Computer Security

Mark Evered and Serge Bogeholz write a brief case study on access control requirements for health information systems. Their goal is to display the defects when using component-based software that implements static per-method access control and provide new constructs to account for these problems. For this case study, their chosen facility operates by using a paper-based system (creating, signing, and filing physical documents). This pre-computer facility provides a simple context and displays how difficult access control can become. To develop a new structure, the facility will need to meet the following 7 criteria: concise, clear, aspect-oriented, fundamental, positive, need-to-know, and efficiency.

To begin construction, a simple object-based structure is used. The authors explain how an object can have constraint mechanisms built into the platform for access control. The constraints would be implemented in the form of interfaces, specific to the accessor or role. For example, constraints based on profession. Whereas a doctor, a nurse, a practitioner, or a clerk might have different privileges assigned. The distinction between different privileges depends directly on the data. Certain types of data may need to be confidential or may only be accessed by proper authority. Therefore, privileges need to be agreed upon beforehand which limits the system when custom access needs to be granted. To solve this problem, built-in functions can be made to grant privileges on a case-by-case basis. Approaches to maintaining this type of system include functions such as: access of resident objects, access dependent on attribute value, access with time constraints, access on call history, access with parameter, and access with logging. Although this system has a lot of functionality, it has become very complex.

To maintain simplicity, and the 7 criteria listed in the first paragraph, a bracket based system is used to modify constraints. This model refines an original constraint by using a modular interface that points to the target object. This approach is used because it is easier to update, remove, and add new permissions. Additionally, a language construct for access constraints are used frequently to provide clarity. These verbiage modifications are helpful descriptors that can be easily translated for a bracketing class.

Overall, this papers goal is to describe the many issues with per-method object-based access control. It adequately shows how complex a simple system can become when using old access control models.