View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by AIR Universita degli studi di Milano

1

A Fuzzy Trust model proposal to ensure the identity of a user in time

Antonia Azzini and Stefania Marrara

Università degli Studi di Milano, Dipartimento di Tecnologie dell'Informazione
via Bramante 65, 26013 Crema (CR), Italy
{azzini, marrara}@dti.unimi.it

Summary. Access controls ensure that all direct accesses to objects are authorized by means of user identification. However, in some scenarios it is also necessary to continuously check the identity of the user in order to avoid malicious behaviors such as person exchanges immediately after the initial authentication phase.

Aim of this work is to propose a methodology based on a balanced mix of strong and weak authentication techniques studied to guarantee a high and prolonged in time level of security combining the advantages of each authenticator.

1.1 Introduction

Access controls ensure that all direct accesses to objects are authorized. By regulating the reading, changing, and deletion of data and programs, access controls protect against accidental and malicious threats to secrecy, authenticity, and system availability. The effectiveness of access controls rests on one important premise, the proper user identification [UPPJ04]: no one should be able to acquire the access rights of another. Traditionally, access control relies on profile information associated to users and resources in a given domain. However, in some scenarios it is also necessary to continuously check the identity of the user in order to avoid malicious behaviors such as person exchanges immediately after the authentication phase used for accessing the system. An example can be a system for university course examinations from remotely connected pc stations: in this situation we can be interested in being sure that the authenticated student is not substituted by another person just after the initial identification process, but she is the one that compiles the entire course test.

Aim of this work is to propose a methodology based on a balanced mix of strong and weak authentication techniques studied to guarantee a high and prolonged in time level of security avoiding the excessive cost of using only biometric devices.

For this reason, remote access is initially provided by means of biometric devices but then it is granted in time by means of other authentication

methods. In such a scenario, the system must distinguish between the initial authentication phase, in which it recognizes the user profile and allows the access, and the following authentication steps in which the system decides if its trust in user's identity is enough high to allow the user to continue to perform the activity she is doing. Focus of this paper is not the semantics used to describe the users profile, but the description of the fuzzy logic based methodology used by a system to continuously check and confirm its trust in the identity of a user.

The structure of the paper is as follows. Section 1.2 presents a brief overview of the authentication devices used to ensure the identity of a user and compares advantages and drawbacks of the different techniques, Section 1.3 describes the general architecture of the fuzzy methodology used to ensure the user identity during time, Section 1.4 presents the fuzzy rules used by the methodology engines to compute the user identity trust level during time and, finally, Section 1.5 reviews the conclusions of this work and propose some future work and open issues.

1.2 User authentication systems and their trustfulness

User authentication is the process of positively verifying the identity of an user, often as a prerequisite to allowing access to resources in a system. User authentication is then essential for reliable access control and rights management systems determine a user authorization to access the content [UPPJ04].

1.2.1 Traditional systems

Traditional cryptosystems do not identify the user as such. The authentication is *knowledge-based*, answering the question: 'What you know' such as a password, or *token-based*, answering the question: 'What you have' such as a key, magnetic or chip card.

A password includes single words, phrases, and personal identification numbers (PINs) that are closely kept secrets used for authentication. The basic problem with this technique is that a memorable password can often be guessed or searched by an attacker and a long, random, changing password is difficult to remember. As result they are stored and released on some alternative authentication mechanism and they can be shared with other users.

An identity or security token is a physical device that can contain passwords, such as a bankcard, or smartcard, that includes tamper-resistant packaging and special hardware that disables the token if it is tampered with or if the number of failed authentication attempts exceeds a chosen threshold. The main problem is that these devices can be lost, stolen, forgotten or disclosed.

Strong authentication methods are usually developed to solve the drawbacks the traditional techniques. Biometric systems implement human authentication and identification in rights management systems. They are defined as

ID-based authenticators, answering the question: 'Who you are'. They are characterized by the uniqueness to one person. The main security defense is that they are difficult to copy or forge.

1.2.2 Biometric systems

Biometrics are automated methods of authentication based on measurable human physiological or behavioral characteristics. Common physical biometrics include fingerprints, hand or palm geometry and retina, iris or facial characteristics. Behavioral features include signature, voice (which has also a physical component), keystroke pattern and gait.

Biometric technologies most commonly implemented are based on:

- *Fingerprint*, based on matching numeric information of finger minutie. It is easy, fast of use and low cost and it has considered the higher authentication form from the people.
- *Hand Geometry*, which involves analyzing and measuring the shape of the hand. It offers a good balance of performance characteristics and is relatively easy of use, the accuracy can be very high.
- *Iris*, which analyzes features found in the iris, uses a fairly conventional camera element and requires no close contact between the user and the reader. It has the potential for higher than average template-matching performance, even though easy of use and system integration have not traditionally been strong points with iris scanning devices.
- *Face*, which analyzes facial characteristics. It requires a digital camera to develop a facial image of the user for authentication.
- *Voice*, which is not based on voice recognition, but on voice-to-print authentication, where complex technology transforms voice into text.
- *Signature*, which analyzes the way a user signs her name. Signing features such as speed and pressure are as important as the finished signature's static shape.

These methods are inherently more reliable than password-based authentication, as biometric features cannot be borrowed, stolen or forgotten; furthermore they are extremely difficult to copy, share and distribute. The main issue in biometric authentication system is performance, defined considering different factors, depending on critical issues in the data acquisition phase.

A comparison between different techniques is in [LS01] and briefly reported in Table 1.1

Once enrolled in a biometric system, a user can be successfully authenticated. The overall process, presented in detail in [UPPJ04, VZ03], is the same for each different biometric approach, and it is represented with a first enrollment phase and a second matching phase. The result is typically explained in terms of a *matching score*; the higher the matching score, the better comparison result is obtained.

Table 1.1. Biometric Comparison.

Characteristics	Fingerprint	Hand Geometry	Iris	Face	Voice	Signature
Ease of use	High	High	Medium	Medium	High	High
Accuracy	High	High	Very High	Very High	High	High
Use acceptance	Medium	Medium	Medium-low	Medium	Very high	High
Required security level	High	Medium	Very high	Medium	Medium	Medium
Long term stability	High	Medium	High	Medium	Medium	Medium

In a such identification system, acceptance is determined considering two types of biometric errors:

- FAR - False Acceptance Rate - that defines the percentage of impostors incorrectly matched to a valid user's biometric.
- FRR - False Rejection Rate - that defines the percentage of incorrectly rejected valid users.

There is a trade off between FAR and FRR in every biometric system, since they are functions of the system threshold t: if t is decreased to make the system more tolerant to input variations and noise, FAR increases. For each biometric technology these rates are calculated by experimental tests. Phenotypic features do not set limits on the FAR, but clearly, over time the phenotypic variation imposes a lower limit on the FRR.

1.2.3 Critical Issue

Some systems incorrectly assume that biometric measurements are secret and grant access to any user presenting matching measurements. On the other hand, as sensitive data, biometrics should be properly protected, but they cannot be considered secret. The only way to secure a biometrics system is to ensure that the characteristics presented come from a real person and they are obtained and authenticated during verification from the person. For this reason it should be defined a *liveness test*, in which, before granting a user access, a system must make sure that the authentication device is verifying a living person; this tests are usually performed by the core biometric technology.

Another critical aspect is that a biometric system must believe that the biometric measurements presented come from a trusted input device and they have been captured at a certain time. If authentication is performed on-device, the device should be trust-worthy; otherwise, if it is performed off-device, the software operating environment and the communication link between the software and the device must be secure.

1.2.4 Advantages and Shortcomings

Biometric characteristics are essentially permanent and unchangeable and users cannot pass them to other users as easily as they do with cards or

passwords. Furthermore these techniques are based on features that cannot be lost or forgotten. A biometric authentication systems is also fast. The authentication of an user in a fingerprint reader system can take under two seconds, whereas finding a key ring, locating the right key and using it can take as long as ten seconds.

Some issues remain jet unresolved. In some cases, if the input sample quality is not sufficient for further processing, the system must reacquire data, and the resulting system might be more complicated or more expensive. Furthermore some biometric sensors, particularly those having contact with users, have a limited lifetime. The most important drawback is that biometric systems could violate user privacy. Biometric characteristics are sensitive data containing personal information: for example a DNA sample contains the user's susceptibility to disease. A biometric system can imply loss of anonymity, and users may consider it intrusive or personally invasive.

1.2.5 Traditional vs Strong Authentication Techniques

Different authentication categories may be appropriate for different applications, depending on perceived user profiles, the need to interface with other systems or database, environmental conditions, and a host of other application specific parameters. The attributes of the three categories of user authentication, described in the previous subsections, are compared in Table 1.2

Table 1.2. Basic user authentication attributes.

Attributes	User Authentication		
	Knowledge Based	Token Based	ID based
Identification	Password, Secret	Token	Biometric
Supports	Secrecy or obscurity	Possession	Uniqueness and personalization
Security Defence	Closely kept	Closely held	Forge resistant
Security Drawback	Less secret	Lost, stolen	Difficult to replace
Examples	Combinational lock, password	Metal key, smart card	Fingerprint, face

The different authentication technologies are compared in detail in [O'G03], giving a number of some potential attacks against user authentication and relative defenses by each technique; however, important issue for each of them can be summarized as follows:

- Knowledge-based: its secrecy and high keyspace defend well against search and host attacks. Its ability to participate in challenge-response protocols protects against replay and transmission attacks, with non expensive costs. The main problem is the difficult to remember passwords for the user.

This technique does not provide a compromise detection and does not offer much defense against repudiation.

- Token-based: it can store or generate multiple passcodes (also if combined with a password). It provides compromise detection and added protection against denial-of-service attacks. The two main shortcomings are inconvenience and cost, and vulnerability to theft. Equipment cost is higher than a password and comparable to a much secure biometric that requires a reader. A token with biometric combination has similar security characteristics to a token plus password, however the inconvenience of FRR for a biometric, defined in 1.2.2, with respect to the inconvenience of remembering a password is matter of user preference.
- Biometrics: one advantage of biometric is that it is less easily lent or stolen than the other authenticators, so it provides a stronger defense against reputation. The relative simplicity also improve a better security and trustworthy authentication process. The stability of such system refers to the fact that a good biometric maintains its distinctive features over time, without compromising information. A problem is the limited lifetime for particular biometrics, but the main drawback is the possible violation of the user privacy.

An appropriate authentication solution depends upon the particular application, each system has its strength and weakness and no a single technique is expected to effectively meet all requirements of all the applications like accuracy, security, trustworthy and cost. Although, few combinations of authenticators are recommended, in order to provide secure and trustworthy authentication systems.

1.3 Architecture of the model

This section introduces an access control model based on a balanced mix of strong and weak authentication techniques studied to guarantee a high level of security combining the advantages of each authenticator. The proposed model describes a trust evaluation process implemented by a system which needs to be continuously confirmed about the identity of the user who is performing a certain activity. As an example, we can imagine an on-line degree system which needs to be sure of the identity of the student who is making an examination, not only before the test takes place, but also during the test itself, in order to avoid people replacements after the initial identification process. Fig. 1.1 shows the basic steps of our trust process: after an initial authentication, the server can require a second or third (or even more) step of authentication based on two parameters, the level of trust previously computed and the time passed from the last authentication. We suppose the first authentication acquired by strong techniques while the following steps can be acquired by strong or weak techniques on the basis of the trust level we have in a certain time.

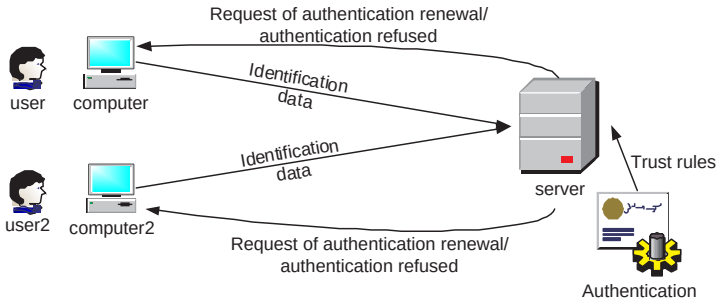

Fig. 1.1. Context for trust evaluation model

1.3.1 Trustworthiness evaluation parameters

After receiving an initial strong authentication, the server accepts or refuses the user on the basis of the biometric value (BIO) which has to be higher than a certain threshold (th) fixed for the application. Indeed, we suppose that our strong acquisition techniques use an internal fuzzy matching function between the actual enrollment and the template stored. In case the user is authenticated, the system receives a fuzzy value (e.g., 0.85) which represents how the biometric enrollment matches the user's template. The timeliness function, which shows how the system's trust in the identity of the user decays in time, is shown in equation 1.1 where the value BIO_{max} represents the initial value obtained at the initial authentication at time t_0 and D is the rate of decay.

$$BIO(t) = BIO_{max} * e^{-(t-t_0)/D} \tag{1.1}$$

Additionally, the system takes into account another parameter TOK that represents the boolean output (high/low or authenticated/denied) of the weak authentication system which supports the evaluation of the trust in the user's identity during the activity. At the initial authentication step, the weak techniques are not directly involved, and the parameter TOK is automatically set to *high*. Prior to the processing of the inputs, it is necessary to create fuzzy membership functions which define the degree of membership of each input parameter in the context of the proposed model. Furthermore, sets of fuzzy rules, based on linguistic variables, which combine the fuzzy sets, are defined in order to characterize the output of the model.

After the preprocessing step, the information obtained by the biometric engine and the parameter TOK are fed into a first fuzzy inference engine *Start* in order to calculate a trustworthiness value *trust* that provides the level of trust of the system in the user's identity after the initial authentication at time t_0. The output $TRUST$ is then fed to another engine, *Confirmation*, that

checks if the user is active ($us(t_0) = OK$) and in case decides if it is necessary a new biometric or weak enrollment to enforce the trust of the system before the user can continue his activity. The enrollments provide new parameters BIO_{t_0} or TOK_{t_0} that are used by another engine, *FinalStepTrust*, to compute the definitive level of trust at time t_0. If the level of trust is higher then the threshold value defined for the application the user is authenticated and can start to work, otherwise she is refused by the system.

After a certain time interval Δt, the system checks if the trust acquired at time t_0 has been affected by the decay rate of the initial biometric authentication and then needs to be confirmed. The trust level achieved by the user at time t_0 and the new value of the parameter BIO at time $t_1 = t_0 + \Delta t$ ($BIO(t_1)$) are now fed to the last fuzzy inference engine *TimeTrust*, which decides the trust level at time t_1 which can cause the system to refuse the user or to ask for trust enforcement by going back to the *Confirmation* engine.

The process, shown in Figure 1.2, stops when the user is not more active or the trust level decays dramatically to the value of *very low*.

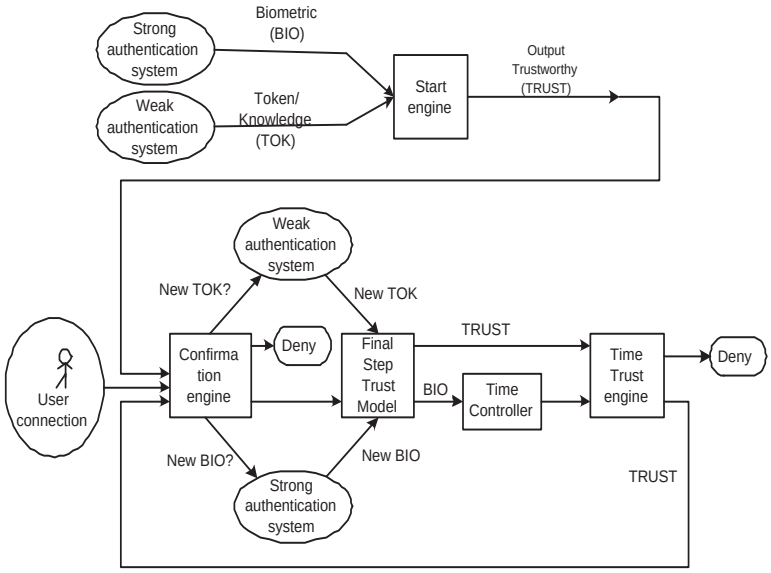

Fig. 1.2. Trust Model combining Strong and Weak Authentication Methods and Fuzzy Systems.

1.4 Trust Model Rules

Each model previously described in Section 1.3, has been implemented with different fuzzy rules, in order to control the trustworthy value at each time

step t with respect to different evolved parameters. An example of fuzzy rules, defined for each implemented model, is reported in Table 1.3.

Table 1.3. Sample Fuzzy Rules defined for each Trust Model.

Model	Fuzzy Rules
Start Model	**IF** BIO is high **AND** TOK is high **THEN** TRUST is high **IF** BIO is medium **AND** TOK is high **THEN** TRUST is medium ... **IF** BIO is low **AND** TOK is low **THEN** TRUST is very low
Confirmation Model	**IF** USER is ok **AND** TRUST is high **THEN** TRUST is high **IF** USER is ok **AND** TRUST is low **THEN** TRUST is medium **AND** New BIO ... **IF** USER is ok **AND** TRUST is medium **THEN** TRUST is medium **AND** New TOK
Final-Step Model	**IF** New BIO is high **THEN** TRUST is high **IF** New TOK is high **THEN** TRUST is medium ... **IF** New BIO is low **THEN** TRUST is very low
Time-Trust Model	**IF** BIO is high **AND** TRUST(t_0) is high **THEN** TRUST(t_1) is high **IF** BIO is medium **AND** TRUST(t_0) is high **THEN** TRUST(t_1) is medium ... **IF** BIO is low **AND** TRUST(t_0) is medium **THEN** TRUST(t_1) is low

The Start Model is carried out at first time, giving a trustworthy value depending on biometric and token/knowledge based acceptance rates, that have been acquired at the initial user login step.

The trust output is then carried out at each step in the other models, and it will be checked: if its value is lower than a fixed threshold value, than the system rejects further user authentication and stops the entire fuzzy model; otherwise the trust value will become one of the inputs for the further models, in order to obtain a new trustworthy value at the new step.

The trustworthy value will go into a loop in which timed checks will be implemented in order to obtain respectively user rights and user status connection.

1.5 Conclusions

In this work we propose a fuzzy logic based methodology based on a balanced mix of strong and weak authentication techniques studied to guarantee a high

and prolonged in time level of security combining the advantages of each authenticator.

In such a scenario, the system, after an initial authentication phase in which it recognizes the user profile and allows the access, performs some other authentication steps in which it decides if its trust in user's identity is enough high to allow the user to continue to perform the activity she is doing. Focus of this paper is the description of the fuzzy logic based methodology used to continuously check and confirm the trust level in the identity of a user.

Future work will include research studies in order to avoid biometric attacks and weak malicious authentication at first access and during the overall examination time.

Acknowledgments

This work was partly funded by the Italian Ministry of Research Fund for Basic Research (`FIRB`) under projects `RBAU01CLNB_001` "Knowledge Management for the Web Infrastructure" (`KIWI`). and `RBNE01JRK8_003` "Metodologie Agili per la Produzione del Software" (`MAPS`).

References

[LS01] S. Liu and M. Silverman. A practical guide to biometric security technology. *IEEE Journal on Security*, (January-February):27–32, 2001.

[O'G03] L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. In *Proceedings of the IEEE*, volume 91, pages 2021–2040, December 2003.

[UPPJ04] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain. Biometric cryptosystems: issues and challenges. In *Proceedings of the IEEE*, volume 92, pages 948–960, June 2004.

[VZ03] M. Vaclav and Z.Riha. Toward reliable user authentication through biometrics. *IEEE Journal on Security and Privacy*, (May-June):45–49, 2003.