UNIVERSITÀ
DEGLI STUDI
FIRENZE

FLORE
Repository istituzionale dell'Università degli Studi di Firenze

Continuous Authentication and Non-repudiation for the Security of Critical Systems

Questa è la Versione finale referata (Post print/Accepted manuscript) della seguente pubblicazione:

Original Citation:

Continuous Authentication and Non-repudiation for the Security of Critical Systems / Schiavone, Enrico; Ceccarelli, Andrea; Bondavalli, Andrea. - ELETTRONICO. - (2016), pp. 0-0. ((Intervento presentato al convegno SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS tenutosi a Budapest [10.1109/SRDS.2016.31].

Availability:

This version is available at: 2158/1049929 since: 2021-03-12T14:23:18Z

Publisher:

IEEE

Published version:

DOI: 10.1109/SRDS.2016.31

Terms of use:

Open Access

La pubblicazione è resa disponibile sotto le norme e i termini della licenza di deposito, secondo quanto stabilito dalla Policy per l'accesso aperto dell'Università degli Studi di Firenze (https://www.sba.unifi.it/upload/policy-oa-2016-1.pdf)

Publisher copyright claim:

(Article begins on next page)

20 December 2021

Continuous Authentication and Non-repudiation for the Security of Critical Systems

Enrico Schiavone, Andrea Ceccarelli, Andrea Bondavalli
Department of Mathematics and Informatics, University of Florence
Viale Morgagni 65, 50134, Florence, Italy
{enrico.schiavone, andrea.ceccarelli, bondavalli}@unifi.it

***Abstract*—User authentication is a key service, especially for systems that can be considered critical for the data stored and the functionalities offered. In those cases, traditional authentication mechanisms can be inadequate 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 security service that these systems may need is non-repudiation, which protect against the denial of having used the system or executed some 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 cyber-physical systems, preventing unauthorized access can avoid undesirable consequences or even catastrophes, and it is true especially when the system is considered highly critical. Traditionally, users' authentication is based on pairs of username and password and performed as a single-occurrence process, only at login phase. Instead, if the operation covers a long period, it may be necessary to repeat the authentication procedure. However, asking for passwords or PINs many times requires users' active participation and it may disturb their main activity. To address this problem and avoid unauthorized access of ICT systems, many solutions based on *biometric continuous authentication* have been studied in the state of the art. Those solutions modify user identity verification from a one-shot procedure to a continuous process [1], [2]. In addition, with appropriate sensors and algorithms, biometric traits can be acquired transparently, thus avoiding reducing system's usability.

Demonstrating user involvement in the usage of a system or application can also be useful. In fact, when a controversy arises or a disaster happens people may try to deny their involvement and to repudiate their behavior. In those situations, 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 first year Ph.D. student for the upcoming years. 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 reliable security services for critical systems.

II. Biometric Continuous Authentication and the Control Room Operators Case Study

Human workers of control rooms are often responsible of executing critical commands, and in charge of managing privacy-sensitive information. The security of this workplace should be granted in order to prevent the intervention of insiders: they may benefit of their position in the control room to fool colleagues, and gain access to machines or accounts. In our previous work [3], we proposed an authentication system for deterring and detecting malicious access to the workstations of control rooms. Specifically tailored for people working in a crisis management system control room, the solution aims to guarantee authentication and, if possible, non-repudiation of operators, reducing the risk that unauthorized personnel (including intruders) misuse a workstation. We developed a continuous multi-biometric authentication mechanism in which biometric data is transparently acquired from the operator and continuously verified. More details about the protocol, the architecture, the algorithm for trust level computation, the prototype realized, and the software implemented can be found in [3].

A. Usability Assessment and Security Trade-offs

To investigate the usability of the system, we are conducting experiments involving a wide group of participants. The users will 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 when the user performs the initial authentication and when the session terminates unexpectedly. Similarly, we are interested in the time necessary to the authentication system to reject an impostor that gains possession of a workstation left unattended.

The *satisfaction* will be measured with a questionnaire we designed to gather users' opinions and comments about their interaction with the system. In addition to the usability assessment, we want to clarify if the *overhead* introduced by our 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 system's *configurations*, e.g. varying the trust threshold (the minimum trust level allowed to remain authenticated). Finally, we are going to conduct a threat analysis and risk assessment for the biometric continuous authentication protocol, to establish its strengths, weaknesses and consequently understand where improvements are needed.

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 addressing 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.

Repudiation can be defined as the denial in 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 [9], [10].

The motivation for non-repudiation services can be the possibility that involved entities may try to cheat each other. Non-repudiation services are usually applied in the transactions domain. However, there can be other scenarios in which non-repudiation may be useful. What the service should generate in all the scenarios is undeniable evidence that can be used if a dispute arises.

A. Biometrics Can Guarantee Non-Repudiation?

Despite biometric traits are sometimes presented in the computer security literature as an authentication factor that may solve the repudiation problem [4], [5], other works like [6], and [7] 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 [8].

Our idea is to study authentication and non-repudiation in order to provide them in different scenarios and eventually involving biometric traits.

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. In addition, we plan to identify mechanisms for providing non-repudiation, specific for various contexts and their related issues, requirements and involved entities.

Finally, another ongoing activity consists in 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.

Acknowledgments

This work has been supported by the European FP7-IRSES project DEVASSES.

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 et al., "Continuous and transparent user identity verification for secure internet services," *IEEE Transactions on Dependable and Secure Computing* 12.3 (2015): 270-283.

[3] E. Schiavone, A. Ceccarelli, and A. Bondavalli, "Continuous user identity verification for trusted operators in control rooms," International Conference on Algorithms and Architectures for Parallel Processing, pp. 187-200, 2015.

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

[5] H. Bidgoli, "Handbook of information security, Threats, Vulnerabilities, Prevention, Detection, and Management". vol. 3. 2006.

[6] 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.

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

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

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

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