01CH37186

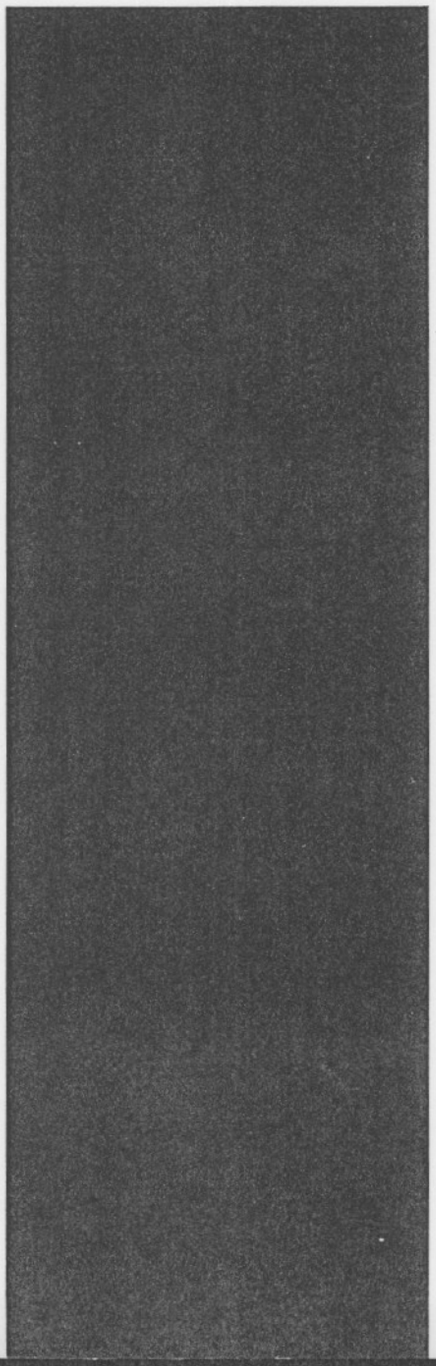
Proceedings

THE INSTITUTE OF ELECTRICAL
AND ELECTRONICS ENGINEERS

35th ANNUAL
2001 International Carnahan Conference on Security Technology

October 16 - 19, 2001

LONDON, ENGLAND



Sponsored by:

- IEEE Lexington Section, USA
- IEEE Aerospace and Electronic Systems Society, USA
- Chung Shan Institute of Science & Technology, Taiwan, ROC
- National Chiao-Tung University Taiwan, ROC

EDITOR
LARRY D. SANSON

01CH37186

Proceedings

THE INSTITUTE OF ELECTRICAL
AND ELECTRONICS ENGINEERS

35th ANNUAL
2001 International Carnahan Conference on Security Technology

October 16 - 19, 2001

LONDON, ENGLAND

Sponsored by:

- IEEE Lexington Section, USA
- IEEE Aerospace and Electronic Systems Society, USA
- Chung Shan Institute of Science & Technology, Taiwan, ROC
- National Chiao-Tung University Taiwan, ROC

EDITOR
LARRY D. SANSON

Additional Records are available from:

IEEE Service Center
445 Hoes Lane
Piscataway, New Jersey 08854

IEEE Catalog Number 01CH37186
Library of Congress Number 79-644630

ISBN (Softbound) 0-7803-6636-0
ISBN (Microfiche) 0-7803-6637-9

Executive Committee Emeritus

In recognition of their past effort and service devoted to the IEEE International Carnahan Committee on Security Technology, this record of the Proceedings is gratefully dedicated to:

Thomas M. Andrews	—	Attorney General's Department
William D. Barkhau	—	Sylvania Electronic Systems
Benjamin Barker	—	U.S. Army Belvoir R&D Command
Cheryl C. Banks	—	University of Kentucky
Richard J. Blackwell	—	Jet Propulsion Laboratory
David K. Blythe	—	University of Kentucky
Albert C. Brooks	—	Inmont Corporation
Ernst Bunge	—	Bundeskriminalamt, Germany
George C. Byrne	—	SRI International
M. Bruce Carpenter	—	General Electric Aerospace
W. Donald Dodd	—	AESS/IEEE
Tandy Y. Haggard	—	IBM Corporation
Kenneth Hopper	—	Bellcore
John S. Jackson	—	University of Kentucky
Walter S. Konar	—	Stanford University
T.G. Krebs	—	South Central Bell
Benjamin Leon	—	University of Kentucky
Ron McGill	—	Lexington Fayette-Urban-Police
Sue McWain	—	University of Kentucky
Sanford A. Mullings	—	Jamaica Constabulary Office
Richard M. Neal	—	Kentucky Utilities Company
Russell E. Puckett	—	University of Kentucky
Alan N. Rapsey	—	United Kingdom Home Office
John A. Russell	—	Union Carbide Corporation
Guy H. Smith	—	Radiation, Inc.
Earl L. Steele	—	University of Kentucky
Ralph J. Summers	—	Sylvania Electronic Systems
Louis L. Taylor	—	Bernard Johnson Engineering
Carmen J. Tona	—	Consultant

Their professional contributions have so greatly advanced the technology of crime countermeasures and the many years of effort committed to the success of these conferences. Emeritus status is granted to the above persons, which provides complimentary registration to all functions of IEEE International Carnahan Conferences on Security Technology.

Committees

ICCST Executive Committee

Alfonso Bilbao, Securitas Seguridad España, Spain

Pong-Fui Chang, Microelectronics Technology, Inc., New Zealand

Hsia-Ling Chiang, National Central University Chung-Li, Taiwan, ROC

Ron Clifton, International Datacasting, Canada

Nigel Custance, Home Office, UK

Pieter de Bruyne, Consultant, Switzerland

Gene Greneker, Georgia Tech Research Institute, USA

Nigel Grist, Attorney General's Office, Australia

Michael Jonckheere, Correctional Service, Canada

Henry Kluepfel, Science Applications International Corp., USA

Richard T. Lazarick, Federal Aviation Administration, USA

Gerald Levett, G. Levett and Associates, Canada

Dan Pritchard, Sandia National Laboratories, USA

Larry Sanson, Consultant, USA

Clifton L. Smith, Edith Cowan University, Australia

G. Dan Smith, US Department of Energy, USA

Gordon Thomas, Police Scientific Development Branch, UK

John Veatch, SAIC, Board of Governors, AESS/IEEE, USA

So-Lin Yen, Ministry of Justice, Taiwan, ROC

Estelle Zannes, University of New Mexico, USA

Organizing Committee

Nigel Custance, Conference Chairperson, in conjunction with colleagues and the Institute of Civil Engineers' Conference Office

International Advisory Committee

Alfonso Bilbao, Securitas Seguridad España, Spain

Pong-Fui Chang, Microelectronics Technology, Inc., New Zealand

Hsia-Ling Chiang, National Central University Chung-Li, Taiwan, ROC

Jiro Chiba, Tohoku University, Sendai, Japan

Ron Clifton, International Datacasting, Canada

Nigel Custance, Home Office, UK

Pieter de Bruyne, Consultant, Switzerland

R. Deng, National University of Singapore, Singapore

R. Govaerts, Katholieke Universiteit Leuven, Belgium

Gene Greneker, Georgia Tech Research Institute, USA

Nigel Grist, Attorney General's Department, Australia

Michael Jonckheere, Correctional Services, Canada

Milõs Klíma, Czech Technical University, Czech Republic

Henry Kluepfel, Science Applications International Corp., USA

Richard T. Lazarick, Federal Aviation Administration, USA

Gerald Levett, G. Levett and Associates, Canada

Peter C. K. Liu, Hong Kong Polytechnic, Hong Kong

H. Luck, Duisburg University, Germany

Dan Pritchard, Sandia National Laboratories, USA

Max Robinson, The Nottingham Trent University, UK

Larry Sanson, Consultant, USA

Clifton L. Smith, Edith Cowan University, Australia

G. Dan Smith, US Department of Energy, USA

Gordon Thomas, Police Scientific Development Branch, UK

John Veatch, SAIC, Board of Governors, AESS/IEEE, USA

C. W. Wannerskog, AB DETEKTOR, Sweden

So-Lin Yen, Ministry of Justice, Taiwan, ROC

Estelle Zannes, University of New Mexico, USA

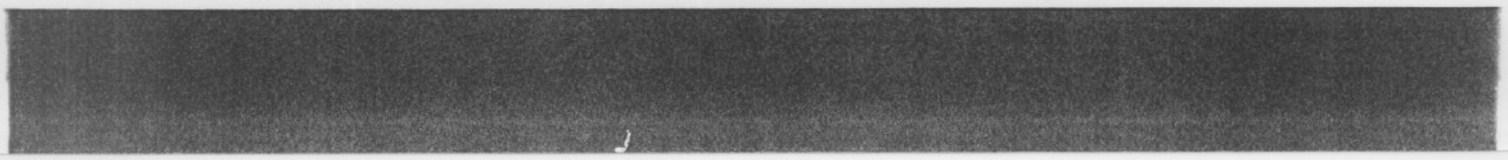


Table of Contents

Wednesday, October 17, 2001

KEYNOTE ADDRESS
Telford Theatre
10.00 - 10.30

Lord Mackenzie of Framwellgate; OBE

SECURITY AND POLICY MANAGEMENT 1
Telford Theatre
11.00 - 12.15

Moderator: Gerry Levett
G. Levett & Associates, Canada

US Department of Energy Security Technologies 19
G. D. Smith, C. J. Piechowski, C. A. Procratsky, M. H. Sparks, *USA*

The Management of Threat Events 27
K. Pearson, *UK*

A New Approach to Security Engineering 34
Major A. H. Hay, *UK*

SECURITY AND POLICY MANAGEMENT 2
Telford Theatre
13.45 - 15.25

Moderator: Michael Jonckheere
Correctional Services, Canada

Public Policing and Private Security: A Changing Balance Not Published
A. Willis, *UK*

Computer Assistance to Communication and Co-ordination During Emergencies 42
C. Ledger, B. Turner, *UK*

Convergence and Synergy: Joining up the Criminal Justice System Not Published
A. Lindfield, *UK*

Do End Users Get the Detection Systems That They Need? Not Published
B. Halkett, *UK*

FACILITY SECURITY 1

Telford Theatre
15.55 - 17.10

Moderator: Estelle Zannes
University of New Mexico, USA

Secured by Design — Not Published
R. P. Kelly, *UK*

Secured by Design – Learning from the Past to Secure the Future! — 45
T. Pascoe, *UK*

The Use of Automatic Number Plate Recognition Reading in Managing Access to The Boots Company Headquarter Site — 52
S. Davidson, *UK*

Vehicle Barriers – Development of a Model and Standard — 54
W. H. T. Spaight, *UK*

The Use of Active Seal Technology at the Y-12 National Security Complex — Not Published
C. A. Pickett, Z. W. Bell, G. D. Richardson, J. R. Younkin, *USA*

Thursday, October 18, 2001

Please note: Parallel sessions throughout the day

Session A – Telford Theatre

FACILITY SECURITY 2

09.00 - 10.40

Moderator: Dan Smith
US Department of Energy, USA

Site Access Management Systems – A Technical Systems Overview — Not Published
G. A. Douglas, *UK*

Rapid Data Collection at Major Incident Scenes Using Three Dimensional Laser Scanning Techniques — 60
P. Forman, I. Parry, *UK*

Vehicle Bomb Blast Effects and Countermeasures — 68
J. W. James, T. M. Wood, E. M. Kruse, J. D. Veatch, *USA*

m-Security (Security and Mobile Telephone) — 76
A. Bilbao, E. Pedrosa, *Spain*

TRANSPORT SECURITY
11.10 - 12.50

Moderator: Jack Veatch
SAIC, Board of Governors, AESS/IEEE, USA

Applications of Technology in Airport Access Control 85
R. Lazarick, *USA*

Test and Evaluation for Determining Screener Training Effectiveness 96
B. A. Klock, J. Rubinstein, *USA*

Remote Air Sampling for Canine Olfaction 100
B. Wickens, *UK*

Multiple View Dual-Energy X-Ray Imaging 103
J. P. O. Evans, M. Robinson, H. W. Hon, *UK*

INFORMATION PROCESSING FOR SECURITY AND LAW ENFORCEMENT
14.00 - 15.15

Moderator: Gene Greneker
Georgia Tech Research Institute, USA

Objective and Subjective Image Quality Evaluation for Security Technology 108
M. Klima, J. Pazderak, M. Bernas, P. Pata, J. Hozman, K. Roubik,
Czech Republic

Multi-Dimensional Cluster Analysis of Class Characteristics for Ballistics Specimen Identification 115
C. L. Smith, *Australia*

Historical Alarm and Near-Realtime Facility Data Analysis 122
D. A. Pritchard, D. G. Adams, *USA*

SECURITY SENSORS
15.45 - 17.25

Moderator: Ron Clifton
International Datacasting, Canada

IntelliFIBER™ – The Next Generation Fiber Optic Fence Sensor 128
F. Kapounek, M. Maki, *USA*

Intrepid Monostatic Microwave Radar Putting Ranging Back into Radar 136
E. Foley, K. Harman, J. Cheal, *USA*

Advantages of a Low Impedance Linear Magnetic Microphonic Sensor Cable 307
I. Macalindin, *UK*

Recent Development of Fibre Optic Sensors for Perimeter Security 142
M. Szustakowski, W. Ciurapinski, N. Palka, *Poland*

Session B – Godfrey Mitchell Theatre

INFORMATION SYSTEMS, SECURITY AND CRYPTOGRAPHY 1
09.00 - 10.15

Moderator: So-Lin Yen
Ministry of Justice, Taiwan, ROC

One-Time Installation with Traitors Tracing for Copyright Programs 149
C. H. Lin, C. Y. Lee, *Taiwan*

Secure Information by Using Digital Data Embedding and Spread Spectrum Techniques 156
C. L. Tsai, K. C. Fan, C. D. Chung, *Taiwan*

Specification of Security Constraint in UML 163
E. Fernandez-Medina, M. G. Piattini, M. A. Serrano, *Spain*

Outdoor Passive Millimeter Wave Security Screening 172
G. N. Sinclair, R. N. Anderton, R. Appleby, *UK*

INFORMATION SYSTEMS, SECURITY AND CRYPTOGRAPHY 2
10.45 - 12.00

Moderator: Gordon Thomas
Police Scientific Development Branch, UK

A Vehicle Identification Scheme Based in Cryptography Not Published
A. Mana, J. Lopez, J. J. Ortega, F. Perea, *Spain*

The Design of Protocol for e-Voting on the Internet 180
J. K. Jan, Y. Y. Chen, Y. Lin, *Taiwan*

Printers are Dangerous 190
J. C. Hernandez, J. M. Sierra, A. Gonzalez-Tablas, A. Orfila, *Spain*

INFORMATION SYSTEMS, SECURITY AND CRYPTOGRAPHY 3
13.30 - 15.15

Moderator: Hank Kleupfel
Science Applications International Corp., USA

Achieving Security in Integrated Circuit Card Applications: Reality or Desire? 197
R. Sanchez-Reillo, *Spain*

Authorization in Data Management Systems 202
D. Raymond, *Canada*

Elliptic Curve Cryptosystems on Smart Cards 213
E. Mohammed, A. E. Emarah, K. El-Shennawy, *Egypt*

FRIARS: A Feedback Control System for Information Assurance Using a Markov Decision Process 223
J. McInerey, S. Subberud, S. Anwar, S. Hamilton, *USA*

INFORMATION SYSTEMS, SECURITY AND CRYPTOGRAPHY 4

15.45 - 17.00

Moderator: Dan Prichard
Sandia Laboratory, USA

The Rijndael Block Cipher (AES Proposal): A Comparison with DES 229
C. Sanchez-Avila, R. Sanchez-Reillo, *Spain*

Adding Security and Privacy to Agents Acting in a Marketplace: A Trust Model 235
S. Robles, J. Borrell, *Spain;* S. Poslad, J. Bigham, *UK*

Using Classifiers to Predict Linear Feedback Shift Registers 240
J. C. Hernandez, P. Isasi, J. M. Sierra, B. Ramos, *Spain;* C. Mex-Perera, *UK*

Friday, October 19, 2001

BIOMETRIC TECHNOLOGIES AND TECHNIQUES 1

Telford Theatre
09.00 - 10.40

Moderator: Clifton Smith
Edith Cowan University, Australia

Fingerprint Verification Using Smart Cards for Access Control Systems 250
R. Sanchez-Reillo, C. Sanchez-Avila, *Spain*

High Confidence Recognition of Persons by Their Iris Patterns 254
J. Daugman, *UK*

Minutiae Detection Algorithm for Fingerprint Recognition 264
V. Espinosa-Duro, *Spain*

Handwritten Signatures Recognizer by Its Envelope and Strokes Layout Using HMM's 267
J. A. Sanchez, C. M. Travieso, I. G. Alonso, M. A. Ferrer, *Spain*

BIOMETRIC TECHNOLOGIES AND TECHNIQUES 2

Telford Theatre
11.10 - 12.25

Moderator: Alfonso Bilbao
Securitas Seguridad España, Spain

Iris Recognition for Biometric Identification Using Dyadic Wavelet Transform Zero-Crossing 272
D. de Martin-Roche, C. Sanchez-Avila, R. Sanchez-Reillo, *Spain*

A Multi-Resolutional Face Verification System via Filter-Based Integration 278
C. C. Han, C. L. Tsai, *Taiwan*

Interpreting the Results of the Biometric Working Group Test Programme Not Published
T. Mansfield, *UK*

ADDITIONAL PAPERS TO BE PRESENTED

Application of an Explosive Detection Device Based on Quadrupole Resonance (QR) Technology in Aviation Security 282
E. Rao, *USA*

How to Distinguish Between a Block Cipher and a Random Permutation by Lowering the Input Entropy 289
J. C. Hernandez, P. Isasi, J. M. Sierra, A. Gonzalez-Tablas, *Spain*

Home Security System and CATV 293
R. Volner, *Slovak Republic*

Author Index

Adams, D. G. 122
Alonso, I. G. 267
Anderton, R. N. 172
Anwar, S. 223
Appleby, R. 172
Bernas, M. 108
Bell, Z. W. .....
Bigham, J. 235
Bilbao, A. 76
Borrell, J. 235
Cheal, J. 136
Chen, Y. Y. 180
Chung, C. D. 156
Ciurapinski, W. 142
Daugman, J. 254
Davidson, S. 52
de Martin-Roche, D. 272
Douglas, G. A. .....
El-Shennawy, K. 213
Emarah, A. E. 213
Espinosa-Duro, V. 264
Evans, J. P. O. 103
Fan, K. C. 156
Fernandez-Medina, E. 163
Ferrer, M. A. 267
Foley, E. 136
Forman, P. 60
Gonzalez-Tablas, A. 190, 289
Halkett, B. .....
Hamilton, S. 223
Han, C. C. 278
Harman, K. 136
Hay, Major A. H. 34
Hernandez, J. C. 190, 240, 289
Hon, H. W. 103
Hozman, J. 108
Isasi, P. 240, 289
James, J. W. 68
Jan, J. K. 180
Kapounek, F. 128
Kelly, R. P. .....
Klima, M. 108
Klock, B. A. 96
Kruse, E. M. 68
Lazarick, R. 85
Ledger, C. 42
Lee, C. Y. 149
Lin, C. H. 149
Lin, Y. 180
Lindfield, A. .....
Lopez, J .....
Macalindin, I. 307
Maki, M. 128
Mana, A. .....
Mansfield, T. .....
McInerey, J. 223
Mex-Perera, C. 240
Mohammed, E. 213
Orfila, A. 190
Ortega, J. J. .....
Palka, N. 142
Parry, I. 60
Pascoe, T. 45
Pata, P. 108
Pazderak, J. 108
Pearson, K. 27
Pedrosa, E. 76
Perea, F. .....
Piattini, M. G. 163
Pickett, C. A. .....
Piechowski, C. J. 19
Poslad, S. 235
Pritchard, D. A. 122
Procratsky, C. A. 19
Ramos, B. 240
Rao, E. 282
Raymond, D. 202
Richardson, G. D. .....
Robinson, M. 103
Robles, S. 235
Roubik, K. 108
Rubinstein, J. 96
Sanchez, J. A. 267
Sanchez-Avila, C. 229, 250, 272
Sanchez-Reillo, R. 197, 229, 250, 272
Serrano, M. A. 163
Sierra, J. M. 190, 240, 289
Sinclair, G. N. 172
Smith, C. L. 115
Smith, G. D. 19
Spaight, W. H. T. 54
Sparks, M. H. 19
Subberud, S. 223
Szustakowski, M. 142
Travieso, C. M. 267
Tsai, C. L. 156, 278
Turner, B. 42
Veatch, J. D. 68
Volner, R .....
Wickens, B. 100
Willis, A. .....
Wood, T. M. 68
Younkin, J. R. .....

Specification of Security Constraint in UML

Eduardo Fernández-Medina, Mario Piattini and Manuel A. Serrano
University of Castilla-La Mancha
Spain.

Abstract - Over recent years various initiatives for solving the problem of security in databases have arisen. However all of them have been only partial solutions which resolved isolated problems. Consequently a global solution to the problem has not been reached yet. We think a methodological approach in which security is taken into consideration from the earliest stages of the development process of the databases is the best strategy. In this paper we present a language for specifying security constraints in models of classes, which is one step of a complete methodology for the development of secure multilevel databases. This language is called OSCL (Object Security Constraint Language). OSCL is based on the constraint language OCL (Object Constraint Language), which is used by the current standard of modeling, UML (Unified Modeling Language).

Keywords: Security Constraints, Multilevel Databases, UML, Methodology, Specification Language, Confidentiality.

Introduction

Throughout the last decade various initiatives have arisen in connection with the security of databases such as analysis and risk management techniques (ISO/IEC, 1997), access control techniques (Castano, et al., 1994; Ferraiolo, et al., 1999; Ferrari and Thuraisingham, 2000; Jajodia, et al., 1995; Sandhu and Bhamidipati, 1997; Tomas and Sandhu, 1997), methodologies for the development of security techniques (Baskerville, 1993), methods for modeling security requirements (Smith, 1990; 1991), and even some methodologies for the development of secure databases (Marks, et al., 1996; Sell and Thuraisingham 1993). All these initiatives are very important and indicate the great interest being demonstrated by both national and international organizations and in general the scientific world in relation to the problem of database security.

The problem that exists is that all the security measures that have arisen are partial, isolated and disconnected solutions which do not offer a global solution to the problem of protecting databases. Consequently, we consider that there should be a methodological approach allowing the construction of databases whilst taking into account aspects of security from the earliest stages of development until completion. This methodology should be an extension of the methodologies and standards of modeling currently in existence, as the organizations really interested in the security of databases would otherwise have to make a great effort to adapt to a new methodology. Moreover, it would be desirable for the information systems constructed that store personal or sensitive data to comply with the existing laws related to the protection of personal data. Some years ago, some initiatives related to methodologies for the development of secure databases (Marks and Thuraisingham, 1996) were applied but with little success. This was due to the fact that the incorporation of security constraints added great complexity to the construction of information systems despite it was the extension of an already known and consolidated development methodology, OMT (Object Modeling Technique) (Rumbaugh, et al., 1991).

Currently the standard of modeling is UML (Booch, et al., 1999), so the idea of endowing UML with security characteristics seems attractive, in order that modeling could be carried out with the syntax and power of UML and with the new characteristics of security provided for use when the application requires such security measures to be fulfilled.

We consider that the first step must be to have a formal language which allows us to specify clearly and

0-7803-6636-0/01/$10.00 ©2001 IEEE

concisely all the security constraints of the application. UML has a standard language of constraints called OCL (Object Constraint Language) (Warmer and Kleppe, 1998) by means of which semantics can be added to class models for certain aspects which cannot be represented graphically, or which even if they could be represented graphically would complicate the comprehensibility and maintainability of the model excessively. This language can be extended in order to allow the representation of security constraints. In this way, we can carry out a modeling of classes for an application and furthermore complete it by using this extended language with information related to security expressed through constraints. Consequently, the idea is to construct the language OSCL (Object Security Constraint Language) using the standard OCL as a base and extending it to support security constraints.

Object Constraint Language (OCL)

This language can be used in modeling in many places and for many purposes. The objective of OCL is to specify constraints in a class model. It would be possible to specify security constraints if the model is equipped with multilevel security attributes in the classes, attributes, methods and associations. The problem is that by including excessive information related to security, the model would become too complicated and would lose descriptive power which would make it difficult to appreciate clearly the semantics of the initial model. As a result, we think it would be convenient to have an extension of the language OCL at our disposal which maintains the initial model intact and which manages the security levels and the constraints between those levels.

OCL is a simple specification language which has certain characteristic which must remain unaltered after any kind of modification or extension. These characteristics are the following:

- OCL must be a language that can express necessary and additional information to the models.
- OCL must be a precise, non-ambiguous language that can be easily written, read and understood.
- OCL must be a declarative language. Its expressions must not have collateral effects.
- OCL must be a language with types.

On creating the extension of the language, all these characteristics of the original language have been taken into consideration, with the objective of maintaining a high level of coherence between the two languages. This is particularly important so that any analyst carrying out modeling with UML and using the constraints language OCL, is able to use the language OSCL without having to make undue changes to his way of working.

The three principal tools that we have at our disposal when modeling constraints in OCL are the Invariants, the Preconditions, and the Postconditions:

- An invariant is a constraint that establishes a condition that must always be fulfilled by all the class instances, types and interfaces. An invariant is described by an expression that is considered to be true if the invariant is fulfilled and to the contrary, false. The invariants must always be considered as true.
- Preconditions are conditions related to class operations and which must be fulfilled at the time of execution of an operation. Unlike invariants, instead of always having to be considered true, it is only necessary just at the moment when the operation is going to be executed.
- Postconditions are conditions related to operations that generally specify the result of the operations and which must be considered true only at the moment when the operation finishes.

In our case what we are most interested in are the invariants, given that through them we will express both the security levels of model elements and their instances, and the constraints of integrity between security levels. Although the preconditions and postconditions could also be used to verify that the security constraints of the operations are being complied with, it would be more normal to do this by means of a general constraint over all the operations.

OCL includes the following types of elements and types of collections of elements:

- OclType. All the types defined in a UML model or those predefined in OCL have a type. This type is an instance of the type OclType. Access to this type

allows the analysis to access the meta-level of the model.

- OclAny. In the context of OCL, the type OclAny is the súpertype of all the types in the model. The characteristics of OclAny are available in each object in all the OCL expressions.
- OclExpression. Each OCL expression is an object in the context of OCL. The type of expressions is OclExpression.
- Real. It represents the mathematical concept of the real number.
- Integer. It represents the mathematical concept of the integer number.
- String. It represents a string of ASCII characters.
- Boolean. The type Boolean represents the typical logical values, true and false.
- Enumeration. It represents the defined enumerations in a UML model.
- Collection. It is the abstract supertype of all the collections of types in OCL. Each occurrence of an object in a collection is called element.
- Set. It is the mathematical representation of a group. It contains elements without repetitions.
- Bag. They are composed of a collection of elements that can be duplicated and that are not in order.
- Sequence. A sequence is a collection in which the elements are in order. An element can be part of a sequence more than once.

All these types defined in OCL together with the operations defined for each of these types are the tools that OCL has at its disposal for expressing the constraint and which we can also use for expressing the security constraints in OSCL. The following are some examples of constraints expressed in OCL:

- Client
  Age > = 18

With this invariant we specify that the field "Age" in all the instances of the class "Client" must be greater than 18.

- Doctor
  Self.patient → size < 20

Suppose that we have a class model where amongst others the classes "Doctor" and "Patient" appear and that a one-to-many relationship exists between the two. In this case, the invariant would indicate that no doctor can be associated with more than 20 patients.

The instances of OclType (we will generalize and call them type) have the following properties:

- type.name: String → Name of the class
- type.attributes: Set (String) → Collection of names of the attributes of the class.
- type.associationEnds: Set (String) → Collection of names of the associations of the class.
- type.operations: Set (String) → Collection of names of the operations of the class.
- type.supertypes: Set (OclType) → Collection of all the direct superclasses of the class.
- type.allInstances: Set (type) → Collection of all the instances of the class and its subclasses.

With all these properties we can easily access the metamodel. Precisely what we aim to achieve is that all the security properties belong to the metamodel and that constraints can be established directly over them.

Object Security Constraint Language (OSCL)

The objective aimed at is to be able to represent multilevel systems by means of a language of the specification of constraints. Consequently, the language must allow the definition of security levels for all the elements of a class model, that is to say, for the classes, the attributes, the operations, the associations etc, in the same way as for any instance of all these elements. Moreover, the language must provide tools in order to be able to specify certain properties related to the security level of the elements that interact in a model.

The first aspect we have to analyze is how to express the security levels that the elements of a class model in UML will have. In order to do this we will broaden the functionality of the type OclType that allows access to the metamodel.

Each class will have a security level or range of intrinsic levels, and the instances of those classes will inherit this security level, unless there is an explicit constraint that indicates the contrary, although in any case it will be a higher level than that of the class and it will depend on the characteristics of the instance. The

same effect will be produced with the attributes with respect to their values, the associations with respect to their links, etc. In order to be able to specify the security level in the model elements, we will access the metamodel by means of OclType.

An initial modification of the language that will be useful for navigating flexibly in certain specifications is as follows:

- type.associationEnds: Set (OclType) (instead of Set (String)). In this way we can access from one class all those that are related with the first via an association.

In order to be able to carry out general specifications on a specific model or, for example, on all the classes of a model, we need an element that acts as a "container" and from which we can access all its classes. We will consider a new class of the type OclType which represents the model and which contains all the elements of a specific model. We will call this new class "Model".

The usual levels of security in a multilevel system are "Unclassified", "Confidential", "Secret" and "TopSecret", but we will allow the designer to specify the appropriate levels for each case. To do this, we will specify a constraint via the class "Model" that indicates the range of possible security levels in a specific model.

- Model.levels: Sequence (String)

We have considered that the security level of a class should be an intrinsic element of the class, as may be the attributes of the class or the operations and as a result we have decided to broaden the class OclType giving it functionality for specifying the level of the classes, attributes, operations and associations:

- type.levels: Sequence (String)
  Post: Model.levels → subsequence
  (type.levels → first, type.levels → last) =
  result.

- type.level: String
  Post: type.levels → first = result.

With the first operation we specify the range of possible levels amongst which a class can be found. A postcondition is used to specify that the range of possible security levels must be correct and be included in the range of values defined for the UML model. Although a class may have a range of security levels, it will always be characterized by one security level which will be the lowest of the range and the lowest level of security that its instances can have. The second operation allows the specification of the level of a class. For example, the class "patient" may have a range of security levels from "confidential" to "secret" as the level of security of the patient will depend on the kind of illness that this person is suffering from (eg. Infection: "confidential", AIDS: "secret", etc.), but at least, the level of the class "patient" will be "confidential".

We need similar operations to specify the level of attributes, operations and associations:

- type.attribute.levels: Sequence (String)
  Post: Model.levels →
  subSequence (type.attribute.levels → first,
  type.attribute.levels → last) = result

- type.attribute.level: String
  Post: type.attribute.levels → first = result

- type.operation.levels: Sequence (String)
  Post: Model.levels →
  subSequence (type.operation.levels → first,
  type.operation.levels → last) = result

- type.operation.level: String
  Post: type.operation.levels → first = result

- type.associationEnd.levels: Sequence (String)
  Post: Model.levels.subSequence
  (type.AssociationEnd.levels → first,
  type.AssociationEnd.levels → last) = result

- type.associationEnd.level: String
  Post: type.associationEnd.levels → first = result

With the tools which we have at our disposal up to this point, we can specify levels of classes, attributes, methods and associations. When the instance of a class is created it directly inherits the security level of the class, unless there is a constraint that obliges that class

to have a higher security level than its class. Constraints of this type are created taking the class containing the element to which we wish to apply the constraint as the context. For example, if we have a class "Employee" with a security range {Unclassified-Secret}, whose objects will be in a classification level according to their value in the field "salary", the constraint would be expressed as follows:

Employee
Self.level= if salary < $1.500
then "Unclassified"
else if salary < $4.000
then "Confidential"
else "Secret"

In addition to these kinds of specific constraints there will also be some general security constraints such as the following:

- All the objects have a security level included in the security level range of the class to which it belongs. The constraint for each class is:

Class 1
Self.OclType.levels → exist (self.level)

For each object of Class 1 it is essential that the security level of the object is present amongst the security levels of the class. This constraint should be applied to all the classes. We could use the class "Model" previously defined in order to generalize the constraint.

Model
Self.class → forAll (C: OclType|
C.allInstances→count (O: Class|
C.levels → notexist(O.level))=0)

In this case we specify that for each class of the model we must ensure that the number of instances whose security levels do not belong to the level range of the class is 0. It is a similar constraint to the previous one but more difficult to understand even though it is more general.

- The associations will have a security level which must be equal to or higher than the level of the classes to which it is related. In the same way, an instance of an association will have a security level higher than or equal to that of the related association and objects.

Model
Self.class → forAll (C1: OclType|
C1.associationEnds→ForAll
(C2: OclType| C1.C2.level >= C1.level And
C1.C2.level >= C2.level)

This expression specifies that for all the classes of a model it is essential that all the associations with another class must have a security level higher of equal to that of the related classes.

- The generalization mechanisms allow us to refine classes (superclasses) into more specific groups that inherit the properties of the first groups (subclasses). The accepted rule for the relationship of generalization is that the security level of the subclasses must be greater than or be more restrictive than the security level of the superclass. The specification of this constraint is as follows:

Model
Self.class → forAll (C1:OclType|
C1.SuperTypes→ForAll (C2:OclType|
C1.level>=C2.level)

The rest of the original constraints language would keep its initial characteristics, thus allowing the expression of all kinds of constraints, including those of security. In the following point we will present an example of a model of a system in which requirements of confidentiality between the objects and these are specified with the new language OSCL.

Example of the Application of the Language OSCL

Let us consider the UML model shown in Figure 1 which models the management of a hospital. In order to be able to analyze the security details more clearly, the model does not show exhaustively the semantics of the hospital management system.

In this model there is a relationship of generalization and various associations. In the generalization

relationship we can see that there is a diversity of security levels as well as in the classes and associations considered in the model.

The security constraints that we would have to specify for this model would be the following:

- Model.levels= Sequence (U, C, S, TS)

We specify that the security levels in our model will be: U (Unclassified), C (Confidential), S (Secret), and TS (Top Secret).

- Person.levels = Sequence (U..S)

We indicate that the class Person will have a range of levels between "Unclassified" and "Secret". Note that it is not necessary to specify "Person.level=U" given that it is an implicit constraint in accordance with the definitions of the operations of the class OclType.

- Patient.levels = Sequence (U..S)

- Patient.Illness.levels = Sequence (U..S)

The attribute "Illness" of the class Patient will grant the security level of the instances. If the Patient has an illness such as cancer or AIDS, the attribute will be secret and therefore the patient, too.

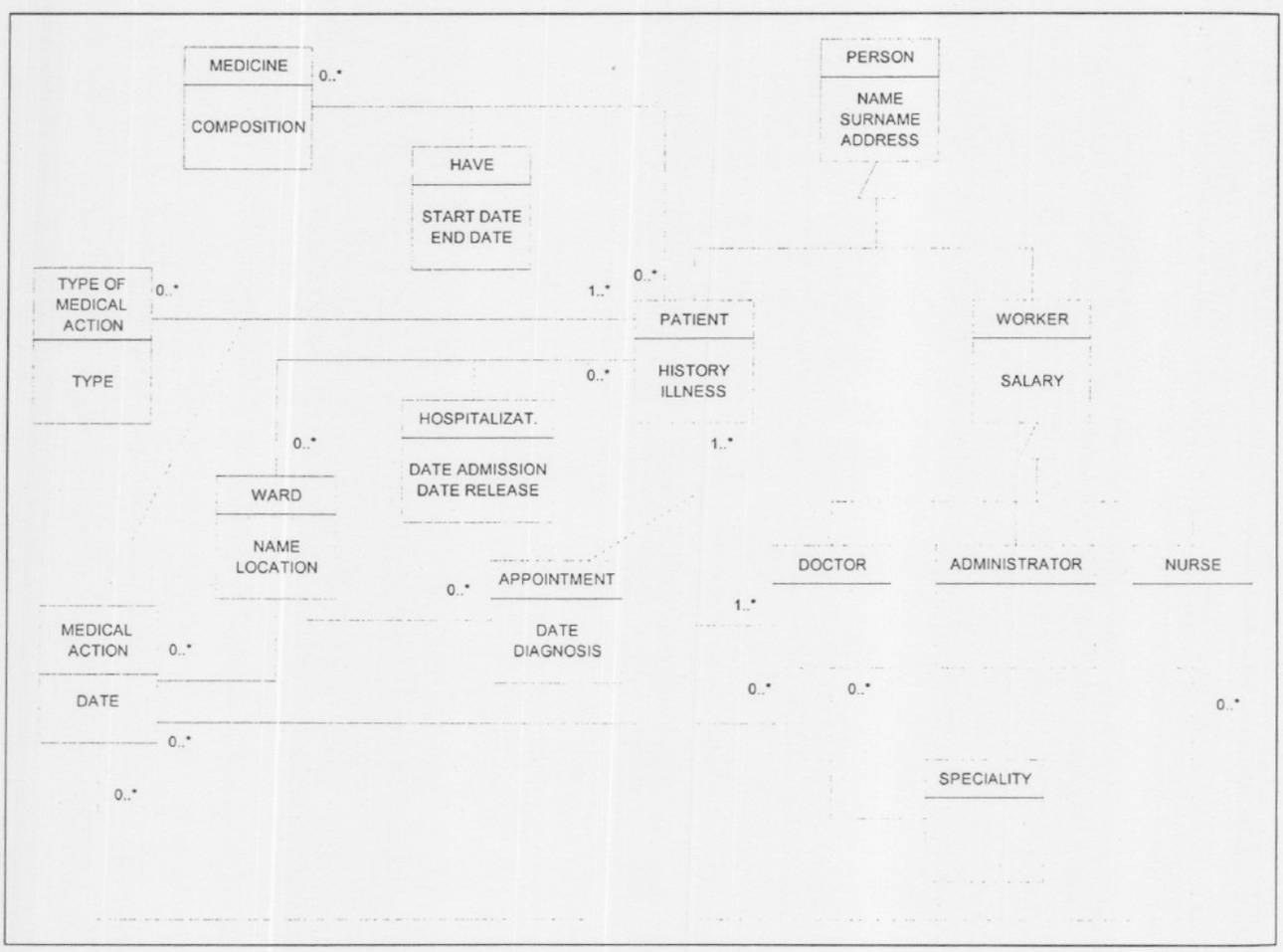


figure 1
Example of Class Model.

- Worker.levels = Sequence (C..S)

- Worker.salary.levels = Sequence (C..S)

The attribute "Salary" of the class Worker will indicate the security level of the instances. Workers with salaries of less than $3.000 will be Confidential and the rest will be Secret.

- Doctor.levels = Sequence (C..S)

- Administrator.levels = Sequence (C..S)

- Nurse.levels = Sequence (C..S)

Note that the constraints imposed by the inheritance of properties in a generalization-specialization relationship are complied with.

- Medicine.level = C

- Medicine.Patient.levels = Sequence (C..S)

We are specifying the security level of an association. In this case, given that we have a class of Association, we could have specified it in this way: Have.Levels = Sequence (C..S)

- Hospitalization.levels = Sequence (U..S)

Note that when nothing is specified about the level of a class, it is considered to be the lower classification level, as in this case in the class "Ward" (given that Hospitalization is an association between Patient and Ward).

- Appointment.levels = Sequence (C..S)

- MedicalAction.levels = Sequence (U..S)

With these lines all the security levels of the classes, attributes and associations are specified. Due to the complexity of the process the ideal thing is to have tools at one's disposal which verify the congruence of all the constraints. These would be the security constraints related to security levels. There are another kind of constraints, which depend of the value of a certain attribute. In this example, we have two of these constraints:

- Worker
  Self.level = (if self.salary < $3.000 Then C Else S)

We specify that for each instance of the class worker, the security level will depend on his salary, so that if he earns less than $3.000. He will have a "confidential" level and if he earns more he will have a "secret" level.

- Patient
  Self.level = (if self.Illness = "AIDS" or
  Self.Illness = "Cancer" Then S Else U)

In this way we specify that the data of patients with certain illnesses will be protected so that their privacy is not invaded.

Conclusions and Future Work

Security in general and more specifically security in databases has become a priority amongst the problems of today's society due above all to the proliferation of means of communication and information technologies, and to the appearance in several countries of new laws for the protection of personal data and the reinforcement of those already existing. The problem of information security has mobilized several organisms and national and international organizations that have worked towards getting methods, recommendations, policies and even standards that aim to resolve aspects related to security. At the current time it can be seen that many partial solutions to the problem of information security exist, but they are not global solutions and moreover they require significant organizational changes. Consequently many organizations simply do not undertake these changes but prefer to run certain risks than take on changes that may prove to be too great and too costly.

We believe that due to its magnitude the problem of database security is a problem that should be treated through a methodological approach. Therefore, information security must be taken into account throughout all the different stages of construction of

the information system, and not be thought of as an incidental requirement which is only a secondary consideration, and which is only analyzed once the construction of the information system has finished.

As the modeling standard is UML we believe that the most appropriate way of dealing with the problem of security in the design of databases is by modifying UML in order to be able to construct information systems in the same way as we have been doing up until now. By this we mean that the development process does not suffer any major changes but during the process we do take into account the security requirements of each system. To do this we have started by modifying the standard constraints language of UML (OCL), in order to obtain a simple constraints specification language, and using the usual syntax we can specify security constraints in the models of UML classes.

Future work will be focused on refining and broadening the new language, OSCL, so that it can support another type of security constraints, relating to the control of access to information depending on certain roles in the organization, or a certain timetable, exceptions, etc. Then, work will be dedicated to the construction of a complete methodology based on UML for developing information system that guarantee information security.

Acknowledgments

This research is part of the RETISBD projet, supported by the Ministry of Culture and Education (TIC2000-1873-E), which is an special action into the National Program of the Information Technologies and Communications.

Bibliography

Baskerville, R. (1993). "Information Systems Security Design Methods: Implications for Information Systems Development". ACM Computing Surveys. Vol. 25. Nº 4, pp. 375-415.

Booch, G., Rumbaugh, J. y Jacobson, I. (1999). "The Unified Modeling Language. User Guide". Addison-Wesley.

Castano, S., Fugini, M., Martella, G. and Samarati, P. (1994). Database Security. Addison-Wesley.

Ferraiolo, D., Barkley, J. and Kuhn, R. (1999). "A role-based access control model and reference implementation within a corporate intranet". ACM Transactions on Information and Systems Security. Vol. 2. Nº 1, pp. 34-64.

Ferrari, E. and Thuraisingham, B. (2000). "Advanced Databases: Technology Design". Chapter 11: Secure Database Systems. Eds.: Piattini, M. and Díaz, O. Artech House. Londres.

ISO/IEC TR 13335 (1997). Information technology-Guidelines for the management of IT Security.

Jajodia, S., Sandhu, R. and Blaustein, B. (1995). "Information Security, An integrated collection of essays". Capítulo 21: Solutions to the Polyinstantiation Problem. Eds.: Abrams, M., Jajodia, S. and Podell, H. IEEE Computer Society. California.

Marks, D., Sell, P. and Thuraisingham, B. (1996). "MOMT: A multilevel object modeling technique for designing secure database applications". Journal of Object-Oriented Programming. Vol. 9. Nº 4, pp. 22-29.

Rumbaugh, J., Blaha, M., Premerlani, W., Eddy, F. and Lorensen, W. (1991). Object-Oriented Modeling and Design. Prentice Hall, Englewood Cliffs.

Sandhu, R. and Bhamidipati, V. (1997). "Database Security XI: Status and Prospects". The URA97 model for role-based user-role assignment. Eds.: T.Y. Lin and S. Qian. Chapman and Hall, London, pp. 262-275.

Sell, P. and Thuraisingham, M.B. (1993). "Applying OMT for Designing Multilevel Database Applications". Proceeding of the Seventh IFIP Working Conference on Database Security. Huntville, Septiembre.

Smith, G.W. (1990). The Semantic Data Model for Security: Representing the Security Semantics of an Application. Proceedings of the Sixth International Conference Data Engineering, IEEE, pp. 322-329.

Smith, G.W. (1991). "Modeling Security-Relevant Data Semantics". Proceedings of the IEEE Transactions on Software Engineering, Vol. 17. Nº 11, November, pp. 1195-1203.

Tomas, R. and Sandhu, R. (1997). "Database Security XI: Status and Prospects". Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management. Ed.: T.Y. Lin and S. Qian. Chapman and Hall, London, pp. 166-181.

Warmer, J. and Kleppe, A. (1998). The object constraint language. Addison-Wesley. Massachusetts.