METHOD FOR SAFEGUARDING DATA TRANSMISSION BETWEEN A FIRST TERMINAL AND A FIRST NETWORK AND BETWEEN A SECOND TERMINAL AND A SECOND NETWORK

Description

Method for safeguarding data traffic between a first terminal and a first network and a second terminal and a second network.

The invention relates to a method for safeguarding data traffic between a first terminal and a first network and a second terminal and a second network. The invention also relates to a corresponding first and a corresponding second terminal, with which the claimed method can be implemented.

Users of mobile telephones today have to be able to access not just a mobile radio network but also further networks, e.g. the internet, via a suitable access network. In the case of internet access it is particularly desirable for the transmitted data to be displayed not on the mobile telephone but on a further terminal, e.g. a laptop.

Methods are known from the prior art, with which a first terminal in the form of a mobile telephone, containing a SIM or USIM module (SIM = Subscriber Identity Module; USIM = Universal Subscriber Identity Module), connects via a local interface to a second terminal in the form of a laptop, the laptop allowing access to a further network, e.g. a WLAN network and/or the internet. The second terminal is hereby authenticated to the further network via an authentication protocol, with keys being used in the protocol, which go back to the SIM or USIM module. Suitable authentication protocols that can be used are for example the following: EAP-SIM (EAP = Extensible Authentication Protocol; SIM = Subscriber Identity Module; see document [1]) or EAP-AKA (EAP = Extensible Authentication Protocol; AKA = Authentication Key Agreement;

see document [2]). The protocol EAP-SIM is hereby used for GSM mobile telephones and the protocol EAP-AKA is used for UMTS mobile telephones.

The authentication protocols EAP-SIM and EAP-AKA require both communication with the network and involvement of the SIM or USIM module in the authentication. This means that both the second terminal and the first terminal are involved in the execution of the authentication protocol. An exchange of data is therefore required between the second terminal and the first terminal via a local interface, e.g. a Bluetooth interface. Authentication data is thereby transmitted via this interface by means of a suitable profile for the purposes of authentication. Bluetooth profiles in particular, e.g. the Bluetooth SIM Access Profile (see document [3]), are known as suitable profiles from the prior art. First session keys, which are actually used for communication between the mobile telephone and the corresponding mobile radio network, are transmitted via the local interface. These first session keys are then used to calculate new session keys in the second terminal, with which new session keys the authentication operates via the authentication protocol. It can be problematic here for the first session keys to be known in the second terminal. This means that an attacker, who gains control of the second terminal, also has access to the first session keys and can impersonate the user of the first terminal, for example making calls at the user's expense in the first network.

The object of the invention is therefore to create a method for safeguarding data traffic between a first terminal and a first network and a second terminal and a second network that satisfies more stringent security requirements. The method is

intended in particular to protect against the attack described above.

This object is achieved by the independent claims. Developments of the invention are defined in the dependent claims.

With the claimed method a first terminal is used, which can communicate with the aid of one or more first session keys in a first network as is a second terminal, which can communicate with the aid of one or more second session keys in a second network. In the method the first terminal is connected to the second terminal via a local interface. The first session key(s) is/are determined in the first terminal and the second session key(s) is/are derived from the first session keys. The second session key(s) is/are transmitted via the local interface by means of a security protocol to the second terminal. The second terminal is finally authenticated to the second network via an authentication protocol with the aid of the second session key(s) and/or with the aid of keys derived from the second session key(s). The claimed method is based on the idea that the first session key(s) is/are not available to the second terminal. Therefore functions that are actually executed by the second terminal are moved to the first terminal. In particular the second session key(s) is/are derived from the first session keys in the first terminal. Therefore an attacker, who gains control of the second terminal, is no longer able to access the first session keys and cannot therefore access the first network.

In a preferred variant the authentication protocol is configured such that the keys derived from the second session key(s) are generated as part of the protocol and used to

protect the messages of the authentication protocol and/or to protect communication in the second network.

In one embodiment the first network is a GSM network and the first session key(s) is/are hereby generated in a SIM module on the first terminal. In this instance the authentication protocol is preferably the protocol EAP-SIM (EAP = Extensible Authentication Protocol; SIM = Subscriber Identity Module). In an alternative embodiment the first network is a UMTS network and the first session key(s) is/are generated in a USIM module (USIM = Universal Subscriber Identity Module) on the first terminal. In this instance the authentication protocol is preferably EAP-AKA (EAP = Extensible Authentication Protocol; AKA = Authentication Key Agreement).

The local interface between the first and second terminals is preferably configured via a wireless interface. A Bluetooth and/or infrared interface in particular is an option.

The second network, which communicates with the second terminal in the claimed method, is preferably a local network, in particular a LAN and/or WLAN network. The local network can in turn be connected to further networks, e.g. the internet.

In a further preferred variant of the invention the security protocol, with which information is exchanged between the first and second terminals, is configured as follows:
- a first signaling message from the second terminal is sent to the first terminal, the first signaling message initiating the derivation of the second session key(s) from the first session keys in the first terminal;
- in response to the first signaling message a second signaling message is sent from the first terminal to the

second terminal, with the second session key(s) being transmitted with the second signaling message.

The second session key(s) is/are hereby transmitted in a simple manner from the first terminal to the second terminal. In a preferred variant parameters from the authentication protocol are transmitted with the first signaling message. The security protocol is preferably an extended Bluetooth SIM Access Profile protocol, containing the first and second signaling messages. The precise specifications and requirements for such an extended protocol are defined in the special description.

In addition to the claimed data traffic safeguarding method, the invention also comprises a terminal, which is configured such that it can be used as the first terminal in the claimed method. The terminal hereby preferably comprises means for determining the first session key(s) and means for deriving the second session key(s) from the first session keys.

The invention also comprises a terminal, which is configured such that it can be used as the second terminal in the claimed method.

Exemplary embodiments of the invention are described in detail below with reference to the accompanying drawing, in which:

Figure 1 shows an example of a scenario, in which the claimed data traffic safeguarding method is used.

Figure 1 shows a first terminal in the form of a mobile telephone 1, which is connected via a local Bluetooth interface 3 to a second terminal 4 in the form of a laptop 4.

The second terminal 4 is in turn connected via a further wireless interface 5 to a second network 6, which is a WLAN network in Figure 1. An authentication protocol operates between the laptop 4 and the network 6 for authentication to the WLAN network. The WLAN network 6 is in turn connected to a further network 7, for example the internet. The mobile telephone 1 is also connected to a mobile radio network 2, for example a GSM or UMTS network, via an air interface. The mobile telephone is identified in the mobile radio network by means of an identity module, which is a SIM module in the case of GSM and a USIM module in the case of UMTS. One or more first session keys, which are generated in the identity module of the mobile telephone, are used to allow the mobile telephone to communicate with the mobile radio network. One or more second session keys are similarly used for communication between the laptop 4 and the WLAN network 6.

In the scenario in Figure 1 it is intended that a user of the mobile telephone should be able to authenticate themselves to the WLAN network via the laptop 4 with the aid of the first session keys generated in the identity module of the mobile telephone. The second session keys are derived from the first session keys for this purpose. An attack, in which the attacker gains control of the laptop 4, is a problem here, if the first session keys are transmitted via the Bluetooth interface 3 to the laptop 4 and derived in the laptop. In this instance the attacker would gain knowledge of the first session keys and could then impersonate the user in the mobile radio network 2. To prevent such attacks, according to the claimed data safeguarding method, the second session keys are not derived in the laptop 4 but in the mobile telephone 1 from the first session keys. The derived second session keys are then transmitted via the Bluetooth interface 3 by means of a

security protocol to the laptop, which uses these second session keys or further keys derived from the second session keys to carry out authentication to the WLAN network using the authentication protocol. The first session keys are therefore no longer stored in the laptop so that an attacker gaining control of the laptop is not able to set up a mobile radio connection using the first session keys.

The invention is described in detail below with reference to two exemplary embodiments. In the first exemplary embodiment the first terminal is a GSM mobile telephone with a SIM module and in the second exemplary embodiment it is a UMTS mobile telephone with a USIM module.

In the first exemplary embodiment the EAP-SIM protocol (see [1]) known from the prior art is used as the authentication protocol for authentication to the WLAN network. It is assumed that the SIM module of the mobile telephone is only involved in a so-called full authentication (see document [1], clause 3) and not a so-called re-authentication (see document [1], clause 4.3). The exact message flow of the authentication process is described in clause 3 of document [1] (see in particular Figure 1). The following steps are required for authentication:

The mobile telephone 1 receives from the laptop 4 the protocol identity (EAP-SIM), two or three GSM challenges RAND and the parameters "Identity", "NONCE_MT", "Version List" and "Selected Version". The parameters "Identity", "NONCE_MT", "Version List" and "Selected Version" are described in more detail in document [1]. The mobile telephone forwards each of the received RANDs one after the other to its SIM module. The

next RAND can only be forwarded to the SIM module, when the module has given its response to the previous RAND.

The following functions are executed for each RAND on the SIM module:
Execution of the GSM algorithms A3/A8, as described in [4], i.e. derivation of a response SRES and a GSM session key Kc. The parameters SRES and Kc are transferred from the SIM to the mobile telephone. Thus at the end of the communication with the SIM the mobile telephone has two or three responses SRES and two or three session keys Kc, depending on the number of RANDs received. The session keys Kc represent the first session keys as set out in the claims.

The mobile telephone then calculates the EAP-SIM master key MK - as described in [1], clause 4.6 - according to the following formula (MK hereby represents a second session key as set out in the claims):

$$MK = SHA1(Identity|n*Kc|NONCE_MT|Version\ List|Selected\ Version)$$

and sends MK and the responses SRES to the laptop.

In the above formula "|" means concatenation. Identity refers to the peer identity of the string without the zero characters at the end. It is the identity of the AT_IDENTITY attribute of the last EAP-Response/SIM/Start Packet or if no AT_IDENTITY was used, the identity of the EAP-Response/Identity Packet. The identity string is used without change and includes the possible identity decoration. The notation n*Kc refers to the n concatenated Kc values. The Kc keys are used in the same sequence as the RAND challenges in the AT_RAND attribute.

NONCE_MT refers to the NONCE_MT values (not the AT_NONCE_MT attribute, just the NONCE value). The "Version List" comprises 2-byte version numbers of the AT_VERSION_LIST in the same sequence as in the attribute. The "Selected Version" is a 2-byte version of AT_SELECTED_VERSION. The network byte order is used, just as in the attributes. The hash function SHA-1 is specified in [5]. If a number of EAP/SIM/Start Loops are used in an EAP/SIM exchange, the parameters NONCE_MT, "Version List" and "Selected Version" from the last EAP/SIM/Start Loop are used and the earlier EAP/SIM/Start Loops are ignored.

The laptop then calculates all further keys from MK, in particular so-called session keys. The laptop also carries out the check "verifies AT_MAC" shown in Figure 1 in clause 3 of document [1]. The key derivation for calculating MK from the session keys Kc is sufficient to prevent the laptop being able to draw conclusions relating to the session keys Kc.

An extended Bluetooth SIM Access Profile is used to transmit the parameters required to calculate the master key in the mobile telephone 1. The message "TRANSFER_APDU_REQ" used in the existing SIM Access Profile is extended to include the parameters "AuthProt", "EAP-Id", "NONCE_MAT", "Version List" and "Selected Version". Transmission of the EAP-Id is optional, if the mobile telephone can derive the EAP-Id from its own data. Two or three GSM challenges RAND also have to be transmitted. Transmission of these challenges is already considered in document [3].

The parameters used in the extended Bluetooth SIM Access Profile are described in more detail below:

Parameter: AuthProt

This parameter indicates the authentication protocol used.
Length: 1 byte
Parameter ID: to be defined by the Bluetooth Special Interest Group (SIG) (not essential to the invention)
Parameter values: EAP-SIM value = 0x01

Parameter: EAP-Id
This parameter contains the EAP identity of the user (permanent identity or pseudonym identity as set out in [1], clause 4.6) used to derive the master key.
Length: variable
Parameter ID: to be defined by the Bluetooth Special Interest Group (SIG) (not essential to the invention)
Parameter values: Suitable coding of EAP identity (coding is not essential to the invention)

Parameter: "NONCE_MT"
This parameter contains the NONCE_MT value of the EAP peer (as set out in [1], clause 4.6) used to derive the master key.
Length: 16 bytes
Parameter ID: to be defined by the Bluetooth Special Interest Group (SIG) (not essential to the invention)
Parameter values: Suitable coding of NONCE_MT (coding is not essential to the invention)

Parameter: "Version List"
This parameter contains the Version List (as set out in [1], clause 4.6) used to derive the master key.
Length: 2 bytes
Parameter ID: to be defined by the Bluetooth Special Interest Group (SIG) (not essential to the invention)
Parameter values: Suitable coding of Version List (coding is not essential to the invention)

Parameter: "Selected Version"
This parameter contains the Selected Version of the EAP peer (as set out in [1], clause 4.6) used to derive the master key.
Length: 2 bytes
Parameter ID: to be defined by the Bluetooth Special Interest Group (SIG) (not essential to the invention)
Parameter values: Suitable coding of Selected Version (coding is not essential to the invention)

The message "TRANSFER_APDU_RESP" is contained in the current specification of the SIM Access Profile (see [3], clause 5.2). This message should be extended to include the parameter "MK". Two or three GSM responses SRES also have to be transmitted. Transmission of the GSM responses is already considered in document [3].

Parameter: MK
This parameter contains the master key calculated in the mobile telephone according to [1], clause 4.6.
Length: 20 bytes
Parameter ID: to be defined by the Bluetooth Special Interest Group (SIG) (not essential to the invention)
Parameter values: Suitable coding of the master key MK (coding is not essential to the invention)

When using a UMTS mobile telephone the EAP-AKA protocol known from the prior art is used as the authentication protocol for authentication in the WLAN network 6 (see document [2]). Authentication here takes place as in [2], clause 3 (see the figure in particular). It is assumed that the USIM module and the mobile telephone are only involved in a full authentication (see document [2], clause 3) and not a re-

authentication (see [2], clause 4.2). The mobile telephone executes the following functions, the parameters below being described in more detail in document [2]:

The mobile telephone receives the protocol identity (EAP-AKA), the AKA challenge RAND|AUTN and the parameter "Identity" from the laptop and forwards RAND and AUTN to the USIM module. The parameter "Identity" here refers to the identity used by the user in EAP, as described in more detail in [2], clause 4.5.

The following functions are executed on the USIM:
Execution of the UMTS algorithms f1 to f5 and f5*, as described in [6], in particular verification of AUTN and MAC and derivation of the response RES and the AKA session keys CK and IK, which represent the first session keys as set out in the claims. The parameters RES, CK and IK are transferred from the USIM module to the mobile telephone.

The mobile telephone then calculates the EAP-AKA master key MK - as described in [2], clause 4.5 - according to the following formula (MK hereby represents a second session key as set out in the claims):

$$MK = SHA1(Identity|IK|CK)$$

and sends MK and RES to the laptop.

In the above formula "|" means concatenation. Identity refers to the peer identity string without the zero characters at the end. This identity is the identity of the AT_IDENTITY attribute of the last EAP-Response/AKA-Identity Packet or, if the AT_IDENTITY was not used, the identity of the EAP-

Response/Identity Packet. The identity string is used without change and only includes the possible identity decoration. The hash function SHA-1 is specified in [5].

The laptop then calculates all further keys from MK, in particular the session keys mentioned in clause 3 of [2]. The key derivation for calculating MK from CK and IK is sufficient to prevent the laptop being able to draw conclusions relating to CK and IK.

To transmit the parameters required to calculate the master key in the mobile telephone, an extended Bluetooth SIM Access protocol is used, with which the parameters are transmitted via the local Bluetooth interface. The parameters used in the extended Bluetooth SIM Access Profile are described in more detail below:

The message "TRANSFER_APDU_REQ" is contained in the current specification of the SIM Access Profile, see [3], clause 5.2. This message should be extended to include the parameters "AuthProt" and "EAP-Id". The transmission of EAP-Id is optional, if the mobile telephone can derive EAP-Id from its own data. The AKA challenge RAND|AUTN also has to be transmitted. Transmission of the AKA challenge is already considered in document [3].

Parameter: AuthProt
This parameter indicates the authentication protocol used.
Length: 1 byte
Parameter ID: to be defined by the Bluetooth Special Interest Group (SIG) (not essential to the invention)
Parameter values: EAP-AKA: value = 0x00

Bibliography

[1] H. Haverinen, J. Salowey "EAP SIM Authentication", internet draft, draft-haverinen-pppext-eap-sim-12, October 2003; http://www.ietf.org/internet-drafts/draft-haverinen-pppext-eap-sim-12.txt

[2] J. Arkko, H. Haverinen, "EAP AKA Authentication", internet draft, draft-arkko-pppext-eap-aka-11, October 2003; http://www.ietf.org/internet-drafts/draft-arkko-pppext-eap-sim-11.txt

[3] "SIM access via 'SIM Access Profile' and Bluetooth link", contribution S3-030436 to the 3GPP meeting SA3#29, San Francisco, 15-18 July 2003; ftp://ftp.3gpp.org/TSG_SA/WG3_Security/TSGS3_29_SanFran/Docs/ZIP/S3-030436.zip; revised text of version 0.95VD_d, attachment att2

[4] GSM Technical Specification GSM 03.20 (ETSI TS 100 929): "Digital cellular telecommunication system (Phase 2+); Security related network functions", European Telecommunications Standards Institute, July 1999

[5] Federal Information Processing Standard (FIPS) Publication 180-1, "Secure Hash Standard", National Institute of Standards and Technology, US Department of Commerce, April 17, 1995

[6] 3GPP Technical Specification 3GPP TS 33.102 V5.3.0: "Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (release 5)", 3rd Generation Partnership Project, September 2003; ftp://ftp.3gpp.org/Specs/latest/Rel-5/33_series/

Claims

1. Method for safeguarding data traffic between a first terminal (1) and a first network (2) and a second terminal (4) and a second network (6), with the first terminal (1) being able to communicate with the aid of one or more first session keys in a first network (2) and the second terminal (4) being able to communicate with the aid of one or more second session keys in a second network (6),
characterized by the following steps:
- the first terminal (1) is connected to the second terminal (4) via a local interface (3);
- the first session key(s) is/are determined in the first terminal (1) and the second session key(s) is/are derived from the first session keys;
- the second session key(s) is/are transmitted via the local interface (3) by means of a security protocol to the second terminal (4);
- the second terminal (4) is authenticated to the second network (6) by means of an authentication protocol with the aid of the second session key(s) and/or with the aid of keys derived from the second session key(s).

2. Method according to claim 1, in which the keys derived from the second session key(s) are generated as part of the authentication protocol and used to protect the messages of the authentication protocol and/or to protect communication in the second network.

3. Method according to claim 1 or 2, in which the first network (2) is a GSM network and the first session key(s) is/are generated in a SIM (SIM = Subscriber Identity Module)

with the second signaling message.

10. Method according to one of the preceding claims, in which parameters from the authentication protocol are transmitted with the first signaling message.

11. Method according to claim 9 or 10, in which the security protocol is an extended Bluetooth SIM Access Profile protocol, containing the first and second signaling messages.

12. Terminal, configured such that it can be used as the first terminal (1) in the method according to one of the preceding claims.

13. Terminal according to claim 12, the terminal having means to determine the first session key(s) and means for deriving the second session key(s) from the first session keys.

14. Terminal, configured such that it can be used as the second terminal in the method according to one of claims 1 to 11.