number of sub-keys 238 can be generated by taking a hash function (e.g., SHA-1) of the key 102 and an appropriate sequence number.

- [0030] In step 204, the key server 126 sends the sub\_key 238 to the application 116. The key server 126 may also send other information about the user 114 to the application 116.
- [0031] The user 114 can independently generate sub\_key 238 (or “traffic key”) from parameters already known to it. Thus, with the sub\_key 238 known to both the application 116 and the user 114, both sides can use the sub\_key 238 to encrypt and decrypt data 240 sent between them, as depicted in step 205.
- [0032] Referring back to FIG. 1, if the user 114 subsequently accesses another application 122, a temp\_ID other than the temp\_ID 108 may be calculated in accordance with Eq (1) as described above. If the function F is chosen so that the relationship between temp\_ID 108 and other temp\_IDs used during different sessions by the same user is not readily discernible, it would be difficult for an unauthorized party to link an intercepted temp\_ID with any particular user, thus preserving the user’s identity privacy.
- [0033] In one embodiment, the parameter set m used to generate temp\_ID in Eq (1) may include an application identity (app\_ID) corresponding to the accessed application. In this way, a key server 126 can tell from the temp\_ID 108 whether application 116 requesting user information from the key server 126 has in fact been accessed by the user 114. For security, the key server 126 may choose to send information about the user 114, including the user identity and the user-specific key, only to an application 116 whose app\_ID matches the app\_ID used to generate temp\_ID 108. This prevents another application such as application 118, which has not been accessed by the user 114, from obtaining information about user 114 from the key server 126.
- [0034] In an embodiment, a user 114 may even be called upon to generate a temp\_ID when the user 114 does not yet know the app\_ID of the application it wishes to access. In this case, the user may nevertheless generate a temp\_ID by using a fixed “wildcard” or “default” app\_ID in place of an application-specific app\_ID. In this embodiment, the key server can be configured to recognize a temp\_ID containing such a “wildcard” or “default” app\_ID, and provide user-specific data to an application even though the wildcard app\_ID does not match the app\_ID of the requesting application. At a later time, once the user has

ascertained the application's app\_ID, the user may generate a new temp\_ID based on the correct app\_ID.

[0035] In another embodiment of the invention, if a new parameter set m' is agreed upon by the user and the application during a session, then, by querying a key server, an application could determine a new temp\_ID to be used during a subsequent session. To do this, the application could provide, for example, the new parameter set m', along with the temp\_ID initially received from the user, to the key server. This saves the user from having to transmit a new temp\_ID to the application every time use of a new temp\_ID is desired.

[0036] FIG. 3 shows an embodiment of a process or method 300 in which the user 114 can securely communicate with an application 116, without using a key server. In this embodiment, it is assumed that the user 114 and application 116 already share a key K through some key distribution scheme, prior to initiating the communications depicted in FIG. 3. In an embodiment, the key K is a variable known only to authorized parties such as the user and the application.

[0037] In step 301, user 114 can generate a Derived\_Key\_ID 310 as follows:

[0038] 
$$\text{Derived\_Key\_ID} = F(K, \text{session variable, other parameters}) \quad \text{Eq (2)}$$

[0039] where F is again a predetermined algorithmic function, session variable is a session-dependent variable such as a counter value, and other parameters may include any parameter not explicitly enumerated herein that is known to both the user 114 and the application 116. As previously noted, a session variable may change each time a temp\_ID is exchanged with an application, and may be a digitally incremented use counter, a time stamp, or output of a pseudorandom number generator. It will be understood that larger session variables may be used for greater security, at the cost of greater implementational complexity. In an embodiment, the session variable can be a 16-bit counter value.

[0040] In step 302, user 114 sends the Derived\_Key\_ID 310 to the application 116. In step 303, application 116, which has pre-calculated the set of Derived\_Key\_ID's over all possible values of key K, session variable, and other parameters and stored this set in memory, can identify the key K, session variable used to generate the received Derived\_Key\_ID 310, and the associated

user 114. With both sides knowing the values of K, session variable 331, and other parameters, both sides can calculate a common key Derived\_K 332 as follows:

[0041] 
$$\text{Derived\_K} = G(\text{K, session variable, other parameters}) \quad \text{Eq (3)}$$

[0042] where G is another predetermined algorithmic function and session variable 331 corresponds to the session variable used to generate Derived\_key\_ID 310 in Equation (2). It may be noted the function G may be chosen to be the same as that used to generate the sub\_key 238 earlier described with reference to FIG. 2. Secure communications can now be conducted using the Derived\_K 332 to send and receive encrypted data 340, as shown in step 304.

[0043] In a further embodiment of the invention, if a new parameter set m' is agreed upon by the user and the application during a session, then the application could determine, using Eq (3), a new temp\_ID to be used by the user during a subsequent session. This would provide protection against linkability attacks by a third-party. For example, a user could vary its temp\_ID's during sessions with different base stations in a mobile network to avoid being tracked by a third-party eavesdropper.

[0044] It may be noted that while the above embodiments have been described in the context of shared-key or symmetric cryptographic systems, public-key or asymmetric cryptographic systems are also susceptible to linkability attacks where a user repeatedly uses the same public key. Aspects of the present invention may also be applied to vary the private key, and hence the public key, according to a session-dependent variable and/or application identity. It may be noted however that in public key systems, the overhead of registration and certificate issuance processes required each time a public/private key pair is changed may lead to the same public/private key pair preferably being used over an extended period of time.

[0045] According to an embodiment, the memory in each of the key server 126 and the user 114 can be of either the volatile or non-volatile type, such as a magnetic hard drive or a RAM (Random Access Memory) circuit. As an alternative, the memory can also be made of other circuit types, such as an

EEPROM (Electrically Erasable Programmable Read Only Memory), an EPROM (Electrical Programmable Read Only Memory), a ROM (Read Only Memory), an ASIC (Application Specific Integrated Circuit), a magnetic disk, an optical disk, and others well known in the art.

[0046] It should be noted the invention can be embodied as a process or method and be coded as computer-readable instructions carried on any computer-readable medium known in the art. Here, the term “computer-readable medium” refers to any medium that participates in providing instructions to any processor, such as the processors in the key server 126 and the user 114 shown in FIG. 1. Such a medium can be of the storage type and may take the form of a volatile or non-volatile storage medium as also described previously, for example, in the description of the memory in the key server 126 and the user 114. Such a medium can also be of the transmission type and may include a coaxial cable, a copper wire, an optical cable, and the air interface carrying acoustic or electromagnetic waves capable of carrying signals readable by machines or computers.

[0047] 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.

[0048] 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.

[0049] 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.

[0050] 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 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. 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.

[0051] 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. While exemplary embodiments have been described, it will be understood by those skilled in the art that these and other changes in form and detail may be made therein without departing from the scope and spirit of the invention.

## CLAIMS

1. A method for protecting user privacy comprising:  
generating a derived identity associated with a user based on a key and at least one parameter comprising a session variable; and  
sending said derived identity to an application.
2. The method of claim 1, further comprising:  
generating a traffic key; and  
communicating with said application using said traffic key.
3. The method of claim 1, wherein said user communicates with the same application for at least two sessions.
4. The method of claim 1, wherein said user communicates with a different application each session for at least two sessions.
5. The method of claim 1, wherein said session variable comprises a counter value.
6. The method of claim 1, wherein said session variable comprises a time stamp.
7. The method of claim 1, wherein said session variable comprises the output of a pseudo-random number generator.
8. The method of claim 5, wherein said counter value comprises an output of an incremental counter, said output being different for each session.
9. The method of claim 1, wherein said at least one parameter comprises an application identity associated with said application in communication with said user.
10. The method of claim 9, wherein said application identity comprises a wildcard application identity, said wildcard application identity being used when an application identity of said application in communication with the user is unknown to the user.

11. The method of claim 1, wherein said generating a derived identity based on said at least one parameter comprises applying a hash function to said at least one parameter.
12. The method of claim 1, wherein said generating a derived identity based on said at least one parameter comprises concatenating at least one of said at least one parameter with the output of a hash function applied to at least one of said at least one parameter.
13. A method for protecting user privacy during communications in a system having a key server, said method comprising:
  - receiving from a user a derived identity generated from a key and at least one parameter comprising a session variable;
  - transmitting said derived identity to said key server; and
  - receiving from said key server information associated with said user.
14. The method of claim 13, further comprising using said information to communicate with said user.
15. The method of claim 14, wherein said information associated with said user comprises a derived key, and said derived key is used to communicate with said user.
16. The method of claim 15, wherein said derived key received from said key server is generated based on at least one of said at least one parameter.
17. The method of claim 13, wherein said derived identity is generated from said at least one parameter by applying a hash function to said at least one parameter.
18. The method of claim 13, wherein said session variable comprises a counter value.
19. The method of claim 13, wherein said at least one parameter further comprises an application identity associated with an application requested by said user.

20. The method of claim 19, wherein said key server is configured not to provide said information if said application identity does not match an application identity associated with a requesting application.

21. The method of claim 13, further comprising:

agreeing with said user on information associated with a subsequent communications session with said user;

transmitting, to said key server, said information associated with said subsequent communications session;

receiving, from said key server, further information associated with said user; and

using said further information to communicate with said user during a subsequent communications session with said user.

22. A method for protecting user privacy comprising:

receiving, from a user, a derived key identity generated from a key and at least one parameter comprising a session variable; and

identifying said key from said derived key identity.

23. The method of claim 22, further comprising generating a derived key based on at least one of said at least one parameter, and engaging in encrypted communications with said user using said derived key.

24. The method of claim 22, wherein said session variable comprises a counter value that is incremented before or after engaging in a communications session.

25. The method of claim 24, further comprising:

agreeing with said user on information associated with a subsequent communications session with said user; and

using said information to communicate with said user during a subsequent communications session with said user.

26. A method for protecting user privacy during communications in a system having a key server, said method comprising:
- receiving from a requesting application a derived identity generated from a key and at least one parameter comprising a session variable; and
  - identifying said user from said derived identity.
27. The method of claim 26, further comprising transmitting information associated with said user to said requesting application.
28. The method of claim 27, wherein said information comprises a sub-key used for encrypting and decrypting data communicated between said requesting application and said user.
29. The method of claim 26, wherein said session variable comprises a counter value.
30. The method of claim 26, wherein said at least one parameter comprises an authorized application identity associated with an authorized application in communication with said user.
31. The method of claim 30, further comprising not transmitting said information associated with said user to said requesting application if said authorized application identity does not match said application identity of said requesting application.
32. An apparatus for protecting user privacy comprising:
- a derived identity generator for generating a derived identity associated with a user based on a key and at least one parameter comprising a session variable;
  - a transmitter for sending said derived identity to an application.
33. The apparatus of claim 32, further comprising a key generator for generating a key, wherein said apparatus communicates with said application using said generated key.
34. The apparatus of claim 32, wherein said apparatus communicates with the same application for at least two sessions.

35. The apparatus of claim 32, wherein said user communicates with a different application each session for at least two sessions.

36. An apparatus for protecting user privacy during communications in a system having a key server, said apparatus comprising:

- a receiver for receiving, from a user, a derived identity generated from a key and at least one parameter comprising a session variable; and

- a transmitter for transmitting said derived user identity to said key server.

37. The apparatus of claim 36, wherein the receiver is further configured to receive, from said key server, information associated with said user; and said information is used by said apparatus to communicate with said user.

38. An apparatus for protecting user privacy comprising:

- a receiver for receiving, from a user, a derived key identity generated from a key and at least one parameter comprising a session variable;

- a processor for identifying said key from said derived key identity.

39. The apparatus of claim 38, further comprising a generator for generating a derived key based on at least one of said at least one parameter, wherein said apparatus communicates with said user using said derived key.

40. An apparatus for protecting user privacy during communications in a system having a key server, said apparatus comprising:

- a receiver for receiving, from a requesting application, a derived identity associated with a user generated from a key and at least one parameter comprising a session variable; and

- a processor for identifying said user from said derived identity.

41. The apparatus of claim 40, further comprising a transmitter for transmitting information associated with said user to said requesting application.

42. An apparatus for protecting user privacy during communications with an application, said apparatus comprising:

- means for generating a derived identity;
- means for sending said derived identity to an application.

43. The apparatus of claim 42, further comprising means for generating a key, wherein said apparatus communicates with said application using said generated key.

44. An apparatus for protecting user privacy during communications in a system having a key server, said apparatus comprising:

- a receiver for receiving from a requesting application a derived identity generated from a key and at least one parameter comprising a session variable;
- means for identifying said user from said derived identity; and
- a transmitter for transmitting information associated with said user to said requesting application.