A Multimodal Authentication System for Authorizing the Access to NGN Services

R.Melen
Università di Milano Bicocca
riccardo.melen@unimib.it

M.Pignolo
Italtel
Maurizio.Pignolo@italtel.it

M.Sioli
Italtel
Moreno.Sioli@italtel.it

Abstract

An essential feature of new generation networks is the availability of many new services offered by several different players. Often, in this scenario, different applications and services have their own authentication method and use different credentials. More reliable, flexible and easy-to-use methods are needed.

We separate the recovery of application-specific credentials, hosted in the network, from the personal identification. Our first implementation combines fingerprint recognition and contactless smart cards in a highly secure system. After the biometric identification is carried out, the contactless smart card allows to sense the user presence, in order to unlock his/her workstation and to recover from a server, using a secure protocol, the credential necessary to access VoIP services. The mechanism strength is guaranteed by limiting in time and space the validity of the logical association between biometric identification and card ownership.

1. Introduction

An essential feature of new generation networks is the availability of many new services offered by several different players (network operators, value-added service providers, content providers and so on). In this scenario the problem of identity verification becomes very complex.

A first issue is that different applications and services employ each its own authentication method and use different credentials (we shall call these authentication methods “application embedded”). In the large majority of applications the authentication is based on the principle of checking “what the users knows”, therefore quite often the user ends up being harassed by a plethora of PINs, usernames and passwords, which are difficult to remember (unless they are kept so simple that they are easy to guess).

There are alternative techniques that do not require that the user remembers too many things: they can be based on objects that the user carries with him (e.g. smartcards [1,2]) or biometrics [3]. However these solutions have their own problems with respect to security and ease of use: smartcards can be lost or stolen, biometric techniques are perceived as intrusive and cumbersome. Moreover they require the distribution of special purpose terminals or cards, and the designer of the application/service is reluctant to be involved in a complex and expensive deployment process.

In many IT environments the problem of credential proliferation is solved by adopting single sign-on systems: it is interesting to evaluate the possibility to follow the same approach also in the more complex, open, multiprovider environment of NGNs. The Liberty Alliance framework [4] is an example of a single sign-on approach applied to the Web Services paradigm, focused on the network identity concept and the exchange of identity assertions, and not dealing directly with personal identification issues.

The considerations about complexity lead us to a second issue: the application embedded authentication methods are not related to the concepts of personal identification and physical presence detection. Therefore a service implying a defined degree of authentication security requires that the user engages always in the same procedures, irrespective of his present situation. Take for instance the case of secure transactions via a cellular phone: the fact that the user carries his phone and knows his PIN is not taken in consideration by the application, which always requires the introduction of credentials (another PIN); in some cases this procedure could be avoided, for instance for operations requiring an intermediate level of security (e.g. checking the account balance).

A related problem is the strong relation between the physical presence/activity of the user at the terminal and the maintenance of his authentication status: depending on a timeout value a short absence from the terminal implies either the complete

0-7695-2622-5/06/$20.00 (c) 2006 IEEE

maintenance of the authentication status (not very secure) or the need to restart the authentication procedure from scratch (rather annoying): it would be interesting to devise an intermediate solution.

At the core of the issues outlined above is the fact that authentication methods are embedded in applications, and do not take full advantage of the fact that the network holds much information about the user and can be a smart mediator in many security procedures.

2. Outline of the technical approach

2.1. Design principles

The approach that we are pursuing is based on two main ideas:

- in order to cope with heterogeneous authentication methods, application-specific credential are recovered from a network-centered secure repository, after a reliable user identification procedure is carried out;
- in order to limit complex and annoying procedures, simple, non intrusive techniques are used in situations when they reinforce/confirm a high level of security already achieved.

As a general principle, we plan to apply the combination of several techniques (biometric, smartcard and traditional PIN/password) in order to obtain a controlled level of security in the access to many types of network-based services, while limiting as much as possible the inconveniences relative to each specific technique. In this scenario, wireless-based detection of user presence (e.g. with contactless smart cards) plays an important role because it achieves the maximum ease of use, not requiring any kind of physical interaction, like introducing a password, reading a smart card or performing biometric recognition. We shall use the term “multimodal” to describe this methodology, because different authentication technologies can be used in various situations, depending on an evaluation of the level of security achieved insofar.

The effectiveness of our approach is based on the collaboration and the trust relations between different parties: the NGN plays a central role, performing critical security functions on behalf of the third party service/application providers; moreover in several cases the public network and the local environment (e.g. a local computer network) must cooperate in the management of the authentication procedures.

2.2. Requirements

We decided to explore the opportunities to implement the above principles in real-world environments. Among the possible reference scenarios are networks of computers with multimedia capabilities and home networks with access to triple-play public services. The systems we intend to realize must satisfy the following requirements:

- the authentication system acts as a trusted gateway towards many communication and information services accessible through the NGN;
- it simplifies the access to services, exploiting a credential repository hosted by the network;
- it has a limited impact on the client environment, requiring only off-the-shelf devices and software running on a standard platform;
- it exploits any authentication feature available in the local environment: for instance it must be integrated seamlessly in the logon procedures available in a computer network;
- it recognizes the user presence through wireless communication with a device that the user is supposed to wear, and manages the access permissions accordingly;
- it can embody sophisticated security features, such as biometric authentication.

2.3. System architecture and operation principles

An architecture satisfying the requirements above can be designed in a straightforward way. Figure 1 depicts a system composed of:

- a fixed terminal capable of accessing advanced services through the NGN,
- a local network featuring an authentication mechanism strong enough to guarantee secure access to all the services (the figure depicts a fingerprint recognition device, but also a password-based mechanism with a sound management policy would be suitable),
- a portable wireless device and a “reader” capable of performing presence detection,
- a network-based credential repository

The system operates as follows.

The user performs an initial logon operation, which comprises an authentication procedure. It is assumed that the authentication method is strong enough for the requirements of all the services in the user profile. As a consequence of the logon, the user profile is loaded and the access to services is enabled.

During this initial logon phase the reader checks for the presence of the wireless device: if it is found nearby, a logical relation is created between the presence of the user and of the wireless device:

afterwards the detection of the latter is assumed as a reliable indication of the presence of the former.

The reader probes periodically the wireless device: if absent the terminal is locked and the corresponding modifications to the service configurations are made (for instance, incoming VoIP calls can be deviated to a voice mailbox); when the user presence is detected again, the terminal is unlocked.

If the absence period is too long, a new authentication procedure is required in order to confirm the binding between user and wireless device. Although the wireless device can be lost, stolen or duplicated, such events can be considered very unlikely in a short timeframe, and the overall system works with the same level of security as if a new authentication were required at the end of any absence period.

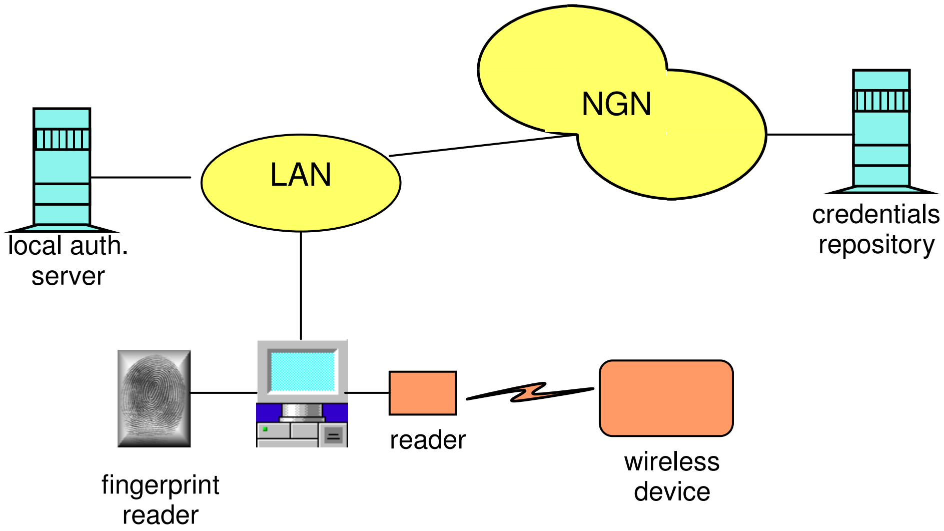

Figure 1

3. Demonstrator design and experimentation

3.1. Demonstrator design

We have developed a demonstrator for a network of Windows workstations. Each computer is interfaced to a contactless smart card reader, and we use an ISO 15693 card [5] as the wireless device. The authentication can be performed according to the standard username/password method, or employing a fingerprint reader: the use of the biometric authentication is an optional feature, which can be activated in the system, and workstations both with and without reader can operate together in the same network (it is also possible to enable some applications only for users which have performed the biometric authentication).

We automated the access to a network-based application called WBT [6]. WBT is a Web telephonyenvironment, supported by Italtel as a value-added application within its SIP-based VoIP platform. It can be described as a software PBX hosted in the network: a user who connects to the WBT service can make and receive voice calls and benefit from other personalized added value services (presence, personal directory…) through an IP network: both internal calls among WBT users and external calls towards the public telephony network are possible. In order to have access to WBT, an authentication procedure based on username and password is required; the effect of the authentication is the creation of a local configuration file where the user credentials are kept. When the connect operation is performed, the client checks for the presence of the configuration file: if absent, the user is prompted for the introduction of username and password.

In an environment running the demonstrator the user has two benefits. First, as soon as the user logs on, the WBT credentials are downloaded from a server and the configuration file is automatically created; therefore the manual introduction of credentials is avoided. Second, the access to the service is well protected without requiring any specific action from the user: the wireless reader checks periodically for the presence of the user, and the WBT service becomes accessible only when the user is present. In any situation where the user loses the control of the workstation (user logoff, administrator logoff) the configuration file is immediately removed from the system.

3.2. Implementation issues

The demonstrator software is made of two main components. The former contains all the functions which are strictly tied to the Windows logon mechanisms [7,8]: it manages the user logon and handles the events related to the user presence, such as the locking and unlocking of the workstation; it is implemented as a custom MSGina.dll. The latter is a process (installed as a Windows service) which handles the interface with the driver of the card reader (passing the significant events to the Winlogon process), interfaces with the server hosting the WBT application credentials and manages the creation and deletion of the configuration file.

The custom MSGina.dll implements a state machine which takes care of the possible workstation states (logged_off, logged_on, locked) and manages the transitions due to the detection of the presence or absence of the card. The complexity in the definition of the state machine was due to the need to make the system behave consistently in several real-world situations, in particular:

- when the logon is performed, if the card is not present or the reader is not connected, everything works in the standard mode, the workstation is locked after a timeout and unlocked with the manual intervention of the user (password),
- in case the user forgets or loses the card, manual unlock is possible,
- administrator unlock is possible, but the access to applications is blocked (e.g. the configuration file is removed),
- the user may decide to enable or disable manually the wireless presence detection mechanism.

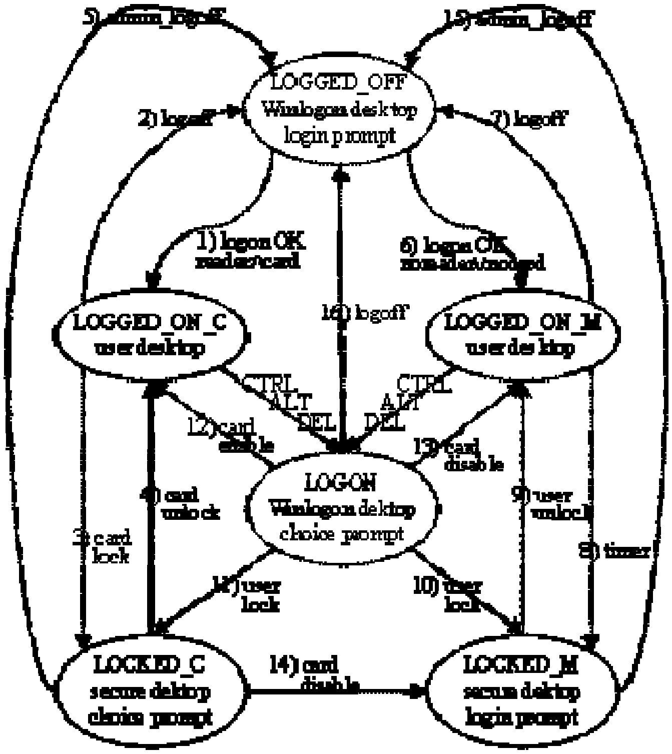

Figure 2

The resulting state machine is depicted in figure 2; each state specifies the desktop visible to the user. The typical states of the Winlogon mechanism have been modified, introducing the distinction between logged_on_c / locked_c, which are the operating states when the card is present, and logged_on_m / locked_m, which are the operating states without the card; the system begins operating in one of the two modes depending on the presence of the wireless detection mechanism. It is possible for the user to perform a manual change of the mode of operation; particular situations such as the physical removal of the reader bring the system in locked state without card.

3.3. Lessons learned

The realization of the demonstrator made us aware of various points requiring further attention.

A limitation of the demonstrator is the short range of commercial contactless smart card readers. With the reader we employed the user cannot “wear” the card while working at the computer, but has to put it close to the reader. This has an undesirable impact on the user, who has to pay some attention to the presence management mechanism. It is hard to overcome this limitation by recurring to inexpensive, off-the-shelf solutions. We are considering two different solutions to this problem: one is recurring to powered cards, the other one is based on the exploitation of the wireless communication capabilities of devices such as PDAs or cellular phones.

A significant part of the demonstrator software implements functions which are related to the Windows logon mechanism. Generally speaking, the adaptation of the authentication system to different environments requires a significant effort, which is not avoidable due to tight embedding of authentication functions in the operating system architectures.

Interfacing with the WBT environment turned out to be very simple; although this is due in part to the architectural characteristics of WBT, we believe that interfacing our system to heterogeneous network-based services/applications will turn out to be a relatively simple task.

The use of biometric verification in the logon phase provides a very sound mechanism, perfectly suited to ensure the very high level of trust that is needed in the authentication and wireless device binding phase. However the use of biometric techniques creates a lot of problems concerning privacy; we are aware of the complexity of these issues, particularly those regarding the storage of biometric identifiers; a future commercial realization of the system would require the separate storage of different portions of the biometric identifier (for instance part in the network-based server and part on a smart card) or its cryptographic protection (the key could be stored in the smart card).

4. Guidelines for further developments

In our first implementation the relation between the local environment and the network is pretty straightforward: as long as the user logs on the PC network, he is also granted access to the network-based services. In the general model we are considering the relation can be more complex. For instance in some cases the application could be more demanding, asking for a stronger security level; because the user has already logged on, there is just a “security gap” to fill, therefore the additional authentication step required could be very simple, such as introducing a password or answering a pre-stored question.

Likewise, we have said that when the user presence is sensed by the wireless reader, after a period of absence, the workstation is unlocked: this could correspond to a level of trust not acceptable for some applications, which could remain unavailable after the absence. In this case also a further authentication procedure could be required.

As indicated above, the long term objective is to decouple the service/application development from the burden of designing a suitable embedded authentication method. The application could ask for a predetermined “level of trust” in the user identification, and the network would ensure this level through various possible techniques, including the access control method to the network itself.

As mentioned in the introduction, the problems we are dealing with are different from the issues tackled by the Liberty Alliance. In those terms, we developed a flexible methodology used by an Identity Provider to authenticate a principal. In the future we plan to explore in more detail how our design can be related to the Liberty Identity Federation Framework.

5. References

[1] http://www.smartcardalliance.org

[2] U.S. General Service Administration: “Government Smart Card Handbook”, February 2004

[3] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar: “Handbook of Fingerprint Recognition,” Springer, New York, 2003

[4] http://www.projectliberty.org

[5] International Organization for Standardization: “ISO/IEC 15693 - Identification cards - Contactless integrated circuit(s) cards - Vicinity cards”, 2001

[6] http://www.italtel.com/ShowContent?item=2012

[7] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthn/security/winlogon_and_gina.asp

[8] D.Solomon, M.Russinovich: “Inside Microsoft Windows 2000”, 3rd ed., Microsoft Press, 2001