論文内容の要旨

博士論文題目

Security Quantification and Risk-Adaptive Authorization Mechanism in Cloud Computing

氏名 FALL DOUDOU

Cloud computing has revolutionized information technology, in that it allows enterprises and users to lower computing expenses by outsourcing their needs to a cloud service provider. However, despite all the benefits it brings, cloud computing raises several security concerns that have not yet been fully addressed to a satisfactory note. Indeed, by outsourcing its operations, a client surrenders control to the service provider and needs assurance that data is dealt with in an appropriate manner. Furthermore, the most inherent security issue of cloud computing is multi-tenancy. Cloud computing is a shared platform where users' data are hosted in the same physical infrastructure. A malicious user can exploit this fact to steal the data of the users whom he or she is sharing the platform with. To address the aforementioned security issues, we propose a security risk quantification method that will allow users and cloud computing administrators to measure the security level of a given cloud environment. Our risk quantification method is an adaptation of the fault tree analysis, which is a modeling tool that has proven to be highly effective in mission-critical systems. We replaced the faults by the probable vulnerabilities in a cloud system, and with the help of the common vulnerability scoring system, we were able to generate the risk formula. In addition to addressing the previously mentioned issues, we were also able to quantify the security risks of a popular cloud management stack, and propose an architecture where users can evaluate and rank different cloud service providers. While being infamous for its numerous security issues, cloud computing is also infamous for being highly dynamic. The dynamicity of cloud computing implies that dynamic security mechanisms are being employed to enforce its security, especially in regards to access decisions. However, this is surprisingly not the case. Static traditional authorization mechanisms are being used in cloud environments, leading to legitimate doubts on their ability to fulfill the security needs of the cloud. We propose a risk adaptive authorization mechanism (RAdAM) for a simple cloud deployment, collaboration in cloud computing and federation in cloud computing. We use a fuzzy inference system to demonstrate the practicability of RAdAM. We complement RAdAM with a Vulnerability Based Authorization Mechanism (VBAM) which is a real-time authorization model based on the average vulnerability scores of the objects present in the cloud. We demonstrated the usefulness of VBAM in a use case featuring OpenStack.

（論文内容の要旨）

（１，２００字程度）

氏　名	FALL DOUDOU

（論文審査結果の要旨）

本博士論文では，クラウドコンピューティング環境などのマルチテナント環境におけるセキュリティリスク軽減のための提案を行なっている．

第一に，クラウド環境におけるセキュリティリスクを定量化するために，脆弱性ツリーを用いた定量化モデルを提案した．この脆弱性ツリーでは，クラウド環境の根源である VMM を起点として，各ゲスト OS，さらに各ゲスト OS 上のアプリケーション等の脆弱性が構成するアタックサーフェスを確率としてとらえる事でリスクを算定する．実運用における値の信頼性も考慮に入れ，各脆弱性の悪用の容易さには，広く用いられている CVSS の Exploitability スコアを改変して採用している．

第二に，クラウドのマルチテナント環境では，オブジェクトにアクセスする主体が動的に変化し，かつある主体に着目しても時間により信頼度が変化する．このクラウド環境特有の動的な変化に対応するために，扱うオブジェクトのリスクとアクセス主体の許容リスクレベルを用いた動的なアクセス制御モデルの提案を行なった．この提案の中ではクラウドプロバイダをまたがるマルチクラウド環境も考慮されている．

本博士論文は研究内容について新規性ならびに有効性があることが認められ，博士（工学）の学位を授与するにあたって十分な内容であると認められる．

（Ａ４　１枚　１，２００字程度）