Strong authentication with mobile phone as security token

Do van Thanh – Telenor & NTNU, Norway – thanh-van.do@telenor.com
Ivar Jørstad – Ubisafe, Norway – ivar@ubisafe.no
Tore Jønvik – Oslo University College, Norway – tore.jonvik@iu.hio.no
Do van Thuan – Linus, Norway – t.do@linus.no

Abstract – **The protection of digital identities is getting more and more crucial. The usage of passwords for authentication is no longer sufficient and stronger authentication schemes are necessary. Strong authentication solutions using two identification factors require often an additional device, which could be inconvenient for the user and costly for the service providers. To avoid the usage of additional device, the mobile phone is adopted as security token. This paper provides a study of the various ways the mobile phone can be used as an authentication token towards service providers on the Internet. It starts with discussing the need for a strong authentication scheme, and the motivation for using the mobile phone to improve on several aspects of the current authentication processes. Thereafter, the general architecture for authentication with mobile phones is presented. Several different authentication solutions using the mobile phone as authentication token are then described, where the solutions vary in complexity, strength and user-friendliness. The paper ends with an evaluation of the different solutions, and a discussion of the most probable attacks. A classification of the solutions is also provided, according to defined criteria.**

Keywords: Strong authentication, Two-factor authentication, Multi-factor authentication, Security token, Identity theft, Identity Management, User identification

I. INTRODUCTION

As the popularity of the Internet increases the number of frauds and abuses is literally exploding. Most serious is the theft of identity which causes grave damages both for the victim and also his entourage such as employee, banks, hobby clubs, etc. The protection of digital identities is getting more and more crucial. The usage of passwords for authentication is not longer sufficient and stronger authentication schemes are necessary. Strong authentication solutions require often two identification factors i.e. in addition to the first factor "something you know" represented by passwords it is introduced a second factor "something you have" materialized by a security token. The introduction of the additional device could be costly for the service providers in terms of deployment and administration at the same time as it could be inconvenient for mobile users. Furthermore, there is very little re-use or sharing such that the same security token can be used for several systems. To remedy the situation, there are proposed several authentication solutions that avoid introducing extra device by re-using existing devices, namely the mobile phone or the SIM cards.

This paper presents a study of the strong authentication solutions using mobile phone as security token adopted by the EUREKA Mobicome[1] project, which is aiming at providing a unified subscription plan for a Fixed-Mobile Convergent IMS environment.

The paper starts with a clarification of the notion of strong authentication in section II. The architecture of the Strong authentication solutions using mobile phone is given III. The Strong authentication solutions are successively described in the sections IV, V, VI and VII. Section VIII provides an evaluation of the different solutions.

II. STRONG AUTHENTICATION

There is no clear and unanimous definition of strong authentication. According to Fermi Lab [1], Strong authentication is a form of computer security in which the identities of networked users, clients and servers are verified without transmitting passwords over the network. The U.S. National Institute of Standards and Technology (NIST) defines four levels of authentication [2] as follows:

- **Level 1:** No identity proof
- **Level 2:** Single factor remote network authentication
- **Level 3:** Multi-factor remote network authentication

[1] The EUREKA Mobicome project (Nov 2007-april 2010) has as partners: Telenor. Telefonica, HuaWei, Ericsson, Polytechnical University of Madrid, Oslo University College, Blekinge Institute of Technology, Linus, Ubisafe and WIP.

978-1-4244-5113-5/09/$25.00 ©2009 IEEE

- **Level 4:** Proof of possession of a key through a cryptographic protocol

It is not specified which authentication level can be considered as strong but level 3 with multi-factor authentication is definitely considered a strong authentication. It is also clear that strong authentication does not have to be multi-factor. According to [3] strong authentication can start with two-factor authentication which combines two of the following authentication options:

- **Something you know:**
  - Passwords
  - Knowledge-Based Authentication (KBA)
- **Something you have:**
  - One-time password tokens
  - Digital certificates
  - Grid cards
- **Something you are:**
  - Biometrics
- **Something known about you:**
  - Risk-based authentication
  - Device ID

Most of two-factor authentication solutions combine "something you know" and "something you have". They require the usage of an additional device, which demands administration from the service provider and extra care from the user.

III. ARCHITECTURE OF STRONG AUTHENTICATION USING MOBILE PHONE

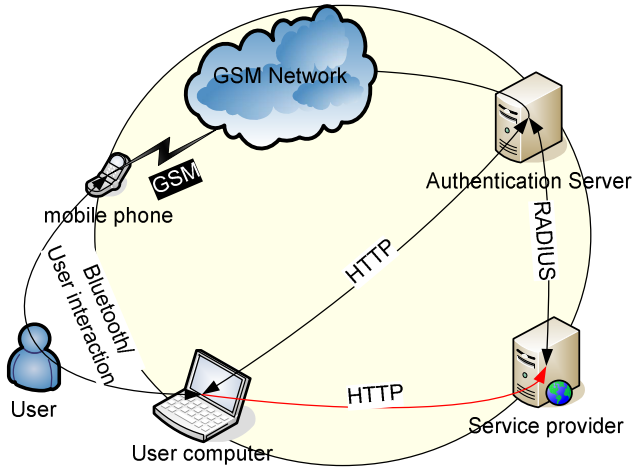

Figure 1 Architecture of the Strong Authentication using mobile phone

As shown Figure 1 the user must have access to a computer connected to the Internet and be in possession of a mobile phone with an operating SIM card. If the computer and mobile phone is equipped with Bluetooth higher usability can be obtained. Through the Internet browser on the computer the user can access web services provided by service providers. The service provider (SP) is connected to an Authentication Server (AS) that will handle the authentication on behalf of the SP. The AS is connected to the GSM network which enables it to communicate with the user's mobile phone and the operators Authentication Center (AuC). The AS is composed of two parts, an authenticator and an AAA (Authentication, Authorization and Accounting) server. The authenticator communicates with the client and relays messages to the AAA server which handles the authentication.

In an authentication scheme which uses two separate devices that communicate over two different networks it is very important to ensure that it is the same user that controls both devices. This is done by ensuring that there is a "closed loop" going through all the components involved in the authentication as illustrated in Figure 1. The loop starts in the device requesting the service, the users computer, goes through the network with SP and AS and then via the mobile phone and back to the initial device either by user interaction or Bluetooth.

This closed loop can be realized in several ways as described in the solutions presented in the coming sections.

IV. SMS AUTHENTICATION WITH SESSION-ID VERIFICATION

This solution exploits that a user with a valid mobile subscription is already authenticated through the GSM system. Session Ids are used to ensure that it is the same user that controls both the computer and mobile phone.

When the user accesses a service provider a unique session ID is created and sent both to the user's computer and mobile phone. The session ID is sent over the Internet to the computer and shown in the web browser and sent to the phone by SMS. Then the user can confirm that the session IDs match and send a confirmation by a Short Message Service (SMS) [4] to the service provider. When receiving the confirmation from the user the AS knows that the user is in possession of the phone and the authentication is successful.

The comparison of the session ID can be made by the user or automatically by software if the phone is connected to the computer by Bluetooth.

V. ONE-TIME PASSWORD FROM PC TO SMS

When the client wants to access the SP the client's identity is requested. The client responds by typing his username in the browser. The message is relayed to the AS which handles the authentication. Upon receiving the client's identity the AS generates a challenge, typically a random number based on the client's profile, and a corresponding

One-Time Password (OTP) [5] [6]. Then the AS sends the challenge to the client. The client enters the challenge on the mobile phone. The OTP applet on the SIM card [7] generates an OTP from the challenge. The OTP is then sent to the AS by SMS. The AS compares the calculated and received OTP and notifies the authenticator that the client is authenticated. The browser is redirected back to the SP and the user is successfully logged in.

In the manual variant, when the client receives the challenge from the AS it is displayed in the browser. The user starts a MIDlet on the phone can communicate with the SIM card through SATSA-APDU [8]. The user is prompted for the challenge and enters it on the phone. The MIDlet transfers the challenge to the OTP applet which responds with an OTP. The user creates an SMS containing the OTP and sends it to the AS.

In the automatic variant, the mobile phone and computer are connected through Bluetooth and the challenge can be sent to the phone automatically.

VI. ONE-TIME PASSWORD FROM SMS TO PC

This solution builds on the same principle as the session ID check, that a user with a working phone is already authenticated through the GSM network. The difference is that the check is done by the server and therefore relieves the user from this burden.

The user starts the authentication procedure by entering his username. The session is redirected to the AS which creates an OTP based on the users identity by a cryptographic hash function. The OTP is then sent to the user by SMS. When receiving the SMS the user types the OTP in the browser. The AS verifies that the OTP is correct and redirects the browser back to the service provider and the user is logged in.

If the mobile phone and the computer are paired through Bluetooth the OTP can be transferred automatically from the phone to the computer and then forwarded to the AS through the browser. This can be handled by a Java applet on the computer communicating with the SIM card through SAP. When the AS has sent the OTP by SMS it notifies the client that this has been done. When receiving this notification the Java application contacts the mobile phone and retrieves the SMS from the AS. The applet retrieves the OTP from the SMS and sends it to the AS through the Internet browser. As in the session ID solution the TP-PID field in the SMS header must be set to “SIM DATA DOWNLOAD” so the SMS is guaranteed to be stored on the SIM card.

IVII. SIM STRONG AUTHENTICATION VIA MOBILE PHONE

This solution makes use of the EAP-SIM protocol [9] [10] to authenticate the user. EAP-SIM is run between the SIM and the AS. The protocol can be run through the computer over Bluetooth and Internet or over the GSM network by SMS.

When the user accesses a Service Provider the browser is redirected to an AS. If the user chooses to run the SIM strong authentication the rest of the procedure is hidden for the user as the SIM card and the AS authenticate each other. If the authentication is successful the browser is redirected back to the SP and the user is logged in [13].

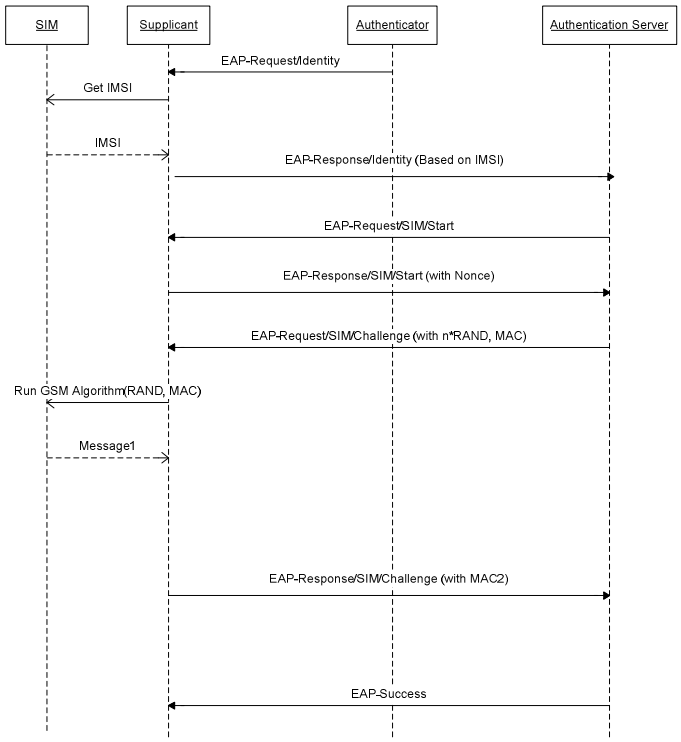

Figure 2 EAP SIM authentication

In order to be able to run the EAP-SIM protocol between the AS and the client the AS needs to communicate with the SIM card. To avoid having to install specific software on the client’s computer this communication is handled by a Java applet [11].

The applet will play the role as supplicant and run in the client’s browser and relay messages between the authenticator and the SIM card

Its main functions will be to:

1. Receive EAP request from the EAP authenticator
2. Send the contest of the these packets to the SIM card
3. Build EAP response packets from the SIM responses
4. Send the EAP response packets to the EAP authenticator.

The applet communicates with the SIM card using Bluetooth SIM Access Protocol (SAP) [12]. The EAP authenticator is implemented as a Java Servlet running inside the AS. The authenticator first request an EAP identity from the supplicant. The supplicant translates this request and relays it to the SIM card. The SIM card responds with the international mobile subscriber identity (IMSI). The authenticator sends the identity received to the AAA server which contacts the user's AuC for GSM triplets. The challenges contained in the triplets are concatenated and sent back to the supplicant. The supplicant relays the challenges to the SIM card that:

1. Authenticates the server by verifying that the MAC1 received is in order
2. Runs the GSM algorithms to calculate a MAC2 that is sent back to the AS

The supplicant receives the response from the SIM and sends them to the authenticator in EAP format. The authenticator relays the response to the AAA server that verifies that the MAC2 is correct. If MAC2 is correct the authentication is successful and the user is logged in. The EAP-SIM authentication is shown in Figure 2.

The SMS variant

This solution is a variant that does not require a Bluetooth enabled mobile phone. Instead the EAP-SIM protocol will run over SMS.

The user chooses to log in using the EAP over SMS solution. When this is done, a web page is presented asking for a session ID. An authentication applet on the SIM card is started by the AS through SAT and the user is asked to confirm that he wants to start the authentication. A session ID is displayed on the mobile phone screen and the user enters the session ID in the browser. If the session ID is correct the user must accept to start authentication by pressing an OK button on the phone. Then EAP-SIM authentication is performed between the SIM card and the AAA server by exchanging SMS messages. If the authentication is successful, the SP is notified that the user with the corresponding session ID is authenticated, and the user is provided access to the protected resources.

To enable the phone to perform EAP authentication over SMS an applet on the SIM card must be installed. The applet generates the session ID to be entered in the browser. Thereafter, the SIM applet performs authentication towards GSM using SMS messages which encapsulate the EAP-SIM protocol. This solution is similar to the previous, however it does not require the Bluetooth connection between the mobile phone and the user's PC since it instead uses SMS to close the authentication loop. SAP is used to control the SIM card and mobile phone during authentication.

The implementation can be optimized so that only two mobile-originated short messages and one server-originated short message are required for full EAP-SIM authentication.

VIII. EVALUATION OF THE AUTHENTICATION SOLUTIONS

The evaluation is performed according to the following criteria:

- Strength & vulnerabilities
- Cost
- User friendliness

As illustrated in Figure 3, the different authentication solutions have the vulnerability points which can be subject to attacks in as follows:

1. On the mobile phone
2. Across the Bluetooth connection
3. On the computer
4. Across the Internet connection
5. Across the connection between service provider and authentication server
6. On and between GSM network components and connections

The following sections will discuss some of the most probable attacks on the different mobile authentication solutions.

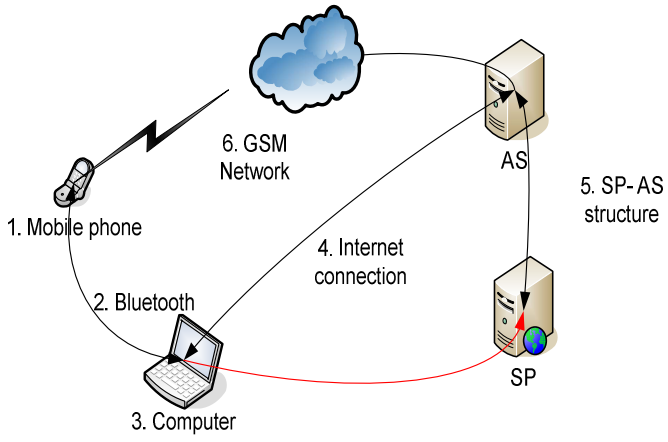

Figure 3 Vulnerability points of the authentication solutions

A. Session-ID check with SMS

With regards to Figure 3, this solution is realistically most susceptible to an attack in the response phase, i.e. when the user sends an acknowledgement back to the AS through the GSM network. Consider a possible hijacker which has as goal to steal a session from a valid user. If the hijacker establishes a session towards a service at the same time as the valid user, using the valid user's identity (i.e., cellular phone number), two messages with session-ids will be sent to the valid user. Being unaware of the hijack attempt, the valid user might respond with acceptance to the invalid user's request, instead of to the valid user's request.

However, such an attempt requires a hijacker to be familiar with the valid user's identity as well as being well synchronised with the valid user's activity (e.g. through visual observation). The likeliness of a successful such hijack attempt is therefore in practice extremely low, since it also assumes that the user does not properly study each of the incoming SMS messages with session-ids. Another problem with the solution is that it is technically possible to spoof SMS sender addresses, i.e., send SMS-messages with the valid user's number. Additional security mechanisms should be applied to prevent this.

B. OTP PC-to-SMS

In this solution, it is the OTP which is the most crucial element. If an eavesdropper can get hold of the OTP, he could in theory hijack a user session. However, since a user's session (and OTP) is associated with a specific challenge, it is not enough to get hold of the OTP, it is also necessary to hijack the HTTP-session which has previously been created by the valid user. The solution could also in addition to the OTP, include a check of the sender address of the SMS carrying the OTP, to further improve the strength and reduce the possibility of malicious attacks.

The automatic variant of the OTP-solution mostly improves the user-friendliness. However, it also reduces the possibility of attacks due to a strong association between the user's phone and computer through an authenticated and encrypted Bluetooth connection. Attacks towards this solution could be launched on the Bluetooth-connection, but this is not trivial

C. OTP SMS-to-PC

Since the OTP in this solution is sent to the user, attacks must be directed towards obtaining the OTP. However, the OTP is typically associated with an HTTP-session created by the valid user. Therefore, both the OTP as well as the HTTP-session must be attacked in order for a malicious user to get access to the valid user's services.

This solution simplifies the work for the user, and prevents eavesdroppers to visually get hold of the OTP which is received by the valid user's mobile phone. The OTP is never actually exposed to the user, but handled only by the system components.

D. SIM Strong Authentication

The SIM strong authentication solution can be used both with the SIM-card in the mobile phone, but also with the SIM-card in a USB-dongle or similar. The two different solutions differ in some of properties.

D.1 SIM in mobile phone

From a user's perspective, this is the most ideal solution, since no additional device is required to perform authentication. Regarding the security properties, this solution requires a wireless Bluetooth connection between the phone and the user's computer, which in theory could be compromised, but as previously discussed, this is in reality unfeasible. The biggest security risk with the solution is loss of terminal, but the SIM is also protected by a PIN-code, which renders the device useless when unknown. The PIN-code must be used to activate the SIM when the phone is switched on, but in addition, the solution can require the user to also enter the PIN-code each time an authentication should be performed, further strengthening the solution in case of loss of mobile phone.

D.2 SIM in USB-dongle

This solution is slightly less user friendly than the previous due to the need of an additional device, and in theory a bit more secure since it requires a physical connection between the user's computer and the SIM-card. This solution also requires a PIN-code for activation of the SIM-card prior to authentication, which prevents use by arbitrary users if the dongle with SIM is lost.

D.3 SIM strong authentication with SMS

This solution combines the strength of SIM strong authentication with the session-id check, and the result is a relatively strong authentication solution. However, it requires the installation of a special applet on the user's SIM-card. The solution also requires a check of session-id, and could also possibly include the PIN-verification procedure to provide further protection in case of loss of mobile phone.

All the SIM strong authentication solutions above are based on well-proven, standardised technologies and protocols where the strength and weaknesses have been scrutinized by computer and communication network security experts.
The solutions are rated with relative weights from 1 to 6 where 6 is the best rating.

E. Comparison of authentication solutions

Table 1 illustrates some of the security properties of the major categories of authentication solutions discussed in this paper. It shows what type of attacks the different solutions can be susceptible to.

Security requirement	Session ID	OTP solutions	SIM strong solutions
Online guessing	n/a	√	n/a
Replay	√	√	√
Eavesdropping		√	√
Shared secrets not revealed	n/a	√	√
Man-in-the-middle			√
Session hijacking			√
Authenticated data transfer			√

Table 1 Security properties

Figure 4 shows a comparison of the different authentication solutions with respect to four parameters; security, cost, infrastructure and user-friendliness. The comparison is informal and only meant to provide some insight into the properties of the various solutions in relation to each other. As with all such solutions, the actual implementations might have other properties than illustrated here. The scores are relative from 1 to 10, where 10 is the best rating. High rating in e.g. cost and infrastructure does not mean high cost nor much infrastructure but rather the opposite.

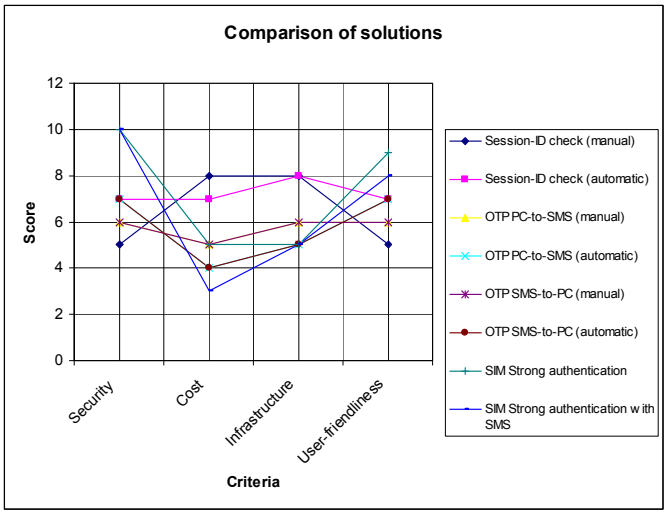

Figure 4 Comparison of the different authentication solutions based on mobile phone

IX. CONCLUSION

This paper has suggested several ways to employ the mobile phone as an authentication token, with the purpose to address shortcomings of existing authentication solutions on the Internet today. The solutions show that there are many different possibilities, and that the authentication process can take one single path back and forth, or exploit several communication channels to complete the authentication. The paper also informally illustrated the security properties of the solutions and provided a comparison between the solutions with respect to four important criteria. As further work, the proposed authentication solutions should be implemented and user trials should be carried out to verify their usability.

REFERENCES

[1] Fermi National Accelerator Laboratory, Office of Science / U.S. Department of Energy: Strong Authentication at Fermilab, Sept 2006

[2] National Institute of Standards and Technology (NIST) U.S. Department of Commerce: Electronic Authentication Guideline - Information Security, Special Publication 800-63-1, December 8, 2008

[3] CA: Managing Strong Authentication: A Guide to Creating an Effective Management System, 2007

[4] 3GPP, 3GPP TS 23.040, Technical realization of the Short Message Service. 2003

[5] OATH, "An industry roadmap for Open Strong Authentication", 2006, available online: http://www.openauthentication.org/

[6] N. Haller, C.M., P. Nesser, M. Straw, RFC 2289 A One-Time Password System. 1989.

[7] ETSI, GSM 11.14 Specification of the SIM Application Toolkit for the Subscriber Module - Mobile Equipment (SIM - ME) Interface. 1996.

[8] Remy Cricco and Y. Vinson. Integrating the SIM Card into J2ME as a Security Element 2005 [cited 2006 October]; Available from: http://www.gemplus.com/pss/telecom/download/jsr177_whitepaper_april05.pdf

[9] B. Aboba, e.a., Extensible Authentication Protocol. IETF, 2004.

[10] IETF (2006), RFC4186: Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)

[11] Lars Lunde, A.W., Using SIM for strong end-to-end application authentication, in Telematics. 2006, NTNU: Trondheim.

[12] Bluetooth-SIG, Bluetooth specification SIM Access Profile v.10. 2005

[13] Do Van Thanh, Tore Jønvik, Do Van Thuan & Ivar Jørstad: Enhancing Internet service security using GSM SIM authentication, Proceedings of the IEEE Globecom 2006 conference – ISBN 1-4244-0357-X – San Francisco, USA, Nov 27 - Dec 1, 2006