EuroPACS2002

20th International Conference, 5.-7.9.2002 Oulu/Finland

Proceedings of the 20th EuroPACS annual meeting

held 5th to 7th September 2002 Oulu, Finland

edited by
JAAKKO NIINIMÄKI,
EERO ILKKO &
JARMO REPONEN

for

Northern Ostrobothnia Hospital District,
Radiological Society of Finland, and
University of Oulu

Handling Security Policies: the Example of an Italian Hospital

Patrizia Asirelli[1], Giovanni Braccini[2], Davide Caramella[3],
Alessandro Coco[1], Fabrizio Fabbrini[1]
[1]Istituto di Elaborazione dell'Informazione, National Research Council, Pisa, Italy
[2]Unità Operativa di Radiologia, AUSL 5, Pisa, Italy
[3]Diagnostic and Interventional Radiology,University of Pisa, Italy
Corresponding author: Fabrizio Fabbrini, IEI-CNR, Via Moruzzi, 1 - 56124 Pisa, email: fabbrini@iei.pi.cnr.it

Security and privacy are crucial in several environments, but their role can hardly be underestimated in the health care sector. Regardless of the policy model and the application environment, once a policy has been defined, it is very important to be able to verify that it really meets the security requirements and prevents any undesired situations. This means that it would be auspicable to have tools that, besides allowing the definition of the policy, permit to define and verify properties that the policy must exhibit.

INTRODUCTION

While the Internet and the Web offer powerful solutions to the ever growing need to grasp information wherever it is located, with beneficial results both for medical and research purposes, they are potential sources of security vulnerabilities.

The general goal of information security management is to guarantee against the impact of security accidents: this should be achieved by providing reliable mechanisms for information sharing, at the same time ensuring confidentiality, integrity and availability.

Laws have been established in both Europe and US to regulate the safe handling of medical records by healthcare personnel. Accordingly, computer science is evolving to provide technical solutions: mechanisms for user identification and authentication, access control, protection of communication have been proposed, and the design and validation of security policies is being addressed.

SECURITY POLICIES

A security policy defines how an organisation manages and protects its information and computing resources to achieve security objectives. It has to express rules to describe users' authorisations upon the objects and the resources to be protected, and to use a set of security mechanisms to guarantee that the access requests match the rules. Defining a security policy means to provide a suitable security model able to prove the properties of the system, that really meets the security requirements. The most important security models in literature belong to the mandatory access control (MAC), discretionary access control (DAC) and role-based access control (RBAC) families.

AN EXAMPLE

The aim of this work was to show how the administrator of a healthcare organisation can handle (define, verify, modify) its security policy. After investigating available security policy models, we have chosen an RBAC approach because of its suitability for a health care environment (indeed, it seems to be more general, since it allows for easier updates to the policy and can be later expanded into mandatory or discretionary, as necessary). Furthermore, we have specified the model in a logical form handled by a logic database management system. Thus, the model specification becomes executable, allowing for exercising the policy on examples (prototyping) and verifying the correctness of the policy and its properties by means of deductive rules and integrity constraints. According to this approach, a security policy has been defined, modeled and verified for the Radiological department of the "Lotti" Hospital in Pontedera, Pisa.

CONCLUSIONS

With this work we have realized a tool suitable for defining and managing the security policy of a radiological department. The characteristics of the model and the flexibility of the implementation allow for adopting the tool into health care organizations with greater dimensions and more complex structure.

References

1 Commission of the European Communities, "*Information Technology Security Evaluation Criteria*", Version 1.2, Office for Official Publications of the European Communities, Luxembourg, June 1991.
2 R. S. Sandhu, E. J. Coyne, H. L. Feinstein e C. E. Youman, "*Role-based access control models*", IEEE Computer, 1996.
3 Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995.
4 P. Asirelli, D. Di Grande, P. Inverardi e F. Nicodemi, "Graphics by a logical Database Management System", *Journal of Visual Languages and Computing*", vol 5, 365-38, 1994.