An Object-Oriented Modelling Approach into the Management of Information Security

J. Leiwo, C. Gamage and Y. Zheng
Monash University, PSCIT
McMahons Rd. Frankston, Vic 3199, Australia, Tel. 61 3 904 4135, Fax. 61 3 904 4124,
e-mail: {skylark,chandag,yuliang}@mars.fcit.monash.edu.au

Abstract

Structured analysis and design methods have been applied in the integration of information security in system development but the emergence of OO paradigm has made them less relevant. OO has improved security of computer systems and databases, so it is reasonable to assume that approach being applicable also to the management of information security. This paper shows how information security can be modelled using Unified Modeling Language (UML) and how formal information security requirements can be derived from class diagrams.

Keywords
Object-Oriented modelling, Information security modelling

1 INTRODUCTION

Structured system analysis and design techniques have been applied in the specification of information security requirements. Baskerville (1988) has proposed a method to integrate security design into data flow diagrams (DFD) and Pernul (1992) has shown how to integrate security design into entity-

relationship (ER) diagrams. More recently, requirement engineering (RE) techniques have been successfully applied for specification of information security requirements (Boswell, 1995; Dubois and Wu, 1996). These are significant results, since lack of integration between security design and general system design easily leads to inadequate security (Caelli, 1997). We shall show how to use UML (Larman, 1997) notation (class diagrams specifically) in the specification of information security requirements. Other common OO modeling techniques include Booch methodology (Booch 1994), and Object Modeling Technique (OMT) by Rumbaugh et. al. (1991). As the UML is the latest, integrated approach, supported by Object Management Group (OMG), it has been selected as the tool used.

Similarly to the software crisis setting new demands for research in software engineering in late 1970s (Pressman, 1997), new approaches are needed for dealing with *information security crisis*. Databases, communication protocols and information systems are insecure, even though significant amount of research has been carried out in many areas of computer and information security. Since OO methods have been efficient in computer security (OOPSLA, 1993) we attempt to expand them also to identifying security requirements of information systems. General advantages of OO modeling are (Booch, 1994) expressiveness of OO languages, improved reuse of components, improved resilience to change, reduction of development risks and appeal to the working of human cognition. Booch also states that experience has shown that these benefits outweigh the two major disadvantages: performance and high start-up costs.

Essential concepts of OO modelling shall be summarised and advantages of OO modeling in security design summarised in section 2. Section 3 shall show how to model security requirements using UML. Conclusions shall be drawn and areas highlighted for future work in section 4.

2 OO MODELING AND INFORMATION SECURITY

An object has a unique identity, structure of data and behaviour (Rumbaugh et. al., 1991; Booch, 1994). Objects with same data structure (attributes) and behaviour (operations) can form classes. Each object is an instance of a class. *Polymorphism* is a property of same operations behaving differently on different classes. The advantage is that the actual implementation of operations can be hidden from other classes and inter-class interfaces be standardised. Hiding of implementation details by providing a standard interface to the functionality is called *encapsulation*. *Inheritance* means that a class can be specified as a subclass of another, and the subclass shares the properties of a parent class unless locally overwritten.

The major difference to structured methods is that OO modeling is concerned with concepts, not implementation. In the organisational security modeling, this has the advantage of forcing security management to exactly specify the nature

and role of information security in the organisation. By applying polymorphism, encapsulation and inheritance generic security designs can be specialized into various organisational units and different views of security objects can be provided for managerial, administrative and technical personnel. Diagrammatic presentation of objects, using object models, can also improve understanding and communication between various views of information security. Objects also form a strong hierarchy, similar to a typical organisation of information security. Object model is a static structure of objects and their relationships and is modelled as a class diagram. A dynamic model is required for implementing the control aspects of the system and a functional model for describing the transformations on values of data within the system. These are, anyhow, not further studied herein.

3 UML AND SECURITY DESIGN

Figure 1 gives an example of modeling secure business processes using UML notation. Assume a generic class BusinessProcess that represents any business process in the organisation. Using specialisation, a class named SecureBusProc is constructed to represent a secure business process. Note, that it is not necessary that there are any instances of BusinessProcess but that all the objects of this class are of type SecureBusProc. Specialisation is rather a modeling tool than an indicator that some business processes might be insecure. SecureBusProc has an attribute Clearance that indicates the organisational security level (SecurityLevel class is assumed but not explicitly modelled herein). Using the similar logic, business processes can be further classified into a hierarchy of various types of business processes. In this example, a classical producer-consumer pair is modelled. ProducerProc is a secure business process, and so is ConsumerProc. They both consist of a Message msg that is communicated between them. Class Message can again be any type of a message being communicated between processes, and can be communicated by any media. Details of Message class are omitted herein.

An important modeling decision here is that a message is first designed as a high level of abstraction focusing on content. This abstraction is then specialized into a trusted message that focuses on the protection of the message. Trusted message is assumed to be protected by a security protocol, being an aggregate of one or more security services that are again aggregates of one or more security mechanisms. The hierarchy can be further deepened by specifying, for example, a class for security enforcement algorithms, that can further be an aggregate of the actual implementation and level of assurance provided by that algorithm.

Strong hierarchy is the major advantage of OO modeling in information security design. At the high organisational level, concepts can be identified and then further details can be added at all the organisational levels. Modeling of various concepts can also be done parallel based on common interfaces. This is also a significant improvement in the support for the full life cycle of information

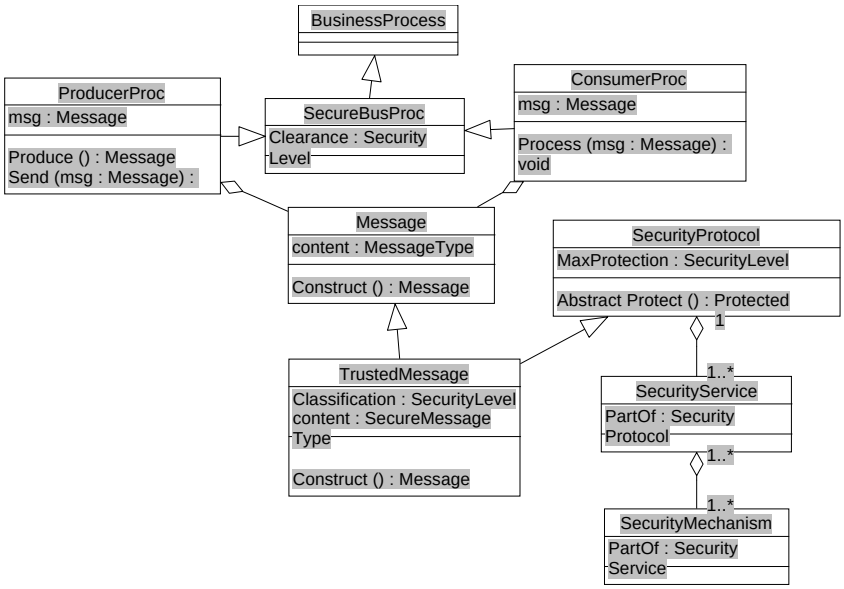

Figure 1 UML modeling example.

security specifications and designs. Since the modeling focus is on concept and their structure, introduction of various implementations of generic classes, such as new security enforcement protocols, does not require significant updates in the overall security design. Instead, new components usually appear as new implementations where the details are hidden from other objects by encapsulation.

Once the class diagram is specified, the interesting question is how to convert class specifications into information security requirements. It appears, that deriving formal security specifications, such as following the notation of (Leiwo and Zheng 1997b) is a considerably straightforward task and shall not be further studied herein.

4 CONCLUSIONS AND FUTURE WORK

The contribution of this paper lies in the identification of advantages OO modeling could offer for the management of information security. Also, guidelines have been provided to illustrate the nature of OO modeling and how that could be applied in the specification of secure business processes. This paper also attempts to open discussion of the integration of security design into enterprise wide object design. As there are numerous advantages, it is hoped that future work on this area will enhance the understanding of the structure of information security as an integral part of business process engineering.

REFERENCES

Baskerville, R. (1988) *Designing Information Systems Security*. John Wiley & Sons.

Booch, G. (1994) *Object-Oriented Analysis and Design with Applications* 2nd ed. Addison-Wesley.

Boswell, A. (1995) "Specification and Validation of a Security Policy Model". *IEEE Transactions on Software Engineering*, Vol. 2, Nr. 2, pp. 63-68.

Caelli, W. (1997) "Information Security in Electronic Commerce". *Proc. 1997 Pacific Asia Conference on Information Systems*.

Dubois, E. and Wu, S. (1996) "A Framework for dealing with and Specifying Security Requirements in Information Systems". *Proc. IFIP/Sec'96*.

Larman, Craig (1997*) UML and Patterns: an Introduction to Object-Oriented Analysis and Design*. Prentice-Hall.

Leiwo, J. and Zheng, Y. (1997b) "A Framework for the Management of Information Security". *Proc. 1997 Information Security Workshop*.

OOPSLA (1993) *Workshop on Security for Object-Oriented Systems* (Thuraisingham, B. and Sandhu, R. and Ting, T.C., ed.). Springer-Verlag Workshops in Computing.

Pernul, G. (1992) "Security Constraints in Multilevel Secure AMAC Schemata" *Computer Security - ESORICS'92*. Springer-Verlag LNCS 648.

Pressman, Roger S. (1997) *Software Engineering: A Practitioner's Approach*, 4th ed. McGraw-Hill.

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

BIOGRAPHIES

Jussipekka Leiwo received his M.Sc. from University of Oulu, Finland in 1995 and is currently a Ph.D. student at Monash University.

Chandana Gamage is a PhD student in computer science at Monash University. He received his B.Sc. from the University of Moratuwa, Sri Lanka, in 1993 and M.Eng. from Asian Institute of Technology, Thailand, in 1995.

Yuliang Zheng's research interests include cryptography and information security. He has chaired or served as a technical and organising committee member for multiple national and international conferences. He leads a research group at Monash University which focuses on information security technology and its applications.