question

In the course book Matt Bishop (05, p251) writes:

Two questions underlie the use of access controls:

1. Given a subject, what objects can it access, and how?

2. Given and object, what subjects can access it, and how?

Explain the practical significance of these questions, including what this implies for what Bishop calls abbreviations of rights and for revocation of rights.

Matt Bishop's questions about access controls are central to understanding how security is managed in any information system. Access control is essentially about managing who (or what) can do what with various resources in a system. Let's explore the practical significance of these questions:

1. **Given a subject, what objects can it access, and how?**
   * **Practical Significance**: This question addresses the permissions a user (or a process, in more technical terms, the 'subject') has within a system. It's about determining what resources (like files, databases, network access – these are the 'objects') a subject can access and in what manner (e.g., read, write, execute, delete).
   * **Implications for Abbreviations of Rights**: In practical terms, it's often necessary to categorize these permissions into roles or groups for efficiency. For example, all members of a 'Human Resources' group might have read and write access to employee records. This is an 'abbreviation of rights', where a set of permissions is bundled under a recognizable label.
   * **Revocation of Rights**: The management of these permissions must be dynamic. When a user changes roles, leaves the organization, or a process is no longer needed, their rights need to be adjusted or revoked to maintain security. This implies a need for a system that can promptly update or remove access rights as circumstances change.
2. **Given an object, what subjects can access it, and how?**
   * **Practical Significance**: This is the inverse of the first question. It's about specifying for a given resource (object) which users or processes (subjects) are allowed access, and what kind of access they are permitted. This is crucial for protecting sensitive information or critical system resources from unauthorized access.
   * **Implications for Abbreviations of Rights**: From this perspective, rights abbreviations help in defining and reviewing the security policies for particular resources. For instance, a document might be tagged as 'Confidential', automatically restricting its access to a certain group of users.
   * **Revocation of Rights**: When the sensitivity of the object changes (e.g., a project moving from confidential to public status) or in response to a security incident, access rights need to be updated. This again underscores the need for a flexible and responsive access control system.

**Overall Significance:**

* **Security and Compliance**: These questions form the basis of implementing security policies that comply with legal and regulatory requirements. For example, ensuring that only authorized personnel can access personal data as per privacy laws.
* **Efficiency and Usability**: By using abbreviations of rights and roles, organizations can manage access controls more efficiently without overwhelming the system with individual permissions for each user and object.
* **Dynamic Security Posture**: The ability to revoke and modify rights is essential for maintaining a secure and adaptable security posture, especially in response to changes within the organization or in the face of evolving external threats.

In summary, the questions posed by Matt Bishop highlight the fundamental considerations in designing and implementing access control systems. These systems need to be robust, flexible, and capable of reflecting the dynamic nature of organizations and the threats they face.