Lecture Notes in Computer Science

The LNCS series reports state-of-the-art results in computer science research, development, and education, at a high level and in both printed and electronic form. Enjoying tight cooperation with the R&D community, with numerous individuals, as well as with prestigious organizations and societies, LNCS has grown into the most comprehensive computer science research forum available.

The scope of LNCS, including its subseries LNAI and LNBI, spans the whole range of computer science and information technology including interdisciplinary topics in a variety of application fields. The type of material published traditionally includes

- proceedings (published in time for the respective conference)
- post-proceedings (consisting of thoroughly revised final full papers)
- research monographs (which may be based on outstanding PhD work, research projects, technical reports, etc.)

More recently, several color-cover sublines have been added featuring, beyond a collection of papers, various added-value components; these sublines include

- tutorials (textbook-like monographs or collections of lectures given at advanced courses)
- state-of-the-art surveys (offering complete and mediated coverage of a topic)
- hot topics (introducing emergent topics to the broader community)

In parallel to the printed book, each new volume is published electronically in LNCS Online.

Detailed information on LNCS can be found at
www.springer.com/lncs

Proposals for publication should be sent to
LNCS Editorial, Tiergartenstr. 17, 69121 Heidelberg, Germany
E-mail: lncs@springer.com

ISSN 0302-9743

Lecture Notes in Computer Science
LNCS LNAI LNBI

springer.com

Gavrilova et al. (Eds.)

LNCS 3982

ICCSA 2006

Marina Gavrilova et al. (Eds.)

Computational Science and Its Applications – ICCSA 2006

International Conference
Glasgow, UK, May 2006
Proceedings, Part III

3 Part III

Springer

Lecture Notes in Computer Science 3982

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Marina Gavrilova Osvaldo Gervasi
Vipin Kumar C.J. Kenneth Tan
David Taniar Antonio Laganà
Youngsong Mun Hyunseung Choo (Eds.)

Computational Science and Its Applications – ICCSA 2006

International Conference
Glasgow, UK, May 8-11, 2006
Proceedings, Part III

Springer

Volume Editors

Marina Gavrilova
University of Calgary, Canada
E-mail: marina@cpsc.ucalgary.ca

Osvaldo Gervasi
University of Perugia, Italy
E-mail: ogervasi@computer.org

Vipin Kumar
University of Minnesota, Minneapolis, USA
E-mail: kumar@cs.umn.edu

C.J. Kenneth Tan
OptimaNumerics Ltd., Belfast, UK
E-mail: cjtan@optimanumerics.com

David Taniar
Monash University, Clayton, Autralia
E-mail: david.taniar@infotech.monash.edu.au

Antonio Laganà
University of Perugia, Italy
E-mail: lag@unipg.it

Youngsong Mun
SoongSil University, Seoul, Korea
E-mail: mun@computing.soongsil.ac.kr

Hyunseung Choo
Sungkyunkwan University, Suwon, Korea
E-mail: choo@ece.skku.ac.kr

Library of Congress Control Number: 2006925086

CR Subject Classification (1998): F, D, G, H, I, J, C.2-3

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-34075-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-34075-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11751595 06/3142 5 4 3 2 1 0

Preface

This five-volume set was compiled following the 2006 International Conference on Computational Science and its Applications, ICCSA 2006, held in Glasgow, UK, during May 8–11, 2006. It represents the outstanding collection of almost 664 refereed papers selected from over 2,450 submissions to ICCSA 2006.

Computational science has firmly established itself as a vital part of many scientific investigations, affecting researchers and practitioners in areas ranging from applications such as aerospace and automotive, to emerging technologies such as bioinformatics and nanotechnologies, to core disciplines such as mathematics, physics, and chemistry. Due to the shear size of many challenges in computational science, the use of supercomputing, parallel processing, and sophisticated algorithms is inevitable and becomes a part of fundamental theoretical research as well as endeavors in emerging fields. Together, these far-reaching scientific areas contributed to shaping this conference in the realms of state-of-the-art computational science research and applications, encompassing the facilitating theoretical foundations and the innovative applications of such results in other areas.

The topics of the refereed papers span all the traditional as well as emerging computational science realms, and are structured according to the five major conference themes:

- Computational Methods, Algorithms and Applications
- High-Performance Technical Computing and Networks
- Advanced and Emerging Applications
- Geometric Modeling, Graphics and Visualization
- Information Systems and Information Technologies

Moreover, submissions from 31 workshops and technical sessions in areas such as information security, mobile communication, grid computing, modeling, optimization, computational geometry, virtual reality, symbolic computations, molecular structures, Web systems and intelligence, spatial analysis, bioinformatics and geocomputations, are included in this publication. The continuous support of computational science researchers has helped ICCSA to become a firmly established forum in the area of scientific computing.

We recognize the contribution of the International Steering Committee and sincerely thank the International Program Committee for their tremendous support in putting this conference together, the near 800 referees for their diligent work, and the IEE European Chapter for their generous assistance in hosting the event.

We also thank our sponsors for their continuous support without which this conference would not be possible.

Finally, we thank all authors for their submissions and all invited speakers and conference attendants for making the ICCSA Conference truly one of the premium events on the scientific community scene, facilitating exchange of ideas, fostering new collaborations, and shaping the future of computational science.

May 2006

Marina L. Gavrilova
Osvaldo Gervasi

on behalf of the co-editors
Vipin Kumar
Chih Jeng Kenneth Tan
David Taniar
Antonio Laganà
Youngsong Mun
Hyunseung Choo

Organization

ICCSA 2006 was organized by the Institute of Electrical Engineers (IEE)(UK), the University of Perugia (Italy), Calgary University (Canada) and Minnesota University (USA).

Conference Chairs

Vipin Kumar (University of Minnesota, Minneapolis, USA), Honorary Chair
Marina L. Gavrilova (University of Calgary, Calgary, Canada), Conference Co-chair, Scientific
Osvaldo Gervasi (University of Perugia, Perugia, Italy), Conference Co-chair, Program

Steering Committee

Vipin Kumar (University of Minnesota, USA)
Marina L. Gavrilova (University of Calgary, Canada)
Osvaldo Gervasi (University of Perugia, Perugia, Italy)
C. J. Kenneth Tan (OptimaNumerics, UK)
Alexander V. Bogdanov (Institute for High Performance Computing and Data Bases, Russia)
Hyunseung Choo (Sungkyunkwan University, Korea)
Andres Iglesias (University of Cantabria, Spain)
Antonio Laganà (University of Perugia, Italy)
Heow-Pueh Lee (Institute of High Performance Computing, Singapore)
Youngsong Mun (Soongsil University, Korea)
David Taniar (Monash University, Australia)

Workshop Organizers

Applied Cryptography and Information Security (ACIS 2006)

Sherman S.M. Chow (New York University, USA)
Joseph K. Liu (University of Bristol, UK)
Patrick Tsang (Dartmouth College, USA)
Duncan S Wong (City University of Hong Kong, Hong Kong)

Approaches or Methods of Security Engineering (AMSE 2006)

Haeng Kon Kim (Catholic University of Daegu, Korea)
Tai-hoon Kim (Korea Information Security Agency, Korea)

Authentication, Authorization and Accounting (AAA 2006)
Haeng Kon Kim (Catholic University of Daegu, Korea)

Computational Geometry and Applications (CGA 2006)
Marina Gavrilova (University of Calgary, Calgary, Canada)

Data Storage Devices and Systems (DSDS 2006)
Yeonseung Ryu (Myongji University, Korea)
Junho Shim (Sookmyong Womens University, Korea)
Youjip Won (Hanyang University, Korea)
Yongik Eom (Seongkyunkwan University, Korea)

Embedded System for Ubiquitous Computing (ESUC 2006)
Tei-Wei Kuo (National Taiwan University, Taiwan)
Jiman Hong (Kwangwoon University, Korea)

4th Technical Session on Computer Graphics (TSCG 2006)
Andres Iglesias (University of Cantabria, Spain)
Deok-Soo Kim (Hanyang University, Korea)

GeoComputation (GC 2006)
Yong Xue (London Metropolitan University, UK)

Image Processing and Computer Vision (IPCV 2006)
Jiawan Zhang (Tianjin University, China)

Intelligent Services and the Synchronization in Mobile Multimedia Networks (ISS 2006)
Dong Chun Lee (Howon University, Korea)
Kuinam J Kim (Kyonggi University, Korea)

Integrated Analysis and Intelligent Design Technology (IAIDT 2006)
Jae-Woo Lee (Konkuk University, Korea)

Information Systems Information Technologies (ISIT 2006)
Youngsong Mun (Soongsil University, Korea)

Information Engineering and Applications in Ubiquitous Computing Environments (IEAUCE 2006)
Sangkyun Kim (Yonsei University, Korea)
Hong Joo Lee (Dankook University, Korea)

Internet Communications Security (WICS 2006)
Sierra-Camara Josè Maria (University Carlos III of Madrid, Spain)

Mobile Communications (MC 2006)
Hyunseung Choo (Sungkyunkwan University, Korea)

Modelling Complex Systems (MCS 2006)
John Burns (Dublin University, Ireland)
Ruili Wang (Massey University, New Zealand)

Modelling of Location Management in Mobile Information Systems (MLM 2006)
Dong Chun Lee (Howon University, Korea)

Numerical Integration and Applications (NIA 2006)
Elise de Doncker (Western Michigan University, USA)

Specific Aspects of Computational Physics and Wavelet Analysis for Modelling Suddenly-Emerging Phenomena in Nonlinear Physics, and Nonlinear Applied Mathematics (PULSES 2006)
Carlo Cattani (University of Salerno, Italy)
Cristian Toma (Titu Maiorescu University, Romania)

Structures and Molecular Processes (SMP 2006)
Antonio Laganà (University of Perugia, Perugia, Italy)

Optimization: Theories and Applications (OTA 2006)
Dong-Ho Lee (Hanyang University, Korea)
Deok-Soo Kim (Hanyang University, Korea)
Ertugrul Karsak (Galatasaray University, Turkey)

Parallel and Distributed Computing (PDC 2006)
Jiawan Zhang (Tianjin University, China)

Pattern Recognition and Ubiquitous Computing (PRUC 2006)
Jinok Kim (Daegu Haany University, Korea)

Security Issues on Grid/Distributed Computing Systems (SIGDCS 2006)
Tai-Hoon Kim (Korea Information Security Agency, Korea)

Technologies and Techniques for Distributed Data Mining (TTDDM 2006)
Mark Baker (Portsmouth University, UK)
Bob Nichol (Portsmouth University, UK)

Ubiquitous Web Systems and Intelligence (UWSI 2006)
David Taniar (Monash University, Australia)
Eric Pardede (La Trobe University, Australia)

Ubiquitous Application and Security Service (UASS 2006)
Yeong-Deok Kim (Woosong University, Korea)

Visual Computing and Multimedia (VCM 2006)
Abel J. P. Gomes (University Beira Interior, Portugal)

Virtual Reality in Scientific Applications and Learning (VRSAL 2006)
Osvaldo Gervasi (University of Perugia, Italy)
Antonio Riganelli (University of Perugia, Italy)

Web-Based Learning (WBL 2006)
Woochun Jun Seoul (National University of Education, Korea)

Program Committee

Jemal Abawajy (Deakin University, Australia)
Kenny Adamson (EZ-DSP, UK)
Srinivas Aluru (Iowa State University, USA)
Mir Atiqullah (Saint Louis University, USA)
Frank Baetke (Hewlett Packard, USA)
Mark Baker (Portsmouth University, UK)
Young-Cheol Bang (Korea Polytechnic University, Korea)
David Bell (Queen's University of Belfast, UK)
Stefania Bertazzon (University of Calgary, Canada)
Sergei Bespamyatnikh (Duke University, USA)
J. A. Rod Blais (University of Calgary, Canada)
Alexander V. Bogdanov (Institute for High Performance Computing and Data Bases, Russia)
Peter Brezany (University of Vienna, Austria)
Herve Bronnimann (Polytechnic University, NY, USA)
John Brooke (University of Manchester, UK)
Martin Buecker (Aachen University, Germany)
Rajkumar Buyya (University of Melbourne, Australia)
Jose Sierra-Camara (University Carlos III of Madrid, Spain)
Shyi-Ming Chen (National Taiwan University of Science and Technology, Taiwan)
YoungSik Choi (University of Missouri, USA)
Hyunseung Choo (Sungkyunkwan University, Korea)
Bastien Chopard (University of Geneva, Switzerland)
Min Young Chung (Sungkyunkwan University, Korea)
Yiannis Cotronis (University of Athens, Greece)
Danny Crookes (Queen's University of Belfast, UK)
Jose C. Cunha (New University of Lisbon, Portugal)
Brian J. d'Auriol (University of Texas at El Paso, USA)
Alexander Degtyarev (Institute for High Performance Computing and Data Bases, Russia)
Frederic Desprez (INRIA, France)
Tom Dhaene (University of Antwerp, Belgium)
Beniamino Di Martino (Second University of Naples, Italy)
Hassan Diab (American University of Beirut, Lebanon)
Ivan Dimov (Bulgarian Academy of Sciences, Bulgaria)
Iain Duff (Rutherford Appleton Laboratory, UK and CERFACS, France)
Thom Dunning (NCSA and University of Illinois, USA)
Fabrizio Gagliardi (Microsoft, USA)
Marina L. Gavrilova (University of Calgary, Canada)
Michael Gerndt (Technical University of Munich, Germany)
Osvaldo Gervasi (University of Perugia, Italy)
Bob Gingold (Australian National University, Australia)
James Glimm (SUNY Stony Brook, USA)

Christopher Gold (Hong Kong Polytechnic University, Hong Kong)
Yuriy Gorbachev (Institute of High Performance Computing and Information Systems, Russia)
Andrzej Goscinski (Deakin University, Australia)
Jin Hai (Huazhong University of Science and Technology, China)
Ladislav Hluchy (Slovak Academy of Science, Slovakia)
Xiaohua Hu (Drexel University, USA)
Eui-Nam John Huh (Seoul Women's University, Korea)
Shen Hong (Japan Advanced Institute of Science and Technology, Japan)
Paul Hovland (Argonne National Laboratory, USA)
Andres Iglesias (University of Cantabria, Spain)
Peter K. Jimack (University of Leeds, UK)
In-Jae Jeong (Hanyang University, Korea)
Chris Johnson (University of Utah, USA)
Benjoe A. Juliano (California State University at Chico, USA)
Peter Kacsuk (MTA SZTAKI Researc Institute, Hungary)
Kyung Wo Kang (KAIST, Korea)
Carl Kesselman (USC/ Information Sciences Institute, USA)
Daniel Kidger (Quadrics , UK)
Haeng Kon Kim (Catholic University of Daegu, Korea)
Jin Suk Kim (KAIST, Korea)
Tai-Hoon Kim (Korea Information Security Agency, Korea)
Yoonhee Kim (Syracuse University, USA)
Mike Kirby (University of Utah, USA)
Dieter Kranzlmueller (Johannes Kepler University Linz, Austria)
Deok-Soo Kim (Hanyang University, Korea)
Vipin Kumar (University of Minnesota, USA)
Domenico Laforenza (Italian National Research Council, Italy)
Antonio Laganà (University of Perugia, Italy)
Joseph Landman (Scalable Informatics LLC, USA)
Francis Lau (The University of Hong Kong, Hong Kong)
Bong Hwan Lee (Texas A&M University, USA)
Dong Chun Lee (Howon University, Korea)
Dong-Ho Lee (Institute of High Performance Computing, Singapore)
Sang Yoon Lee (Georgia Institute of Technology, USA)
Tae-Jin Lee (Sungkyunkwan University, Korea)
Bogdan Lesyng (ICM Warszawa, Poland)
Zhongze Li (Chinese Academy of Sciences, China)
Laurence Liew (Scalable Systems Pte, Singapore)
David Lombard (Intel Corporation, USA)
Emilio Luque (University Autonoma of Barcelona, Spain)
Michael Mascagni (Florida State University, USA)
Graham Megson (University of Reading, UK)
John G. Michopoulos (US Naval Research Laboratory, USA)
Edward Moreno (Euripides Foundation of Marilia, Brazil)

Youngsong Mun (Soongsil University, Korea)
Jiri Nedoma (Academy of Sciences of the Czech Republic, Czech Republic)
Genri Norman (Russian Academy of Sciences, Russia)
Stephan Olariu (Old Dominion University, USA)
Salvatore Orlando (University of Venice, Italy)
Robert Panoff (Shodor Education Foundation, USA)
Marcin Paprzycki (Oklahoma State University, USA)
Gyung-Leen Park (University of Texas, USA)
Ron Perrott (Queen's University of Belfast, UK)
Dimitri Plemenos (University of Limoges, France)
Richard Ramaroson (ONERA, France)
Rosemary Renaut (Arizona State University, USA)
Reneé S. Renner (California State University at Chico, USA)
Paul Roe (Queensland University of Technology, Australia)
Alexey S. Rodionov (Russian Academy of Sciences, Russia)
Heather J. Ruskin (Dublin City University, Ireland)
Ole Saastad (Scali, Norway)
Muhammad Sarfraz (King Fahd University of Petroleum and Minerals, Saudi Arabia)
Edward Seidel (Louisiana State University, USA and Albert-Einstein-Institut, Potsdam, Germany)
Jie Shen (University of Michigan, USA)
Dale Shires (US Army Research Laboratory, USA)
Vaclav Skala (University of West Bohemia, Czech Republic)
Burton Smith (Cray, USA)
Masha Sosonkina (Ames Laboratory, USA)
Alexei Sourin (Nanyang Technological University, Singapore)
Elena Stankova (Institute for High Performance Computing and Data Bases, Russia)
Gunther Stuer (University of Antwerp, Belgium)
Kokichi Sugihara (University of Tokyo, Japan)
Boleslaw Szymanski (Rensselaer Polytechnic Institute, USA)
Ryszard Tadeusiewicz (AGH University of Science and Technology, Poland)
C.J. Kenneth Tan (OptimaNumerics, UK and Queen's University of Belfast, UK)
David Taniar (Monash University, Australia)
John Taylor (Streamline Computing, UK)
Ruppa K. Thulasiram (University of Manitoba, Canada)
Pavel Tvrdik (Czech Technical University, Czech Republic)
Putchong Uthayopas (Kasetsart University, Thailand)
Mario Valle (Swiss National Supercomputing Centre, Switzerland)
Marco Vanneschi (University of Pisa, Italy)
Piero Giorgio Verdini (University of Pisa and Istituto Nazionale di Fisica Nucleare, Italy)
Jesus Vigo-Aguiar (University of Salamanca, Spain)

Jens Volkert (University of Linz, Austria)
Koichi Wada (University of Tsukuba, Japan)
Stephen Wismath (University of Lethbridge, Canada)
Kevin Wadleigh (Hewlett Packard, USA)
Jerzy Wasniewski (Technical University of Denmark, Denmark)
Paul Watson (University of Newcastle Upon Tyne, UK)
Jan Weglarz (Poznan University of Technology, Poland)
Tim Wilkens (Advanced Micro Devices, USA)
Roman Wyrzykowski (Technical University of Czestochowa, Poland)
Jinchao Xu (Pennsylvania State University, USA)
Chee Yap (New York University, USA)
Osman Yasar (SUNY at Brockport, USA)
George Yee (National Research Council and Carleton University, Canada)
Yong Xue (Chinese Academy of Sciences, China)
Igor Zacharov (SGI Europe, Switzerland)
Xiaodong Zhang (College of William and Mary, USA)
Aledander Zhmakin (SoftImpact, Russia)
Krzysztof Zielinski (ICS UST / CYFRONET, Poland)
Albert Zomaya (University of Sydney, Australia)

Sponsoring Organizations

Institute of Electrical Engineers (IEE), UK
University of Perugia, Italy
University of Calgary, Canada
University of Minnesota, USA
Queen's University of Belfast, UK
The European Research Consortium for Informatics and Mathematics (ERCIM)
The 6th European Framework Project "Distributed European Infrastructure for Supercomputing Applications" (DEISA)
OptimaNumerics, UK
INTEL
AMD

Table of Contents – Part III

Workshop on Approaches or Methods of Security Engineering (AMSE 2006, Sess. A)

General Tracks

Metrics of Password Management Policy

Carlos Villarrubia, Eduardo Fernández-Medina, and Mario Piattini

Alarcos Research Group,
Information Systems and Technologies Department,
UCLM-Soluziona Research and Development Institute,
University of Castilla-La Mancha,
Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
{Carlos.Villarrubia, Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Abstract. The necessity to management the computer security of an institution implies an evaluation phase and the most common method to carry out this evaluation it consists on the use of a set of metrics. As any system of information needs of an authentication mechanism being the most used one those based on password, in this article we propose a set of metric of password management policies based on the most outstanding factors in this authentication mechanism. Together with the metrics, we propose a quality indicator derived from these metrics that allows us to have a global vision of the quality of the password management policy used and a complete example of calculation of the proposed metric. Finally, we will indicate the future works to be performed to check the validity and usefulness of the proposed metrics.

Keywords: Security management, assurance, metrics, passwords.

1 Introduction

Information and its support processes together with systems and nets are important resources for any organization. These resources are continuously subjected to risks and insecurities coming from a great variety of sources, where there are threats based on malicious code, programming errors, human errors, sabotages or fires.

This concern has encouraged many organizations and researchers to propose several metrics to evaluate security of their information systems. In general, there is a consensus regarding the fact that choosing these metrics depends on the concrete security need of each organization. The majority of performed proposals put forward methods to choose these metrics [1, 4, 19, 22, 26, 27]. In addition, sometimes, it is suggested the need of developing specific methodologies for each organization [7].

In any proposal, the need is to quantify the different security aspects to be able to understand, control, and improve confidence in the information system.

If an organization does not use security metrics for its decision making process, the choices will be motivated by subjective aspects, external pressures and even purely commercial motivations.

With the purpose of systematizing all these proposals, we have developed a classification outline of security metrics [29] where the proposed metrics in the existing literature have been included. In our work, we will conclude that the majority

M. Gavrilova et al. (Eds.): ICCSA 2006, LNCS 3982, pp. 1013 – 1023, 2006.

of proposed metrics are general. This class of metrics only measure generic actions related to security and in an indirect way, specific objectives such as confidentiality, integrity and availability.

1.1 Authentication Systems

The use of an authentication system requires the integration of multiple elements; depending on the used techniques, it is necessary to use cryptography, medicine, psychology, systems analysis and protocol design. All authentication systems are designed to assure the identity of a participant to other participant and this process requires that the first participant demonstrates his identity according to any kind of information (knowledge evidence, possession evidence, and biological evidence). This authentication evidence can be a word or a password as it is used in the majority of operating systems and applications (knowledge evidence), a cryptographic card (possession evidence) or any biological characteristic of the individual to be authenticated and that is measured through a biometric device (biological evidence).

Historically, the use of a mechanism based on passwords has been the most used method. The importance of this authentication mechanism has led to the elaboration of rules and recommendations of multiple levels [11, 12, 13, 14, 20, 21]. The fact that this method is very easy to use in all systems together with its low cost has motivated this acceptation [18]. Deficiencies of this method have been widely studied and measures have been proposed to limit these disadvantages [2, 9, 23]. In some designs, the main disadvantages are linked to the necessary confidence in users when dealing with passwords while in other occasions, these disadvantages are motivated by designs that assumed a secure environment (such as, intranets) and that have been used in other environments (for example, the Internet) [10].

All these problems should indicate that passwords are a mechanism to be replaced but the users' acceptation of their use, their low cost together with the complexity and costs of the alternative methods guarantee their short and medium term continuance.

In this paper, we will propose metrics and indicators related to the password management policy due to the lack of specific proposals in special relevant areas in information system security.

In section 2, we will propose password management policy metrics justifying why they are necessary and classifying the proposed set according to several criteria. In section 3, we will put forward a classification according to levels of password management policies that allow organizations to know their current situation, to propose the relevant improvement and to relate comparisons between different institutions to know the best practices. Finally, we will present some of the obtained conclusions and a proposal of future work in this field.

2 Proposal of Password Management Metrics

The methodology used to derive the password management metrics has consisted on a study of all the factors that intervene in the password management. For this purpose, it has been gathered of the existent literature these factors [2,3,9,13,18,20,21]. These metrics do not try to cover the whole problem but to capture the most representative problems. In this hypothesis, it is not included the use of passwords for the authentication between processes or hosts. On the contrary, it is only studied the participation of a

person as an entity to be authenticated. Multifactor authentication systems where one of the authentication mechanisms is a password are not included either.

The definition of these metrics will be performed by defining the following aspects:

- *Name*: Representative name of the metric.
- *Description of the metric*: Generally, it describes the name of the metric by indicating the method to calculate values.
- *Life cycle phase*: For a better understandability and analysis of measures, metrics are classified according to their role within the life cycle of passwords.
  - *General*: Those metrics that could be in two or more phases are included.
  - *Assignment*: All metrics related to the assigning of initial identificators and passwords to the users are included.
  - *Storage*: It contemplates the problem of storing passwords by the system.
  - *Transmission*: It includes the metrics related to the authentication protocols used by the user or the communication of the password to the user by the authentication system.
  - *Use*: Metrics that measure the way of use of the password by the user.
  - *Renewal*: Area of metrics related to the password modification.
- *Scale*: Set of values associated of this metric.
- *Multivalue*: Some of this metrics are susceptible of having several simultaneous measures. With this attribute it is indicated if the metric can have or not several simultaneous measures.

The names, description of the metrics, life cycle phase and multivalue that we have considered are as follows:

Table 1. Password management metrics

Name	Description	Phase	Mult.
Users Training	Type of training received by users for dealing with and selecting, if it is the case, passwords.	General	Yes
Group Password	Existence of passwords used by a group of users or passwords necessary to access to resources that do not have an access control mechanism separated from the authentication mechanism.	General	No
Action Register	Type of register used by the information system to monitor the actions related to the password management.	General	Yes
Alphabet Size	Number of characters of the alphabet used for the creation of passwords valid in the system.	Assignment	No
Number of Different Classes Demanded	Number of classes which the alphabet is divided into and that are required to determine a valid password.	Assignment	No
Minimum Length	Number of minimum characters required for a valid password.	Assignment	No
Source Selection	Set of agents that can be used to choose a password.	Assignment	No
Selection Restriction	Set of restrictions that avoid that the selection source uses a password easy to be found out by third parties.	Assignment	Yes
User Identificator Class	Type of user identificator used by the system.	Assignment	No
Predefined Users	Treatment that predefined users receive from the system.	Assignment	Yes

Table 1. (*continued*)

Storage Class	Way of passwords storage in the authentication system.	Storage	Yes
Initial Communication	Method of communication of the initial password or a re-assignation of the user by the authentication system.	Transmission	Yes
Net Transmission	Mechanism of transmission used by the authentication protocol for the confidentiality and integrity of password.	Transmission	No
Input Visualization	Method used by the system for the visualization of the password when it is required to the user.	Use	No
Maximum Number of Erroneous Attempts	Maximum number of failed attempts before the authentication system makes a defense operation because of the risk of identity usurpation by a third party.	Use	No
Information about Use	Group of mechanisms used by the authentication system to inform the user about the authentications performed in the past.	Use	No
Authentication Period	Maximum time after which the access control asks for a user re-authentication.	Use	No
Block by User Cancellation	Procedures used to guarantee that users that were legitimate in the past, are avoided to access the system.	Renewal	No
Minimum Life Time	Minimum life time of a valid password.	Renewal	No
Maximum Life Time	Maximum life time of a valid password. When this time goes by, the user is forced to change the password.	Renewal	No
Record Length	Number of valid passwords used by the user in the past and that the system does not allow to reuse.	Renewal	No
Password Reassigning	Procedure used to reactivate the credential of a user that does not remember his password.	Renewal	No

3 Indicator of Level of Security in the Password Management

The definition of a set of metrics is not enough for an organization to be able to use them to manage the necessary changes in the field of those metrics. It is necessary to have information about the way of use and the impact of the values of the metrics on the system management.

With this objective, we have proposed some pre-established values for each metric that facilitates its use. Except for some of them, these values are ordered according to a hierarchy, starting by a minimum value to a maximum one, passing through intermediate values in the majority of metrics. When an organization has a superior value in each metric, it will have a higher confidence in its authentication system.

As a general principle of computer security, it is not generally adequate to increase the values in some metrics without a generalized increase in all of them. Taking this principle as an objective, it is proposed an indicator of quality of password management policy based on five levels. This proposal is based on the usefulness shown in the maturity models and in the metrics management programmes [5, 6, 8, 26].

These levels are structured from a minimum level (level 1) to a maximum level (level 5). The values required in each metric are defined in each level. In some of these metrics, it is also defined a recommended value for each level. These

recommendations have the purpose of providing the indicator with flexibility, making it possible to define the required values at the lowest possible measure in each level.

When a metric has several values demanded in a level, this indicates that all those values should be had to consider that level has been reached. When in a metric it is demanded the same values in several levels, it is considered that the metric is in the higher level.

Anyway, the character of having recommended in a value of a metric does not have influence in its level and only has meaning for the calculation of the value of the indicator of quality of password management like it is described later on this section. Finally, the value '+' it indicates that the value of that metric in that level is overcome because this metric have a bigger value that the one demanded or recommended for that level. Table 2 shows our analysis for each metric, considering the above-mentioned levels.

Table 2. Values of metric and associate level

Users Training (Multivalue)	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
No Training	Oblig.[1]				
Information when the user registration is made	Rec.[2]	Oblig.	Oblig.	Oblig.	Oblig.
Compulsory course	Rec.	Rec.	Rec.	Oblig.	Oblig.
Periodic course	+[3]	+	+	Rec.	Oblig.
Group Password	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Existence of group passwords or access to resources passwords	Oblig.				
Unique existence of a group of administrators	+	Oblig.	Oblig.		
There are not group passwords	+	+	Rec.	Oblig.	Oblig.
Action Register (Multivalue)	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
No action register	Oblig.				
Registration register	+	Oblig.	Oblig.	Oblig.	Oblig.
Renewal and cancellation register	+	Rec.	Oblig.	Oblig.	Oblig.
Block and re-assignation register	+	Rec.	Rec.	Oblig.	Oblig.
Alphabet Size	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Less than or equal to ten characters	Oblig.				
Between eleven and twenty-five characters	+	Oblig.			
Between twenty-six and fifty characters	+	Rec.	Oblig.		
Between fifty-one and seventy-five characters	+	+	Rec.	Oblig.	
More than seventy-five characters	+	+	Rec.	Rec.	Oblig.
Number of Different Classes demanded	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
One	Oblig.				
Two	+	Oblig.			
Three	+	+	Oblig.	Oblig.	
Four or more	+	+	+	Rec.	Oblig.
Minimum Length	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Less than or equal to four characters	Oblig.				
Between five and eight characters	+	Oblig.			
Between nine and twelve characters	+	+	Oblig.		
Between thirteen and sixteen characters	+	+	+	Oblig.	
Greater than sixteen characters	+	+	+	+	Oblig.

[1] Oblig. Obligatory value.
[2] Rec.: Recommended value.
[3] +: Overcome value in this level.

Table 2. (*continued*)

Source Selection	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
User	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
System	+	+	+	Rec.	Rec.
Selection Restriction (Multivalue)	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
No restriction					
User information	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Keys combinations	+	Rec.	Rec.	Oblig.	Oblig.
Dictionary password	+	+	Rec.	Oblig.	Oblig.
Variations of the previous ones	+	+	+	Rec.	Oblig.
User Identificator Class	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Public identificator	Oblig.	Oblig.	Oblig.		
Semi-public identificator	+	+	Rec.	Oblig.	
Private identificator	+	+	+	Rec.	Oblig.
Predefined Users (Multivalue)	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
No change					
Password change	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Identificator change	+	+	Rec.	Oblig.	Oblig.
Storage Class (Multivalue)	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Clear storage					
Irreversible storage	Oblig.	Oblig.	Rec.	Rec.	Rec.
Encrypted storage	+	+	Oblig.	Oblig.	Oblig.
Initial Communication (Multivalue)	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Non-secure transmission	Oblig.				
Transmission with compulsory change of password	+	Oblig.	Oblig.	Rec.	Rec.
Secure transmission	+	+	Rec.	Oblig.	Oblig.
Net Transmission	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Clear transmission					
Use of a challenge-response protocol	Oblig.	Oblig.	Oblig.		
Encrypted transmission	+	+	Rec.	Oblig.	Oblig.
Input Visualization	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Clear visualization					
Visualization of number of characters	Oblig.	Oblig.	Oblig.		
No visualization	+	+	Rec.	Oblig.	Oblig.
Maximum Number of Erroneous Authentication Attempts	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
No limit	Oblig.				
Between eleven and fifty attempts	Rec.	Oblig.			
Between four and ten attempts	+	Rec.	Oblig.	Oblig.	
Less than or equal to three attempts	+	+	+	Rec.	Oblig.
Information about Use	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
No information	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Information about the last use	+	+	Rec.	Rec.	Rec.
Authentication Period	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Work session	Oblig.	Oblig.			
Maximum of fifteen minutes inactivity	+	+	Oblig.	Oblig.	
Maximum of five minutes inactivity	+	+	+	Rec.	Oblig.
Block by User Cancellation	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Without an established method	Oblig.				
Periodic elimination (maximum of six months period)	Rec.	Oblig.	Oblig.		
Time limit established during registration	+	+	Rec.	Oblig.	Oblig.
Minimum Life Time	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
There is not minimum life time	Oblig.	Oblig.	Oblig.	Oblig.	
There is a minimum life time (equal to or greater than 1 day)	+	+	Rec.	Rec.	Oblig.

Table 2. (*continued*)

Maximum Life Time	Level 1	Level 2	Level 3	Level 4	Level 5
Greater than twelve months	Oblig.				
Lower than or equal to twelve months	+	Oblig.			
Lower than or equal to six months	+	+	Oblig.	Oblig.	
Lower than or equal to three months	+	+	+	Rec.	Oblig.
Record Length	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
One	Oblig.				
Lower than or equal to three	+	Oblig.			
Lower than or equal to ten	+	+	Oblig.		
Lower than or equal to twenty-five	+	+	+	Oblig.	
Greater than twenty-five	+	+	+	+	Oblig.
Password Reassigning	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
The previous password is reassigned	Oblig.				
A new password is assigned	Rec.	Oblig.	Oblig.	Oblig.	Oblig.

The calculation of the value of the indicator of quality of the password management policy requires them to be had as minimum the values of the metric ones with the requirement of obligatory, overcome or recommended. It is necessary to highlight that although the number of metric is twenty-two, the obtained values can be greater because several metric they can have several values simultaneously (for example, users training). The minimum number of values to reach the corresponding level is shown in the table 3.

Table 3. Number of values in each level

Level	Minimum number
1	22
2	22
3	23
4	28
5	30

3.1 Application of Metrics

In this section a concrete case of application of metric is detailed. The used system of information has the following characteristic: the new user is informed the password management policy and in the maximum term of one month he receives a formation session where aspects of computer security are included. The election of password carries out it the user with the following restrictions: 8 minimum characters of an alphabet with discrimination between uppercase and lowercase and with a mixture of digits. In the communication of the initial password to the user puts under an obligation to this to a change of password and these they are stored encrypted and using a dispersion function to be irreversible. These characteristics together with others that are deduced from the table 4 allow us to obtain the following values for the metric.

Table 4. Values of each metric in the example

Metric: Value	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Users Training: Information when the user registration is made	Rec.	Oblig.	Oblig.	Oblig.	Oblig.
Users Training: Compulsory course	Rec.	Rec.	Rec.	Oblig.	Oblig.
Group Password: Unique existence of a group of administrators	+	Oblig.	Oblig.		
Action Register : Registration register	+	Oblig.	Oblig.	Oblig.	Oblig.
Alphabet Size : More than seventy-five characters	+	+	Rec.	Rec.	Oblig.
Number of Different Classes demanded: Two	+	Oblig.			
Minimum Length: Between five and eight characters	+	Oblig.			
Source Selection: User	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Selection Restriction: User information	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
User Identificator Class: Public identificator	Oblig.	Oblig.	Oblig.		
Predefined Users: Password change	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Storage Class: Irreversible storage	Oblig.	Oblig.	Rec.	Rec.	Rec.
Storage Class: Encrypted storage	+	+	Oblig.	Oblig.	Oblig.
Initial Communication: Transmission with compulsory change of password	+	Oblig.	Oblig.	Rec.	Rec.
Net Transmission: Encrypted transmission	+	+	Rec.	Oblig.	Oblig.
Input Visualization: Visualization of number of characters	Oblig.	Oblig.	Oblig.		
Maximum Number of Erroneous Authentication Attempts: Between eleven and fifty attempts	Rec.	Oblig.			
Information about Use: No information	Oblig.	Oblig.	Oblig.	Oblig.	Oblig.
Authentication Period: Work session	Oblig.	Oblig.			
Block by User Cancellation: Periodic elimination (maximum of six months period)	Rec.	Oblig.	Oblig.		
Minimum Life Time: There is not minimum life time	Oblig.	Oblig.	Oblig.	Oblig.	
Maximum Life Time: Lower than or equal to twelve months	+	Oblig.			
Record Length: Lower than or equal to ten	+	+	Oblig.		
Password Reassigning: A new password is assigned	Rec.	Oblig.	Oblig.	Oblig.	Oblig.

With these measures the table 5 is obtained with a summary for level and for the obligatory, recommended or overcome character of each metric.

The table 4 shows that the used password management policy has the levels 1 and 2 because has all the required values. However, to obtain the level 3 he has to improve in four metrics: number of different classes demanded, minimum length,

Table 5. Values for level in the example

Total	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Obligatory value	9	18	16	13	12
Recommended value	4	2	4	3	2
Overcome value	11	4			
Total of values	24	24	20	16	13

authentication period and maximum life time. Finally, to reach the level 4 he needs to improve in eight metrics and for the level 5 in ten metrics.

4 Conclusions and Future Work

In this work, we have proposed a set of metric and an indicator of level of security in password management policy that they complete the objective of evaluating the authentication process through passwords.

We have proposed twenty-two metrics grouped into six areas covering the whole cycle of password management. Due to the diversity of these metrics, where some of them have a potentially infinite value range (for instance, password length) and others have a very limited value range (for instance, password reassignation), the definition of metrics includes a limited set of values that simplifies the process of obtaining measures and the use of metrics for decision making.

As a method of global valuation of the password management policy, it is proposed an indicator of quality whose range of values is formed by five levels. This indicator makes it possible to inform, in a single and comprehensible way, all actors involved in the organization security about the level of quality reached in an information system.

It is included one application example, a supposition where the level of each metric one is obtained together with the indicator of level of security of the whole group of metric. In this supposition we show the simplicity in the orientation to the manager to direct their future actions.

This proposal is made within the framework of a wider project of metrics definition that studies all security general areas. Nevertheless, in the area of identification and authentication, it is necessary to extend these metrics to the exploitation of the information system to complete the password management system.

Furthermore, the majority of organizations have a diversity of information systems with different requirements as well as different authentication mechanisms. To obtain an overall vision, through a set of metrics, it is necessary to combine all this information in a coherent and useful way for the organization board of directors and technical staff. In this aspect, the proposed metrics must be completed with others taking into account these circumstances.

Finally, we intend to be carried out like future works a study of the password management policy of a group of organizations selected to check the utility of the metric proposals, to validate the proposed group and to be a reference in best practices in this environment.

Acknowledgements

This research is part of the DIMENSIONS projects, partially financed by the FEDER and the Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha (PBC-05-012-1), CALIPO (TIC2003-07804-C05-03) and RETISTIC (TIC2002-12487-E) granted by the “Dirección General de Investigación del Ministerio de Ciencia y Tecnología” (Spain).

References

1. ACSA, editor. *Proceedings of the Workshop on Information Security System Scoring and Ranking*, Williamsburg, Virginia, may 2001.
2. A. Adams, M. A. Sasse, and P. Lunt. *Making passwords secure and usable*. In Proceedings of Human Computer Interaction, Bristol, England, aug 1997.
3. M. Bishop. *Comparing authentication techniques*. In Proceedings of the Third Workshop con Computer Incident Handling, pp. 1–10, aug 1991.
4. P. Bouvier and R. Longeon. *Le tableau de bord de la sécurité du système d'information*. Sécurité Informatique, jun 2003.
5. Carnegie Mellon University, Pittsburgh, Pennsylvania. *SSE-CMM Model Description Document, 3.0 edition*, jun 2003.
6. D. A. Chapin and S. Akridge. *How can security be measured?* Information Systems Control Journal, 2:43–47, 2005.
7. C. Colado and A. Franco. *Métricas de seguridad: una visión actualizada*. SIC. Seguridad en Informática y Comunicaciones, 57:64–66, nov 2003.
8. Departament of the Air Force. *AFI33-205. Information Protection Metrics and Measurements Program*, aug 1997.
9. A. Halderman, B. Waters, and E. W. Felten. *A convenient method for securely managing passwords*. In Proceedings of the 14th International World Wide Web Conference, pp. 471–479, Chiba, Japan, may 2005.
10. ISO. *ISO 7498-2. Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture*, 1989.
11. ISO/IEC. *ISO/IEC TR 13335-1. Guidelines for the Management of IT Security. Part I: Concepts and Models of IT Security*, 1996.
12. ISO/IEC. *ISO/IEC 15408. Evaluation Criteria for IT Security*, dec 1999.
13. ISO/IEC. *ISO/IEC 17799. Code of Practice for Information Security Management*, 2000.
14. G. King. *Best security practices: An overview*. In Proceedings of the 23rd National Information Systems Security Conference, Baltimore, Maryland, oct 2000. NIST.
15. J. M. Marcelo. *Seguridad de las Tecnologías de la Información, capítulo Identificación y Evaluación de Entidades en un Método AGR*, pp. 69–103. AENOR, 2003.
16. W. L. McKnight. *What is information assurance?* CrossTalk. The Journal of Defense Software Engineering, pp. 4–6, jul 2002.
17. R. T. Mercuri. *Analyzing security costs*. CACM, 46(6):15–18, jun 2003.
18. R. Morris and K. Thompson. *Password security: A case history*. CACM, 22(11):594–597, 1979.
19. F.Nielsen. *Approaches of security metrics*. Technical report, NIST-CSSPAB, jun 2000.
20. NIST. *FIPS-112: Password Usage*, may 1985.
21. NIST. *FIPS-181: Automated Password Generator*, oct 1993.
22. S. C. Payne. *A guide to security metrics*. Technical report, SANS Institute, jul 2001.
23. B. Pinkas and T. Sander. *Securing passwords against dictionary attacks*. In Proceedings of the ACM Computer and Security Conference (CSC' 02), pp. 161–170, nov 2002.
24. G. Schuedel and B. Wood. *Adversary work factor as a metric for information assurance*. In Procedings of the New Security Paradigm Workshop, pp. 23–30, Ireland, sep 2000.
25. M. Swanson. *Security self-assessment guide for information technology systems*. Tech. Report NIST 800-26, National Institute of Standards and Technology, nov 2001.
26. M. Swanson, N. Bartol, J. Sabato, . J. Hash, and L. Graffo. *Security metrics guide for information technology systems. Technical Report NIST 800-55*, National Institute of Standards and Technology, jul 2003.

27. R. B. Vaughn, Jr., R. Henning, and A. Siraj. *Information assurance measures and metrics – state of practice and proposed taxonomy*. In Proceedings of the 36th Hawaii International Conference on Systems Sciences, 2003.
28. R. B. Vaughn, Jr., A. Siraj, and D. A. Dampier. *Information security system rating and ranking*. CrossTalk. The Journal of Defense Software Engineering, pp. 30–32, may 2002.
29. C. Villarrubia, E. Fernández-Medina, and M. Piattini. *Towards a classification of security metrics*. In Proceedings of the 2nd international workshop on security in information systems (WOSIS 2004), pp. 342–350, apr 2004.