Availability versus Confidentiality of Electronic Health Records

Robert de Groote,
Database group, University of Twente, The Netherlands
e.degroote@ewi.utwente.nl

October 13, 2006

Digitization of healthcare data is an ongoing process that will eventually lead to large nationwide information systems where sensitive medical data is stored. An important issue in this process is the protection of patients' privacy. Applying security measures so that a desired level of privacy protection can be attained has proven to be an interesting and difficult problem when considering the requirements of clinical systems.

An important aspect of clinical systems is the requirement of high data availability; low availability might seriously jeopardize the safety of patients in for example an emergency situation in which fast access to data is necessary. Any access control mechanisms protecting healthcare data should therefore be relatively simple and fast. Such a simple and fast mechanism should also protect the patient's privacy, disclosing information only in those situations when the information is needed. The latter requirement requires a highly complex mechanism and is hard to combine with the first requirement of a simple mechanism. Motivated by these conflicting requirements, a mechanism called Audit-Based Access Control (ABAC) has been suggested in the literature [1]. The central idea behind ABAC is that access control does not take place a priori, as is traditionally the case, but rather a-posteriori. In such a setting, access to data is justified later on by using an audit logic for accountability.

Another characteristic of clinical systems is that they are highly heterogeneous. The different systems that constitute the wider system may each employ different levels of security. Ideally, confidentiality of data should be invariant of its environment. In hospitals where the data resides in paper records for example, the security policy is made invariant of changes in environment by law enforcement. In applications dealing with digital information, such an enforcement can be achieved using cryptography. Cryptographical enforcement of access control [3] prevents an attacker from accessing data through the file system, and lowers the required level of trust that needs to be put in the system storing the data. But where cryptography solves the problem of the enforcement of access control, it is rather incompatible with data availability; emergency access to data is a desired option, but is made impossible when using cryptography in its purest sense.

A natural way to solve the availability problem of encrypted healthcare data is to use key escrow: a trusted agency stores copies of the cryptographic keys protecting the data, allowing recovery of a key when it is necessary to do so. There are however a number of important security issues that need to be addressed when using this approach. Key escrow creates a new vulnerable path to the unauthorized recovery of data, and requires an enormous amount of trust to be put in the escrow agency. We believe that by using *multiple* escrow agencies, e.g. applying a *partial key escrow* setting using proactive secret sharing techniques [2], the required amount of trust in a single agency can be decreased. This approach, combined with the auditing mechanisms mentioned in [1], may pave the road for an environment in which data confidentiality and availability can co-exist.

References

[1] M. Dekker and S. Etalle. Audit-based access control for electronic health records. In *Views on Designing Complex Architectures, Electronic Notes in Theoretical Computer Science*, 2006.

[2] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive secret sharing or: How to cope with perpetual leakage. *Lecture Notes in Computer Science*, 963:339–352, 1995.

[3] C. C. "M. Petkovic and M. Hammoutene". "cryprographically enforced personalized role-based access control". In *21st IFIP International Information Security Conference*, 2006.