Securing Critical Systems through Continuous User Authentication and Non-repudiation

Enrico Schiavone

Department of Mathematics and Informatics, University of Florence

Viale Morgagni 65, 50134, Florence, Italy

enrico.schiavone@unifi.it

***Abstract*— Providing a mechanism for authenticating a user's access to resources is very important, especially for systems that can be considered critical for the data stored and the functionalities offered. In those environments, traditional authentication mechanisms can be ineffective to face intrusions: they usually verify user's identity only at login, and even repeating this step, frequently asking for passwords or PIN would reduce system's usability. Biometric continuous authentication, instead, is emerging as viable alternative approach that can guarantee accurate and transparent verification for the entire session: the traits can be repeatedly acquired avoiding disturbing the user's activity. Another important property that critical systems may need to be guaranteed is non-repudiation, which means protection against the denial of having used the system or executed some specific commands with it. The paper focuses on biometric continuous authentication and non-repudiation, and it briefly presents a preliminary solution based on a specific case study. This work presents the current research direction of the author and describes some challenges that the student aims to address in the next years.**

Keywords—authenticity; non-repudiation; continuous authentication; biometrics; security;

I. Introduction

In the last decades, the constant growth and diffusion of Information and Communications Technology (ICT) contributed to make people's life easier. Today, users and operators can exploit technologies to share confidential data from a long distance or to execute critical commands in real-time. However, the need for security services has gone hand in hand with the technological progress.

Especially when some operation is considered highly critical, preventing unauthorized access can avoid undesirable consequences or even catastrophes. The system in charge to execute an operation has to verify that the involved users are really who they claim to be, before giving them the permission to accomplish the action.

Authentication is the process of providing assurance in the claimed identity of an entity. The identity verification is obtained exploiting a piece of information and/or a process called *authentication factor* that belongs to one of the following categories: knowledge (e.g. password, PIN); possession (e.g. passport, private key); inherence (biometric characteristics, physiological or behavioral, e.g. fingerprint or keystroke).

Traditionally this verification is based on pairs of username and password and performed as a single-occurrence process, only at login phase. No checks are executed during sessions, which are terminated by an explicit logout or expire after an idle activity period of the user. Instead, if the operation covers a long period, it may be necessary to repeat the authentication procedure; however, asking for passwords and secrets several times requires users' active participation, and it may disturb their main activity. In order to design an effective continuous authentication mechanism for critical systems, together with security, also usability has to be taken into account.

To prevent unauthorized access of ICT systems, solutions based on *biometric continuous authentication* have been studied in literature. They modify user identity verification from a single-occurrence to a continuous process [1], [2]. To enhance security, authentication can also exploit multiple traits, being multimodal; in fact it has been verified that using various biometric traits, properly combined, can improve the performance of the identity verification process. In addition, with appropriate sensors, some biometric traits can be acquired transparently.

However, most of the existing solutions suffer from high computational overhead or their usability has not been adequately substantiated. Our goal is to design a multi-biometric continuous authentication system that is usable, incurs in little system overhead and permits to easily manage the trade-off between security and usability through configuration parameters.

Besides authentication, being able to demonstrate user involvement in the usage of a system or application can also be useful. In fact, when a dispute arises or a disaster happens people may try to deny their involvement and to repudiate their behavior.

Repudiation can be defined as the denial of having participated in all or part of an action by one of the entities involved. Consequently *non-repudiation* is the ability to protect against denial by one of the entities involved in an action of having participated in all or part the action.

A non-repudiation mechanism should guarantee the establishment of the facts even in front of a court of law. Therefore, a non-repudiation service can be useful both as a mean to obtain accountability as well as a deterrent for deliberate misbehaviors.

This paper presents the research plan of a second year Ph.D. student and it follows [13] and [14]. The objective of the research direction identified is to study, define, and possibly test, mechanisms that can offer authentication and non-repudiation, with the aim to provide trustworthy security services for ICT systems.

The present work is focused on biometric continuous authentication and describes a case study regarding control room workstations, in which traditional mechanisms -i.e. password-based authentication- are not sufficient for the expected requirements. In addition, it addresses the issue of repudiation and study scenarios, and possible solutions in which a biometric-based non-repudiation service can help solving disputes between entities.

The paper proceeds as follows: Section II presents our contribution in providing continuous authentication, briefly describing the approach we followed, some results regarding its usability and the ongoing work related to risk assessment; Section III concentrates on non-repudiation, its connection with biometrics and introduces some scenarios.

II. Biometric Continuous Authentication of Control Room Operators

A. *Context and Requirements*

Control room operators are a category of users that can access potentially sensitive information to issue critical commands for the entire working session. They are also directly responsible for such commands and for the data accessed, modified and deleted.

For instance, transportation (e.g. airways, railways), electric power generation, military or aerospace operations are some contexts in which control rooms are often adopted. Operators are in charge of analyzing and interpreting situations that describe the current status of events and activities. They are also able to command intervention teams on field, or to dispatch instructions in a target area. It is required to protect the control rooms and their workstations from unauthorized people, both *intruders* and *insiders*, that may want to acquire privacy-sensitive data, disrupt the operations, disseminate false information, or simply commit errors which will be ascribed to the operator in charge of the workstation.

Consequently, in order to protect the workstations, we need to guarantee *authenticity* and *non-repudiation* of the commands/functions executed, meaning that the identity of the worker which sends the commands from a workspace should be properly verified and they cannot deny that action.

In addition, the workspace should be usable for the legitimate worker: the security mechanism should not disturb or excessively slow down the working activity of the operator. For that reason the verification process should be transparent.

B. *The Proposed Continuous Authentication Protocol*

To comply with the above requirements we defined a client-server multimodal continuous authentication protocol (for further details on requirements please refer to [3]). The overall architecture of the biometric system is composed of the operator workstation and the connected sensors required for acquiring the biometric data. It is based on three biometric subsystems, for face recognition, fingerprint recognition and keystroke recognition.

The protocol is shown in the sequence diagram of Fig. 1. and is divided in two phases: the initial phase and the maintenance phase.

Initial phase. It is composed of the following steps:

- The user logs in with a strong authentication or a successful biometric verification executed with all the three subsystems in a short time interval.
- Biometric data is acquired by the workstation and transmitted to the authentication server.
- The authentication server matches the operator’s templates with the traits stored in a database and verifies his/her identity.
- In case of successful verification, the Critical System establishes a session and allows all restricted functions expected for the operator's role.
- The authentication server computes and updates a *trust level* that decreases as time passes; the session expires when such level becomes lower than a threshold.

*Maintenance phase***.**

- The authentication server waits for fresh biometric data, from any of the three subsystems.
- When new biometric data is available, the authentication server verifies the identity claimed by the operator and, depending on the matching results of each subsystem, updates the trust level.
- When the trust level is close to the threshold, the authentication server may send a notification to the operator, to signal that the session will expire soon.
- When the trust level is below the threshold, the Critical System disables the restricted functions,

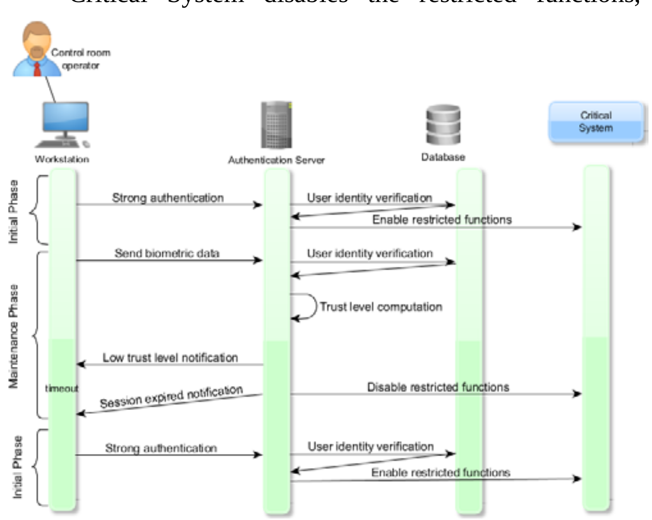

Fig. 1 Sequence Diagram of the Protocol

which will be available again only when the operator restarts from the initial phase.

No active participation of the operator is necessary, which only needs to use the mouse – that should incorporate a fingerprint scanner at the place where users would normally place their thumb-, a keyboard, or to be positioned in front of a webcam.

More details about the protocol, the algorithm for trust level computation the prototype realized and the software implemented can be found in [3].

C. Usability and Risk Assessment

To investigate the usability of the system, we are conducting an experiment (which in part is a replication of [10]) involving a wide group of participants, asking them to complete four tasks on a workstation provided with our continuous authentication application running in background. First, we want to measure the *effectiveness* of our solution, calculating the FAR (False Acceptance Rate), and the FRR (False Rejection Rate) for each of the biometric subsystem, and for the main biometric continuous authentication system.

Then, we are going to measure the *efficiency* of the system, tracking the time interval between the initial authentication and any unexpected termination (meaning that the trust level has fallen below the threshold). Similarly, we are interested in the time necessary to the authentication system to reject an impostor. The user *satisfaction* will be measured with a questionnaire. In addition to usability testing, we want to clarify if the *overhead* introduced by the continuous authentication system can slow down the workstation and consequently increase the users' required effort. Another main goal is to perform the specified measurements with different *parameters configuration*, e.g. varying the trust threshold (the minimum trust level allowed to remain authenticated).

Preliminary results are in [11]. They show that the system appears to be secure and usable, and there is every chance to increase its usability integrating three highly accurate recognition algorithms. In fact, 75% of the users completed the tests without unexpected expirations, and this result is interesting if compared with the previous studies. As expected, modifying parameters we were able to obtain a highly usable configuration, with which the users remained authenticated for the whole duration of the session. In terms of resources utilization, Biometric Continuous Authentication System did not have any significant impact on task performance, and its overhead was negligible.

We are also conducting a NIST-compliant qualitative risk assessment for the biometric continuous authentication protocol [15]. The activity focuses on both threats related to transmission and specific for the biometric system level. The goal is to establish its strengths, weaknesses and consequently understand the countermeasures needed in order to improve the security of our authentication solution.

The proposed protocol addressed the problem of non-repudiation exploiting the biometric nature of the credentials, which are supposed to provide it inherently. However, this is still under discussion, as described in Section IV; for this reason we are working on improvements that should fully guarantee non-repudiation.

III. Non-repudiation

Explanatory tests show that with our solution for continuous authentication, the *authenticity* of control room operators is guaranteed. However, although with this solution it appears very hard for the user to deny having accessed the system, the deniability is related to error rates: is an intruder still able to repudiate actions?

Trying to directly address this problem, we aim to discuss if a continuous authentication mechanism, based on the usage of biometric traits, provides sufficient undeniable evidence of user's participation in an action.

A. Biometrics Can Guarantee Non-Repudiation?

According to the author of [12], unlike passwords and tokens, biometrics - because of their strong binding to specific persons- is the only authentication factor capable of guaranteeing that authentication cannot subsequently be refused by a user.

In [4] the author claims that for authentication mechanisms, non-repudiation depends on: (i) The ability of the authentication mechanism to discriminate between individuals; (ii) The strength of binding between the authentication data and the individual in question; (iii) Technical and procedural vulnerabilities that could undermine the intrinsic strength of the binding; (iv) Informed consent of the individual at the time the authentication is given.

In addition, the discrimination capabilities of biometrics depend on the technology used and on other application-related factors, that are quantified in terms of error rates (FAR and FRR) [4]. Despite biometric traits are sometimes presented in the computer security literature as an authentication factor that may solve the repudiation problem [12], [4], other works like [5], [6] draw completely different conclusions. Analyzing the state of the art, we can state that the answers to this question are contradictory.

However, the situation changes if biometric authentication is coupled with another security mechanism like digital signature, which is commonly considered as the standard approach to achieve non-repudiation. In fact, public key infrastructure, or PKI, and biometrics can well complement each other in many security applications [7].

Apart from biometrics, our opinion is that a non-repudiation service should be capable of:

- Reliably (and if necessary continuously) verifying the user's identity. In other words, we think that non-repudiation is impossible without authentication.
- Generating an undeniable and unforgeable evidence of the action and bind it with the user's identity.

B. Further Non-repudiation Scenarios

There are many actions that an individual or an entity may want to deny, e.g. for economic reasons, to fraud someone or to hide a malpractice. The most studied non-repudiation protocols in the state of the art regard the transactions and exchange of messages scenario [8], [9].

Usually a basic transaction is defined as the transferring of a message M from user A to user B, and the following are the typical disputes that may arise:

- A claims that it has sent M to B, while B denies having received it;
- B claims that it received M from A, while A denies sending it; and
- A claims that it sent M before a deadline T, while B denies receiving it before T.

Transactions, especially in the e-commerce field, are often denied by consumers. According to The New York Times, 0.05% of MasterCard transactions worldwide are subjects of disputes, that probably means around 15 million questionable charges per year. Analysts, in general, estimate that 20% of disputes involve fraud. Providing a non-repudiation service for this scenario and solving those disputes, would probably make issuers save a lot of money.

Non-repudiation services can cover other kind of actions, not only transactions. In fact, there are many scenarios in the field of information exchange that may be better protected with proper authentication and non-repudiation services. Changing the mean of communication, the nature of exchanged data or the kind of information flow (i.e. one-time occurrence or continuous), we can distinguish several issues to address and related solutions. For instance, e-mails, instant messaging, VoIP communications or accessing files stored in a private area on a server are some of the possible scenarios. In general, what the service should generate is undeniable evidence that can be used if a dispute arises. Evidence is a crucial object, and sometimes has to be processed by a Trusted Third Party (TTP) [8].

IV. Conclusions and Future Works

Security is a fundamental property in the ICT field, especially for critical systems and applications in which confidential data are managed and where unauthorized accesses and behaviors can cause undesirable consequences or even catastrophes. In this context, *authentication* and *non-repudiation* are common requirements. The aim of our research is to study approaches to guarantee them. First, we are planning to integrate an existing biometric continuous authentication mechanism [2] with a non-repudiation service and our solution will probably combine biometric continuous authentication with digital signature.

Finally, another ongoing activity is investigating if biometrics-based solutions permit to obtain irrefutable evidence of user identity: for different scenarios we will study which biometric trait –single or combined- can be appropriate, also considering the error rates that may be admissible, the technological or environmental limitations and the user acceptability. A strategy can be searching a set of the most accurate biometric verification algorithms in literature (e.g. exploiting initiatives like [16]), and trying to evaluate the probability of successful non-repudiation for a user of a continuous authentication system based on a combination of those algorithms.

Acknowledgments

The author would like to thank his supervisor Prof A. Bondavalli and co-supervisors, Dr. A. Ceccarelli and Prof. A. Carvalho that are assisting this research providing insight and expertise. This work has been supported by the European FP7-IRSES project DEVASSES and by the Joint Program Initiative (JPI) Urban Europe via the IRENE project.

References

[1] S. Kumar, T. Sim, R. Janakiraman, and S. Zhang, “Using continuous biometric verification to protect interactive login sessions,” In: 21st Annual Computer Security Applications Conference (ACSAC), pp. 441-450, 2005.

[2] A. Ceccarelli, L. Montecchi, F. Brancati, P. Lollini, A. Marguglio, and A. Bondavalli, “Continuous and transparent user identity verification for secure internet services,” In: IEEE Transactions on Dependable and Secure Computing, 12(3), pp. 270-283, 2015.

[3] E. Schiavone, A. Ceccarelli, and A. Bondavalli, “Continuous user identity verification for trusted operators in control rooms,” Proc. of ICA3PP, pp. 187-200, 2015.

[4] H. Bidgoli, “Handbook of information security, Threats, Vulnerabilities, Prevention, Detection, and Management”. vol. 3. 2006.

[5] D.R. Kuhn, V.C. Hu, W.T. Polk, and S.J. Chang, “Introduction to public key technology and the federal PKI infrastructure”. National Inst of Standards and Technology Gaithersburg MD, 2001.

[6] A. Kholmatov, and Y., Berrin, "Biometric cryptosystem using online signatures." *Computer and Information Sciences–ISCIS 2006*. Springer Berlin Heidelberg, 2006. 981-990.

[7] H. Feng, and C. Choong Wah, "Private key generation from on-line handwritten signatures." *Information Management & Computer Security* 10.4 (2002): 159-164.

[8] J.A. Onieva, J. Zhou, and J. Lopez. "Multiparty nonrepudiation: A survey." *ACM Computing Surveys (CSUR)* 41.1 (2009): 5.

[9] S. Kremer, O. Markowitch, and J. Zhou, “An intensive survey of fair non-repudiation protocols”, 2002.

[10] G. Kwang, R.H. Yap, T. Sim, and R. Ramnath, “An usability study of continuous biometrics authentication”. In *Advances in Biometrics* (pp. 828-837). Springer Berlin Heidelberg, 2009.

[11] E. Schiavone, A. Ceccarelli, A. Bondavalli, and A. Carvalho “Usability Assessment in a Multi-biometric Continuous Authentication System” Proc. of Dependable Computing (LADC), 2016 Seventh Latin-American Symposium on, 43-50, 2016.

[12] Li, Stan Z. “Encyclopedia of biometrics”: I-Z. Vol. 1. Springer Science & Business Media, 2009.

[13] E. Schiavone “Providing Continuous Authentication and Non-Repudiation Security Services” Student Forum of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2016

[14] E. Schiavone, A. Ceccarelli, and A. Bondavalli “Continuous Authentication and Non-repudiation for the Security of Critical Systems, "Reliable Distributed Systems (SRDS), 2016 IEEE 35th Symposium on", 207-208, 2016.

[15] E. Schiavone, A. Ceccarelli, and A. Bondavalli “Risk Assessment of a Biometric Continuous Authentication Protocol for Internet Services” to appear in Proc. of ITASEC17 The Italian Conference on cybersecurity, 2017.

[16] Kemelmacher-Shlizerman, Ira, et al. "The megaface benchmark: 1 million faces for recognition at scale." *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2016.