Proceedings

DEXA

ARES 2006

The First International Conference on Availability, Reliability and Security

20th-22nd April 2006 Vienna University of Technology, Austria

In Cooperation with

enisa European Network and Information Security Agency

TU WIEN Technische Universität Wien Vienna University of Technology

Oesterreichische Computer Gesellschaft Austrian Computer Society

Published by the IEEE Computer Society
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314

IEEE Computer Society Order Number P2567
Library of Congress Number Pending
ISBN 0-7695-2567-9

Proceedings

The First International Conference on Availability, Reliability and Security

ARES 2006

IEEE Computer Society Order Number P2567
ISBN 0-7695-2567-9
ISBN 978-0-7695-2567-9
Library of Congress Number 2006923025

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 800 272 6657
Fax: + 1 714 821 4641
http://computer.org/cspress
csbooks@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
http://shop.ieee.org/store/
customer-service@ieee.org

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Individual paper REPRINTS may be ordered at: <reprints@computer.org>

Editorial production by Bob Werner
Cover art production by Joe Daigle/Studio Productions
Printed in the United States of America by The Printing House

IEEE Computer Society
Conference Publishing Services
http://www.computer.org/proceedings/

Table of Contents: ARES 2006

First International Conference on Availability, Reliability and Security

Session 4: Protocol and Communication

Session 5: Security as Quality of Service

Session 6: Networking and Fault Tolerance

Session 7: Identification and Authentication

Session 8: High Availability and Dependability

Session 9: Reliability and Availability

Session 10: Security and Privacy Issue

Session 11: Security Management

Session 12: Distributed Systems

Session 13: Software Security and Dependability

International Symposium on Frontiers in Availability, Reliability and Security (FARES)

Session 1: IP Network and Adhoc Network

Session 2: Wireless and Sensor Network

Session 3: Authentication and Authorization

Session 4: Trust Management and Recovery

Session 5: Secure Information System

Session 6: Availability

Session 7: Software Security 1

Session 8: Software Security 2

Session 9: Safety and Security

Session 10: E-commerce and E-Government

Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2006)

Session 1: Construction of Dependable Overlay Networks

Session 2: Security

Session 3: Social Front

Workshop on Bayesian Networks in Dependability (BND2006)

Workshop on Dependability in Large-scale Service-oriented Systems (DILSOS)

Workshop: Security in E-Learning (SEL)

Workshop "Dependability Aspects on Data WArehousing and Mining Applications (DAWAM 2006)

Workshop on Bioinformatics and Security (BIOS 06)

Workshop: Information Security Risk Management (ISRM)

Workshop "Dependability and Security in e-Government" (DeSeGov 2006)

Message from the Organizing Committee

The idea for this conference came from the colleagues of the various ARES 2006 committees; our goal being to build a bridge amongst the various aspects of system dependability as an integrated concept.

The idea to launch the conference in Austria in the first half of the year 2006 has also to do with Austria's Presidency of the European Union from January to June 2006.

The European Union and the Austrian Governmental Bodies are very keen to bridge the gap between the scientific work and applications in this area — especially in the areas of e-Government.

We are very pleased therefore to have this conference organised in cooperation with ENISA (The European Network and Information Security Agency). ENISA supports the idea of this conference due to the urgent need of research and dissemination of new techniques in this key area.

We hope that the conference will have a real benefit for innovative applications which have to consider the various dependability issues, and furthermore will build a platform for in-depth discussions between researchers in the different areas of Dependability such as Availability, Reliability, and Security.

We received 159 papers from 35 countries for ARES and the Program Committee eventually selected 58 papers, making an acceptance rate of 36.47 percent of submitted papers.

Eight workshops are organised on special topics of ARES, i.e.:

- Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2006)
- Workshop on Bayesian Networks in Dependability (BND2006)
- Workshop on Dependability in Large-scale Service-oriented Systems (DILSOS)
- Workshop: Security in E-Learning (SEL)
- Workshop "Dependability Aspects on Data WArehousing and Mining Applications" (DAWAM 2006)
- Workshop on Bioinformatics and Security (BIOS 06)
- Workshop: Information Security Risk Management (ISRM)
- Workshop "Dependability and Security in e-Government" (DeSeGov 2006)

As an additional feature of ARES we have invited distinguished scientists for the International Symposium on Frontiers in Availability, Reliability and Security (FARES) to present and discuss special aspects relevant for future applications and research.

We would like to express our gratitude to all program committee members, workshop organisers and committee members and all the external referees who reviewed the papers very thoroughly and in a timely manner.

Due to the high number of submissions and the quality of the submitted papers, the reviewing, and discussion process was an extraordinarily challenging task. In total they have dealt with 232 papers.

Special thanks must be given to Mr. Tho Manh Nguyen for all his support in the organization of the PC-tasks of ARES 2006 and workshop coordination. We would also like to thank all the authors who submitted their papers to ARES 2006.

Finally many thanks to Ms. Christine Tronigger for providing a great deal of support in administering the registrations.

Prof. Norman Revell, Prof. Roland Wagner (Honorary Co-chairs)
Prof. Günther Pernul, Prof. Makoto Takizawa (General Co-chairs)
Prof. Gerald Quirchmayr, Prof. A Min Tjoa (Program Co.-chairs)

ARES and Workshops Committees

Honorary Co-Chairs
Norman Revell, Middlesex University, United Kingdom
Roland Wagner, University of Linz, Austria

General Co-Chairs
Guenther Pernul, University of Regensburg, Germany
Makoto Takizawa, Tokyo Denki University, Japan

Program Co-Chairs
Gerald Quirchmayr, University of Southern Australia, Australia
A Min Tjoa, Vienna University of Technology, Austria

Workshops Co-Chairs
Nguyen Manh Tho, Vienna University of Technology, Austria
Abdelkader Hameurlain, University of Toulouse, France
Leonard Barolli, Fukuoka Institute of Technology (FIT), Japan

International Liaison Chair
Maria Wimmer, University of Koblenz-Landau, Germany
Charles Shoniregun, University of East London, United Kingdom

Publicity Chair
Vladimir Marik, Czech Technical University, Czech Republic

Publication Chair
Monika Lanzenberger, Norwegian University of Science and Technology, Trondheim, Norway

Local Organizing Co-Chairs
Maria Schweikert, Vienna University of Technology, Austria
Markus Klemen, Vienna University of Technology, Austria

Program Committee

Jemal Abawajy, Deakin University, Australia
Abiola Abimbola, Napier University, UK
Rafael Accorsi, University of Freiburg, Germany
Alessandro Acquisti, Carnegie Mellon University, USA
John Andrews, Loughborough, University, UK
Lisa Bartlett, Loughborough University, UK
Elisa Bertino, Purdue University, USA
Bharat Bhargava, Purdue University, USA
Stefan Biffl, Vienna University of Technology, Austria
Michael Burmester, Florida State University, USA
Jiannong Cao, Hong Kong Polytechnic University, Hongkong, China
Jordi Castellà-Roca, Rovira i Virgili University of Tarragona
Anirban Chakrabarti, Infosys Technologies, India
Guihai Chen, Nanjing University, China
John A. Clark, University of York, UK
George Davida, University of Wisconsinat Milwaukee, USA
Pierpaolo Degano, Università diPisa, Italia
Robert Deng, Singapore Management University, Singapore
Yvo Desmedt, University College London, UK

Zoran Despotovic, DoCoMo Euro-Labs, Germany
Roger Dingledine, The Free Haven Project, USA
Paolo Donzelli, Office of the Prime Minister, Italy
Jeroen Doumen, University of Twente, Neitherland
Schahram Dustdar, Vienna University of Technology, Austria
Gerhard Eschelbeck, Webroot Inc., USA
Yung-Chin Fang, Dell Corp., USA
Pascal Felber, Université de Neuchâtel, Switzerland
Elena Ferrari, Universita' dell' Insubria, Italy
Jordi Forné, Universitat Politècnica de Catalunya, Spain
Felix C. Freiling, RWTH Aachen University, Germany
Steven Furnell, University of Plymouth, UK
Stephan Groß, Technische Universität Dresden, Germany
Daniel Grosu, Wayne State University, USA
Yong Guan, Iowa State University, USA
Ibrahim Haddad, Concordia University, Canada
Abdelkader Hameurlain, Université Paul Sabatier, France
Marit Hansen, Independent Centre for Privacy Protection Schleswig-Holstein Kiel, Germany
Naohiro Hayashibara, Tokyo Denki University, Japan
Xubin (Ben) He, Tennessee Technological University, USA
Yanxiang He, Wuhan University, China
Rattikorn Hewett, Texas Tech University, USA
Jimmy Huang, York University, Canada
Jan Jürjens, Munich University of Technology, Germany
Erland Jonsson, Chalmers University of Technology, Sweden
Oliver Jorns, ftw. Forschungszentrum Telekommunikation Wien, Austria
Audun Josang, University of Queensland, Australia
Yukiko Kawai, National Institute of Information and Communications Technology, Japan
Dogan Kesdogan, RWTH Aachen Informatik IV, Germany
Hiroaki Kikuchi, Tokai University, Japan
Hong Ong Oak, Ridge National Laboratory, USA
Seungjoo Kim, Sungkyunkwan University, Korea
Christian Kirchsteiger, European Commission
Peter Küng, Credit Suisse, Switzerland
Sy-Yen Kuo, National Taiwan UniversityTaiwan, R.O.C
Marc Lacoste, France Télécom Division R&D., France
Kwok-Yan Lam, Tsinghua University, China
Monika Lanzenberger, Norwegian University of Science and Technology, Trondheim, Norway
Chokchai (Box) Leangsuksun, Louisiana Tech University,USA
Yih-Jiun Lee, Chienkuo Technology University,Taiwan, R.O.C
Chin-Laung Lei, National Taiwan University, R.O.C
Chae Hoon Lim, Sejong University, Korea
Ching Lin, Macquarie University, Australia
Tong Liu, Dell Corp., USA
Javier Lopez, University of Malaga, Spain
Sanlu Lu, Nanjing University, China
Burgazzi Luciano, ENEA, Italy
Jianhua Ma, Hosei University, Japan
Josef Makolm, Federal Ministry of Finance, Austria
Geyong Min, University of Bradford, UK
Yi Mu, University of Wollongong, Australia
Günter Müller, Telematik Universitaet Freiburg, Germany
Junghyun Nam, Sungkyunkwan University, Korea
Tho Manh Nguyen, Vienna University of Technology, Austria
Jesper Buus Nielsen, Aarhus University, Denmark
Flemming Nielson, Technical University of Denmark, Denmark

Juan Gonzalez Nieto, Queensland University of Technology, Australia
Thomas Nowey, University of Regensburg, Germany
Manish Parashar, Rutgers University, USA
Fernando Pedone, Universita della Svizzera Italiana, Switzerland
María S. Pérez-Hernández, Universidad Politécnica de Madrid,Spain
Mario Piattini, University of Castilla La Mancha, Spain
Makan Pourzandi, Ericsson Inc.
Christopher Price, University of Wales Aberystwyth, UK
Philipp Reisner, MD at LINBIT Information Technologies GmbH, Austria
Heiko Rossnagel, Johann Wolfgang Goethe University Frankfurt, Germany
Bimal Roy, Indian Statistical Institute, India
Rei Safavi-Naini, University of Wollongong, Australia
Kenji Saito, Keio University, Japan
Kouichi Sakurai, Kyushu University, Japan
Henrique Santos, Universidade do Minho, Portugal
Stephen L. Scott, Oak Ridge National Laboratory
Jean-Marc Seigneur, University of Geneva, Switzerland
Ahmed Serhrouchni, Telecom Paris, France
Ingrid Schaumüller-Bichl, ITSB Linz, Austria
Charles Shoniregun, University of East London, UK
Amund Skavhaug, Norwegian University of Science and Technology (NTNU), Norway
Neal. A. Snooke, University of Wales Aberystwyth, UK
Ketil Stølen, SINTEF and University of Oslo, Norway
Peter Struss, Technische Universitat and Occ'm Sofwtare, Germany
Tsuyoshi Takagi, FutureUniversity – Hakodate, Japan
Makoto Takizawa, Tokyo Denki University, Japan
A Min Tjoa, Vienna University of Technology, Austria
Jorge Villar, Universitat Politècnica de Catalunya, Spain
Roland Wagner, University of Linz, Austria
Edgar Weippl, Vienna University of Technology, Austria
Chuan-Kun Wu, Chinese Academy of Sciences, China
Cheng-Zhong Xu, Wayne State University, USA
Mariemma I. Yagüe, University of Malaga, Spain
Laurence T. Yang, St.Francis Xavier University, Canada
Alec Yasinsac, Florida State University, USA
George Yee, National Research Council, Canada
Sung-Ming Yen, National Central University, Taiwan, R.O.C
Bill Yurcik, National Center for Supercomputing Applications (NCSA)
Nicola Zannone, University of Trento, Italy
Jianhong Zhang, North China University of Technology, China
Jianying Zhou, Institute for Infocomm Research, Singapore
Huafei Zhu, Institute for Infocomm Research, Singapore

Workshop on Dependable and Sustainable Peer-to-Peer Systems (DAS-P2P 2006)

Workshop Organizers
Yusuke Doi, Toshiba Corporation, Japan
Youki Kadobayashi, Nara Institute of Science and Technology, Japan
Kenji Saito, Graduate School of Media and Governance, Keio University, Japan

Program Committee
Stéphane Bressan, National University of Singapore, Singapore
Bernard Burg, Panasonic Research, USA
Ian Clarke, Freenet Project, UK
Roger Dingledine, The Free Haven Project, USA
Yusuke Doi, Toshiba Corporation, Japan (co-chair)
Claudiu Duma, Linköping University, Sweden
Debojyoti Dutta, University of Southern California, USA
Noria Foukia, University of Otago, New Zealand
Maria Gini, University of Minnesota, USA
Achmad Nizar Hidayanto, University of Indonesia, Indonesia
Sam Joseph, University of Hawaii, USA
Youki Kadobayashi, Nara Institute of Science and Technology, Japan (co-chair)
Anirban Mondal, University of Tokyo, Japan
Akiko Orita, Keio University, Japan
Omer F. Rana, Cardiff University, UK
Kenji Saito, Keio University, Japan (co-chair)
Claudio Sartori, University of Bologna, Italy
Nguyen Manh Tho, Vienna University of Technology, Austria
Sheng Zhong, State University of New York at Buffalo, USA

Workshop on Bayesian Networks in Dependability (BND2006)

Workshop Co-chairs
Stefania Montani, University of Piemonte Orientale
Hichem Boudali, University of Twente

Workshop Committee
Joanne Bechta Dugan, University of Virginia
Marc Bouissou, Electricite' de France
Helge Langseth, Sintef, Norway
Luigi Portinale, University of Piemonte Orientale
John L. Quigley, University of Strathclyde, Glasgow
Luis E. Sucar, Department of Computer Science, INAOE, Puebla, Mexico
Philippe Weber, Université Henri Poincaré, Nancy

Workshop on Dependability in Large-scale Service-oriented Systems (DILSOS 2006)

Program Chairs
Karl M. Göschka, Vienna University of Technology, Austria
Schahram Dustdar, Vienna University of Technology, Austria
Mehdi Jazayeri, University of Lugano, Switzerland

Organizational Chair
Martin Treiber, Vienna University of Technology, Austria

Program Committee
Marco Aiello, University of Trento, Italy
Mikio Aoyama, Nanzan University, Japan
Luciano Baresi, Politecnico di Milano, Italy
Boualem Benatallah, UNSW, Australia
Sara Bouchenak, University of Grenoble I, France
Sjaak Brinkkemper, Univ. of Utrecht, Netherlands
Tevfik Bultan, University of California, USA
Fabio Casati, HP, USA
Malu Castellanos, Hewlett-Packard, USA
Gianpaolo Cugola,, Italy
Harmke de Groot,, Netherlands
Asuman Dogac, METU, Turkey
Dieter Fensel, DERI, Ireland
Gianluigi Ferrari, University of Pisa, Italy
Jacqueline Floch, Sintef, Norway
Kary Fraemling, Helsinki University of Technology, Finland
Claude Godart, INRIA, France
Paul Grefen, Eindhoven Uni. of Technology, Netherlands
John Grundy, University of Auckland, New Zealand
Mohand-Said Hacid, Universite Claude Bernard Lyon, France
Manfred Hauswirth, EPFL, Switzerland
Alfons Kemper, TU Muenchen, Germany
Bernd Kraemer, University of Hagen, Germany
Frank Leymann, University of Stuttgart, Germany
Ozelin Lopez, ATOS Origin, Spain
Brahim Medjahed, University of Michigan, USA
Joachim Nern, Aspasia Systems, Germany
Beng Chin Ooi, National University of Singapore, Singapore
Maria Orlowska, UQ, Australia
Aris M. Ouksel, University of Illinois at Chicago, USA
Mike Papazoglou, Tilburg Univ., Netherlands
Jose Pereira, Universidade do Minho, Portugal
Barbara Pernici, Politecnico di Milano, Italy
Marco Pistore, Universita di Trento, Italy
Dimitris Plexousakis, FORTH, Greece
Alexander Romanovsky, University of Newcastle, UK
Anne-Marie Sassen, European Commission, EU
Vladimiro Sassone, University of Sussex, UK
Ian Sommerville, Lancaster University, UK
Jianwen Su, UCSB, USA
Katia Sycara, Carnegie Mellon University, USA
Stefan Tai, IBM Watson, USA
Paolo Traverso, ITC, Italy
Elena Troubitsyna, Aabo Akademi, Finland
Wil van der Aalst, Eindhoven University of Technology, Netherlands

Jos van Hillegersberg, Univ. of Twente, Netherlands
Steve Vinoski, IONA, USA
Martin Wirsing, Ludwig-Maximilians-University Munich, Germany
Jian Yang, Macuquarie University, Australia
Gianluigi Zavattaro, University of Bologna, Italy

Workshop: Security in E-Learning (SEL)

Program Chair
Edgar Weippl, Vienna University of Technology, Austria

Program Committee
Elke Franz, Dresden University of Technology, Germany
Gerald Quirchmayr, University of South Australia, Australia
Tomaz Klobucar, Jozef Stefan Institute, Slovenija
Günther Pernul, University of Regensburg, Germany

Workshop "Dependability Aspects on Data WArehousing and Mining Applications" (DAWAM 2006)

Organizer Co-chairs
Jimmy Huang, York University, Canada
Josef Schiefer, Senactive IT-Dienstleistungs GmbH, Austria
Nguyen Manh Tho, Vienna University of Technology, Austria

Program Committee
Jemal Abawajy, Deakin University, Australia
Aijun An, York University, Canada
Pawan Chowdhary, IBM T J Watson Research Center, USA
LiWu Chang, Naval Research Laboratory, USA
Josep Domingo-Ferrer, Rovira i Virgili University of Tarragona, Spain
Elena Ferrari, University of Insubria at Como, Italy
Ulrich Flegel, University of Dortmund, Germany
Tyrone Grandison, IBM Almaden Research, USA
Jimmy Huang, York University, Canada
Jun-Jang (JJ) Jeng, IBM T.J. Watson Research Center, USA
Hillol Kargupta, University of Maryland, Baltimore County, USA and Agnik, LLC
Zongwei Luo, University of Hong Kong, Hong Kong
Taneli Mielikäinen, University of Helsinki, Finland
Tho Manh Nguyen, Vienna University of Technology, Austria
Daniel E. O'Leary, University of Southern California, USA
Stanley Oliveira, Embrapa Information Technology, Brazil
Arnon Rosenthal, MITRE Corporation, USA
Josef Schiefer, Senactive IT-Dienstleistungs GmbH, Austria
Ben Soh, La Trobe University, Australia
David Taniar, Monash University, Australia
Juan Trujillo, University of Alicante, Spain
Vassilios S. Verykios, University of Thessaly, Greece
Justin Zhan, University of Ottawa, Canada
Sheng Zhong, State University of New York at Buffalo, USA

Workshop on Bioinformatics and Security (BIOS 06)

Workshop Chairs
Küng Josef, University of Linz, FAW Austria
Mazuran Petra, FAW, Austria
Wagner Roland, University of Linz, FAW Austria

Program Committee
Eisenacher Martin, University of Münster, Germany
Hochreiter Sepp, TU Berlin, Germany
Hof Sonja, (DWS) AG,Switzerland
Kramer Stefan, TUM, Germany
Marik Vladimir, Technical University Prag, Czech
Mazuran Petra, FAW, Austria
Palkoska Jürgen, FAW Austria
Retschitzegger Werner, University of Linz, Austria
Revell Norman, Middlesex University, UK
Tjoa A Min, Technical University of Vienna, Austria

Workshop: Information Security Risk Management (ISRM)

Workshop Chairs
Professor Dr. D. Karagiannis, University of Vienna, Austria
Dr. L. Marinos, ENISA, Greece

Program Committee
M. Dietrich, BSG Unternehmensberatung, Switzerland
M. Hoevers, ECP-NL, Platform voor eNetherland, The Netherland
K. Kalmelid, Swedish Emergency Management Agency, Sweden
S. Lebel, Dir. Centrale de la Sécurité des Systèmes d'information, France
Prof. Dr. G. Müller, Telematik, Univ. of Feiburg, Germany
M. Rohde, European Commission, DG Information Society and Media, Belgium
Dr. I. Schaumüller-Bichl, IT Security Consultant, Austria

Workshop "Dependability and Security in e-Government" (DeSeGov 2006)

Workshop Chairs
A Min Tjoa, Vienna University of Technology, Austria
Erich Schweighofer, University of Vienna, Austria

Program Committee
Peggy Agouris, University of Maine, USA
Yigal Arens, USC/Columbia University Digital Government Research Center, USA
Jon Bing, University of Oslo, Norway
Fernando Galindo, University of Zaragoza, Spain
Dieter Klumpp, Alcatel SEL Foundation, Germany
Robert Krimmer, Vienna University of Economics and Business Administration, Austria
Scott F. Midkiff, Virginia Polytechnic Institute and State University,USA
Enrico Nardelli, University of Rome TorVergata, Italy
Tho Manh Nguyen, Vienna University of Technology, Austria
Erich Schweighofer, University of Vienna, Austria
Efthimios Tambouris, CERTH/ITI, Greece
A Min Tjoa, Vienna University of Technology, Austria
Greg B. White, The University of Texas at San Antonio, USA
Maria A. Wimmer, University of Koblenz, Germany

Quality 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 use of passwords is the most common method to carry out the authentication of users in information systems. For this reason, quality in the password management is a need to reach reasonable levels in the typical objectives of security. In this paper, we propose a set of metrics of password 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. Finally, we will indicate the future works to be performed to check the validity and usefulness of the proposed metrics.

1. Introduction

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.

1.1 Security Metrics

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, 27, 28]. In addition, sometimes, it is suggested the need of developing specific methodologies for each organization [7].

0-7695-2567-9/06 $20.00 © 2006 IEEE

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 [30] where the proposed metrics in the existing literature have been included. In our work, we will conclude that the majority 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.

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. Password Policy Metrics

We will propose a series of metrics that try to cover the most relevant factors of password management taken from the study performed about the problem of password management. 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.

The name and description of the metrics we have considered are as follows:

- *Users Training*: Type of training received by users for dealing with and selecting, if it is the case, passwords.
- *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.
- *Action Registers*: Type of register used by the information system to monitor the actions related to the password management.
- *Alphabet Size*: Number of characters of the alphabet used for the creation of passwords valid in the system.
- *Number of Different Classes Demanded*: Number of classes which the alphabet is divided into and that are required to determine a valid password.
- *Minimum Length*: Number of minimum characters required for a valid password.
- *Selection Source*: Set of agents that can be used to choose a password.
- *Selection Restriction*: Set of restrictions that avoid that the selection source uses a password easy to be found out by third parties.
- *User Identificator Class*: Type of user identificator used by the system.
- *Predefined Users*: Treatment that predefined users receive from the system.
- *Storage phase*: Way of passwords storage in the authentication system.
- *Initial Communication*: Method of communication of the initial password or a re-assignation of the user by the authentication system.
- *Net Transmission*: Mechanism of transmission used by the authentication protocol for the confidentiality and integrity of password.
- *Input Visualization*: Method used by the system for the visualization of the password when it is required to the user.
- *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.
- *Information about Use*: Group of mechanisms used by the authentication system to inform the user about the authentications performed in the past.
- *Authentication Period*: Maximum time after which the access control asks for a user re-authentication.

0-7695-2567-9/06 $20.00 © 2006 IEEE

- *Block by User Cancellation*: Procedures used to guarantee that users that were legitimate in the past, are avoided to access the system.
- *Minimum Life Time*: Minimum life time of a valid password.
- *Maximum Life Time*: Maximum life time of a valid password. When this time goes by, the user is forced to change the password.
- *Record Length*: Number of valid passwords used by the user in the past and that the system does not allow to reuse.
- *Password Reassigning*: Procedure used to reactivate the credential of a user that does not remember his password.

The proposed metrics are divided into a set of areas that correspond to the different phases of the life cycle of passwords in the system.

The areas we have considered are as follows (see Table 1 to analyze the area for each metric):

- *General*: Those metrics that could be in two or more areas 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.

Metric	General	Assignment	Storage	Transmission	Use	Renewal
Users Training	√					
Group Password	√					
Action Register	√					
Alphabet Size		√				
Number of Different Classes Demanded		√				
Minimum Length		√				
Source Selection		√				
Selection Restriction		√				
User Identificator Class		√				
Predefined Users		√				
Storage Class			√			
Initial Communication				√		
Net Transmission				√		
Input Visualization					√	
Maximum Number of Erroneous Attempts					√	
Information about Use					√	
Authentication Period					√	
Block by User Cancellation						√
Minimum Life Time						√
Maximum Life Time						√
Record Length						√
Password Reassigning						√

Table 1. Classification of metrics according to areas

3. Security Levels

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, 27].

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. Table 2 shows our analysis for each metric, considering the above-mentioned levels.

Users Training	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
No Training	√				
Information when the user registration is made	Rec.[1]	√	√	√	√
Compulsory course	Rec.	Rec.	Rec.	√	√
Periodic course				Rec.	√
Group Password	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Existence of group passwords or access to resources passwords	√				
Unique existence of a group of administrators		√	√		
There are not group passwords			Rec.	√	√
Action Register	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
No action register	√				
Registration register		√	√	√	√
Renewal and cancellation register		Rec.	√	√	√
Block and re-assignation register		Rec.	Rec.	√	√
Alphabet Size	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Less than or equal to ten characters	√				
Between eleven and twenty-five characters		√			
Between twenty-six and fifty characters		Rec.	√		
Between fifty-one and seventy-five characters			Rec.	√	
More than seventy-five characters			Rec.	Rec.	√
Number of Different Classes demanded	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
One	√				
Two		√			
Three			√	√	
Four or more				Rec.	√
Minimum Length	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Less than or equal to four characters	√				
Between five and eight characters		√			
Between nine and twelve characters			√		
Between thirteen and sixteen characters				√	
Greater than sixteen characters					√
Source Selection	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
User	√	√	√	√	√
System				Rec.	Rec.
Selection Restriction	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
No restriction					
User information	√	√	√	√	√
Keys combinations		Rec.	Rec.	√	√
Dictionary password			Rec.	√	√
Variations of the previous ones				Rec.	√
User Identificator Class	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Public identificator	√	√	√		
Semi-public identificator			Rec.	√	
Private identificator				Rec.	√

[1] Rec.: Recommended

Predefined Users	Level 1	Level 2	Level 3	Level 4	Level 5
No change					
Password change	√	√	√	√	√
Identificator change			Rec.	√	√
Storage Class	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Clear storage					
Irreversible storage	√	√	Rec.	Rec.	Rec.
Encrypted storage			√	√	√
Initial Communication	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Non-secure transmission	√				
Transmission with compulsory change of password		√	√	Rec.	Rec.
Secure transmission			Rec.	√	√
Net Transmission	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Clear transmission					
Use of a challenge-response protocol	√	√	√		
Encrypted transmission			Rec.	√	√
Input Visualization	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Clear visualization					
Visualization of number of characters	√	√	√		
No visualization			Rec.	√	√
Maximum Number of Erroneous Authentication Attempts	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
No limit	√				
Between eleven and fifty attempts	Rec.	√			
Between four and ten attempts		Rec.	√	√	
Less than or equal to three attempts				Rec.	√
Information about Use	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
No information	√	√	√	√	√
Information about the last use			Rec.	Rec.	Rec.
Authentication Period	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Work session	√	√			
Maximum of fifteen minutes inactivity			√	√	
Maximum of five minutes inactivity				Rec.	√
Block by User Cancellation	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Without an established method	√				
Periodic elimination (maximum of six months period)	Rec.	√	√	√	√
Time limit established during registration			Rec.	√	√
Minimum Life Time	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
There is not minimum life time	√	√	√	√	
There is a minimum life time (equal to or greater than 1 day)			Rec.	Rec.	√
Maximum Life Time	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Greater than twelve months	√				
Lower than or equal to twelve months		√			
Lower than or equal to six months			√	√	
Lower than or equal to three months				Rec.	√
Record Length	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
One	√				
Lower than or equal to three		√			
Lower than or equal to ten			√		
Lower than or equal to twenty-five				√	
Greater than twenty-five					√
Password Reassigning	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
The previous password is reassigned	√				
A new password is assigned	Rec.	√	√	√	√

Table 2. Values according to the level of each metric.

The calculation of the value of the indicator of quality of the password management policy requires that the metrics values fulfil at least the "demanded" requirement, and a minimum of values of these metrics must fulfil the recommended value too. The minimum

number of recommended values according to levels is shown in Table 3.

Level	Minimum number
1	3
2	3
3	8
4	7
5	2

Table 3. Minimum number of metrics with recommended values

3.1. Protection of Personal Data

The use of metrics and computer security indicators allow organizations to materialize their security objectives without a considerable effort. For example, in Spain, any organization from the public or the private sector must comply with the Real Decreto 994/1999 of 11th June that approves the regulation of security measures of the automated files containing personal data [24].

In this regulation, files are classified into three levels: basic, intermediate and high. Such levels are established according to the nature of the studied information, in relation to the higher or lower need to guarantee information confidentiality and integrity.

For low level files, article 11, in sections two and three, establishes that when the authentication mechanism is based on the existence of passwords, there will be an assignation, distribution and storage process that guarantee confidentiality and integrity. At the same time, passwords will be periodically changed according to the period of time established in the security document and, while they are valid they will be stored in a comprehensible way. Level 1 of our indicator of quality of password management policy widely fulfils these requirements.

Regarding intermediate level files, together with the security measures applicable to the low level files, complementary measures must be applied. Regarding identification and authentication, article 18 establishes that the person in charge of the file will establish a mechanism that allows the unequivocal identification of any user trying to access the information system and that the verification is authorized. In addition, the possibility of trying the non authorized access to the information system several times will be limited. In our case, Level 2 fulfils these requirements offering additional guarantees.

4. Conclusions and Future Work

The need to manage information systems security forces us to use metrics and indicators that allow us to evaluate the real situation. In this work, we have proposed a set of metrics and password management policy indicators that fulfil this requirement in a practically generalized scope in any information system, 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 re-assignation), 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.

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.

5. 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).

6. 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] Real Decreto 994/1999, de 11 de junio, que aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal, jun 1999.

[25] 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.

[26] M. Swanson. Security self-assessment guide for information technology systems. Tech. Report NIST 800-26, National Institute of Standards and Technology, nov 2001.

[27] 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.

[28] 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.

[29] 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.

[30] 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.