Title: A METHOD AND DEVICE FOR AUTHENTICATING USERS

Abstract: This invention relates to authenticating users towards Internet services, using their SIM card as an authentication token, and reusing the existing authentication infrastructure of GSM networks. The method allows the authentication of subscribers from different GSM operators through a centralized authentication point towards their home network.
For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
A METHOD AND DEVICE FOR AUTHENTICATING USERS

Field of the invention

The present invention relates to the use of Internet services, and in particular an improved method for authenticating users when logging in to Internet services.

Technical Background

The main problem area

Figure 1 illustrates the primary problem area. A user accesses several services provided by different service providers through different terminals (e.g. a cellular phone, a PDA, a laptop computer or a stationary PC). However, the user is required to authenticate himself towards most services, i.e., to provide proofs that he really is who he claims to be.

For most Internet services today, the user must create a user account, and select a username and password, which are later used to authenticate him.

Known solutions

Username/password based Authentication

Username/password based authentication is the most common method in the Internet today and is used in services like:

Web shops

Web mail

Member sites/discussion forums

Etc.

PKI Authentication

Public Key Infrastructure (PKI) [1] relies on a pair of keys for each user; a public and a private key. The public key can be freely distributed to anyone, whereas the private key must be kept secret by the owner. To use PKI for authentication, the distribution of keys
is crucial. It must be ensured that nobody else than the rightful owner has the private key, and it must also be ensured that the public key is distributed correctly, i.e., that the ones that receive the public key really gets the key of the person they believe to get the key of (and not an imposter).

OTP Authentication

One-Time Password (OTP) authentication is a solution where the system guarantees a new password on every authentication. There are several possible solutions for OTP, but the system usually relies on a hash algorithm which is used to calculate a response based on a challenge provided by an OTP server. This way, it doesn’t help an attacker to steal the OTP response in transit, since the challenge is different each time.

Mostly used by Internet banking services

Smart Card Authentication

Smart Card authentication can be based on both PKI and OTP. The strength is increased by introducing a physical token.

Used by e.g. Norsk Tipping for online betting

Used for company authentication to VPN, etc.

Problems with known solutions

Strength

The username/password solution can be sufficient for many types of services, but there are several problems with it:

Users tend to use the same username/password combination for several accounts with different service providers

Users tend to choose simple usernames and passwords, which are easy to remember. These are then easy to guess by potential attackers

Users often write down usernames and passwords; most people cannot remember an unlimited amount of username/password combinations
Usernames/passwords are often sent in cleartext, which can then be intercepted by an eavesdropper and used in replay attacks.

**Deployment and Administrative Issues**

Common to the solutions discussed above is the deployment and administrative issues. Each of these solutions requires that the user obtains an artifact which is used to authenticate the user, e.g. public/private keys, certificates, OTP calculator and/or Smart Card with Smart Card reader.

**Brief summary of the invention**

This invention alleviates all the challenges with known authentication solutions discussed above.

The scope of the invention appears from the appended claims.

**Description of the drawings**

The invention will now be described in detail with reference to the appended drawings, in which:

- Fig. 1 is a schematic diagram showing a user accessing several services on the Internet,
- Fig. 2 is a diagram showing the overall architecture of the inventive system,
- Fig. 3 is a sequence diagram illustrating an authentication process according to the present invention

**Detailed description of the invention**

This invention relates to authenticating users towards Internet services, using their SIM card as an authentication token, and reusing the existing authentication infrastructure of GSM networks. The innovation lies in the method that allows the authentication of subscribers from different GSM operators through a centralized authentication point towards their home network, thus maximizing the potential user base of the authentication service, which is crucial for the adoption of the authentication service by service providers.
This invention enables strong authentication of users for Internet services using the GSM [2] authentication mechanism, and it can be used for users having subscription at different GSM operators. More specifically, it allows a user that wants to access Internet services from a terminal (such as a cellular phone, PDA, laptop PC or stationary PC), to authenticate using a cellular phone (or another SIM reader) to authenticate towards his home GSM operator, no matter where in the world the user is currently located. For example, when travelling and surfing the Web on an Internet café, it will still be possible for a user to authenticate towards services using his cellular phone, even if there is no GSM network coverage in the current location. The authentication will proceed all the way towards the Home Location Register (HLR) of the home GSM operator. This is solved by a mobile network gateway which acts as a Visitor Location Register (VLR), and forwards, based on the user identity, IMSI (International Mobile Subscriber Identity) authentication requests towards the appropriate HLR.

The system components

Cellular phone

Since GSM phones already include a SIM (Subscriber Identity Module) card, such a terminal can be used in the authentication process. Services can either be delivered directly to the cellular phone, or the cellular phone can be used to authenticate services accessed through a second terminal. The second terminal will then communicate further towards the authentication mechanisms implemented as a distributed function in the Internet.

SIM Reader

An option to using the cellular phone directly, it is possible to embed a SIM card in a specialised Smart Card reader, i.e., a SIM reader, connected to the terminal either using USB or PCCARD. It is also possible to use a 3G PCMCIA datacard, which already embeds a SIM, in the authentication process.

Terminal

Services may be accessed either through the cellular phone, or a through a second terminal. The terminal is a device with an Internet connection (wired or wireless), and it can be either a cellular phone, PDA, laptop PC or stationary PC or any other terminal with such connection.
Authenticator

The Authenticator has service level agreement with Service Providers, and may be responsible for carrying out the authentication procedure on behalf of the users and the service providers (the authentication process may be outsourced to the Authenticator). The Authenticator can communicate with the MAP GW, which again communicates towards the GSM operators.

Service Provider

A service provider is an entity that can provide services, and which requires the users to authenticate prior to access to these services.

Mobile network gateway

This component can receive authentication requests and forward them to any HLR, as long as a roaming agreement for authentication exists. The component supports the EAP-SIM/EAP-AKA over RADIUS protocol on one side and SS7 up to the MTP3 layer on the other side. The mobile network gateway may be a combined RADIUS server/MAP gateway.

HLR

This is a standard GSM Home Location Register, which in turn is connected to an Authentication Centre (AuC).

The authentication process

Figure 3 shows the authentication process. Some message exchanges are left out for clarity. Messages 4, 5, 8, 9, 12, 13, 14 and 15 are embedded in the EAP-SIM protocol. Messages 5, 8, 13 and 14 can in addition be embedded in the RADIUS protocol, but this is optional. The message exchanges in the process are detailed below:

\textit{invokeService()}: UserA tries to access a service using a terminal, which can be a cellular phone, PDA, laptop PC, stationary PC, etc.

\textit{invokeService()}: Software on the terminal requests a service from a service provider (e.g. through a WWW browser)
authenticate(): The service provider requires the user to authenticate himself before providing the requested service and send the authentication request to the authenticator

getIMSI(): The Authenticator communicates with a software component on the terminal which again communicates with the SIM card to get the user identity (IMSI)

authRequest(IMSI): The Authenticator requests authentication from a RADIUS server/MAP gateway.

authRequest(IMSI): Using the IMSI which contains the operator code, the RADIUS server/MAP gateway deducts the correct HLR and route the authentication request to the correct HLR. The operator code usually consists of IMSI digits 4-5 (in Europe) or IMSI digits 4-6 (in North America).

authRequestResponse(TRIPLET): The HLR responds with triplets (RAND, XRES, Kc)

authRequestResponse(RAND): The RADIUS/MAP GW responds to the Authenticator with the random challenge from a triplet.

authRequestResponse(RAND): The Authenticator responds to the software component on the terminal with the random challenge.

runA3(RAND): The terminal initiates the A3 algorithm on the SIM card, using the random challenge as input (the A3 algorithm also uses a secret key, Ki stored on the SIM)

runA3Response(SRES): The SIM responds with a signed response (SRES = A3(RAND, Ki))

authRequest(SRES): Software on the terminal returns the signed response, received from the SIM, to the Authenticator

authRequest(SRES): The Authenticator returns the signed response to the RADIUS server

authRequestResponse(Success): The RADIUS indicates whether authentication was successful or not to the Authenticator
authRequestResponse(AuthenticationToken): If authentication was successful, the Authenticator returns a token to the software on the terminal as a confirmation of the authentication

invokeService(AuthenticationToken): The software on the terminal (e.g. WWW browser) re-invokes the service, and provides the authentication token as a proof of the successful authentication

provideService(): By verifying the authentication token, the service provider provides the originally requested service to the terminal software

18. provideService(): Finally, the software on the terminal will provide the user with the requested service

This invention alleviates all the challenges with known authentication solutions discussed in the introduction. In particular:

The invention supports strong authentication of users who subscribe to different GSM operators. This means that a large number of users will be able to use the simplified, strong authentication towards Internet services

The invention provides strong authentication to Internet services

There are no additional administrative or deployment issues; the users already have a SIM card and a subscription at the GSM operator

However, while the invention has been described in relation to Internet services, it may as well find applications in any network where users want to gain access to a service. The invention is in fact applicable in all circumstances where a user is asked to identify himself. Large service providers may also possess their own Authenticator servers or services. The invention is neither limited to GSM networks, as corresponding functionality for authentication is present in other mobile networks as well.
Claims

1. A method for authenticating a user attempting to access a service on an IP based network, said service being provided by a service provider, the method being characterized in:
retrieving an International Mobile Service Identity for the user from a SIM card possessed by the user,
deducting which mobile network Home Location Register the user belongs to from said identity information,
sending an authentication request to said Home Location Register,
receiving authentication data from the Home Location Register,
performing authentication towards the SIM card obtaining an authentication result,
providing said authentication result to the service provider with a request of access to the service.

2. A method as claimed in claim 1, wherein the Home Location Register responding to the authentication request with a random challenge,
processing said random challenge using said SIM card, The SIM card providing a response,
controlling the correctness of the response in order to obtain said authentication result.

3. A method as claimed in claim 1, wherein the method is initiated by a user terminal sending a service request to the service provider,
the service provider sending an authentication request to an Authenticator server,
said step of retrieving the International Mobile Service Identity including the Authenticator server retrieving said International Mobile Service Identity of the user from said SIM card and providing said International Mobile Service Identity to a mobile network gateway,
said step of deducting which mobile network Home Location register the user belongs to including the mobile network gateway deducting the Home Location Register of the user from said International Mobile Service Identity,
said step of providing authentication data including the mobile network gateway sending the random challenge message to the Authenticator server,
the Authenticator server sending the random challenge message to the user terminal,
said step of performing authentication including processing said message by the user terminal initiating an A3 algorithm on the SIM card using the random challenge message as input,
The user terminal returning the response from the SIM card to the Authenticator server,
the Authenticator server sending the response to the mobile network gateway,
the mobile network gateway controlling the response and indicating whether the
authentication was successful or not to the Authenticator server,
if the authentication was successful, the Authenticator server providing an
authentication token to the user terminal,
said step of providing said result to the service provider including the user terminal re-
invoking the service providing said authentication token as a proof of successful
authentication.

4. A method as claimed in claim 3, wherein said mobile network gateway
being a RADIUS server/MAP gateway.

5. A method as claimed in claim 4, wherein said RADIUS server/MAP
gateway has an interface to a Signalling number 7 network.

6. A method as claimed in claim 1, wherein the identity information is
retrieved from a SIM card enclosed either in a SIM enabled device embedded in the
terminal, or in a SIM card reader or a cellular phone connected with said user terminal.

7. A method as claimed in claim 4, wherein the RADIUS server/MAP
gateway supports EAP-AKA over RADIUS protocol on one side and Signalling number
7 protocol from MTP1 layer to MTP3 layer on another side.

8. A method as claimed in claim 3, wherein said user terminal is a cellular
phone, or a PDA, or a laptop PC, or a stationary PC.

9. A device for authenticating a user attempting to access one or more
services on an IP based network, said service(s) being provided by at least one service
provider,
characterized in that said device is connected to said at least one service
provider, and being adapted to receive authentication requests from said service
provider(s), said authentication requests relating to users using user terminals and
requesting services from said service provider(s),
said device being connected to said user terminals and being adapted to retrieve user
identification data from SIM cards in or connected to said user terminals, and
said device being connected to at least one mobile network gateway and being adapted
to provide said user identification data to said gateway and receive user authentication
services from said gateway.
10. A device as claimed in claim 9, wherein said mobile network gateway is a RADIUS server/MAP gateway.
Figure 1

Figure 2