Abstract

Security in software applications is motivated by the need to prevent unauthorized usage of information and computing resources in a multi-user environment. The $UCON_{ABC}$ usage control is one of the primary protection mechanisms, which supports the enforcement of application specific security requirements. A usage control model is an abstract representation of software applications specifically designed to analyze the theoretical security properties.

The safety decidable usage control models require algorithms to decide whether a given initial configuration is *safe* with respect to a *usage right*, a *subject* and an *object*. Expressivity is the range of usage control policies expressible in the model. Safety decidability and expressivity are the two fundamental issues in usage control. This work generalizes the $UCON_{ABC}$ usage control model to accommodate more usage control policies and present theorems on safety analysis of the generalized model. This work also investigates beyond primitive safety analysis and presents a temporal logic based security property specification language to express desirable properties of usage control configurations. Then, it presents a formal property verification tool to verify the security properties on the given usage control policies.

Security analysis of the model can provide theoretical assurance of security. Security of usage control in software applications depends on the correct usage control implementation as well. This work also presents the approaches for verifying the correctness of application specific concurrent usage control implementations.

Keywords: Usage Control, Safety Analysis, Decidability, Formal and Semi-formal Verification.