ACSF: An Autonomous Cloud Security Framework

Cloud computing has a broad appeal because it enables IT managers to provision services to users faster and in a cost-effective way. However, it does raise some concerns and chief among them is securing data in the cloud because of their operational models, the enabling technologies, and their distributed nature, clouds are easy targets for intruders. Current security defense strategies have many deficiencies which hinder their adoption in a cloud environment. In his presentation, I introduce our Autonomous Cloud Security Framework (ACSF) to define a proper defense strategy for cloud systems. ACSF is an effective attack and vulnerability detection and response framework to accurately identify the attacks and mitigate the risk to the cloud users. ACSF defines a proper defense strategy for cloud systems that is distributed and scalable to adapt the cloud characteristics and to avoid any single point of failure. Furthermore, its flexible architecture integrates both behavior and knowledge based techniques. ACSF collects and correlates security events and user behaviors from all environments in the cloud system and provides a security measure to assess the system risk to automatically select an appropriate response to mitigate the risk consequences. In this presentation, I will focus on two elements only of ACSF:

The first element is the masquerade detection approach and the second element is the autonomic response system that deals with the optimal response selection as a multi-objective optimization problem that calculates, for each alternative response, the minimum of (risk, cost) and maximum of (benefit). Lastly, I will discuss my current research agenda and the ongoing funded research projects.

This research has resulted in two patents in United State Patent and Trade Mark Office (USPTO) and in several papers on main journals and scientific conferences. The main one describes masquerade detection and it appeared on IEEE Transaction on Dependable and Secure Computing Journal while the optimal response selection is described in a paper on the Computing Journal of Springer.

Bio:

Hesham A. Kholidy received his PhD in Computer Science in a joint PhD program between University of Pisa in Italy and University of Arizona in USA. He got the first rank in Galileo Galilei Doctorate School. He works as a postdoctoral associate at the Distributed Analytics and Security Institute (DASI) at College of Electrical and Computer Engineering, Mississippi State University and he leads the Cybersecurity team at DASI. Prior to that, he worked as a program manager of Cybersecurity R&D at IBM branch in Egypt and an assistant professor at the Computer Science department at Fayoum University. During his PhD, he worked as associate researcher in NSF Cloud and Autonomic Computing Center in Electrical and Computer Engineering Dept. at the University of Arizona and he taught some courses there. He holds two patents in Cybersecurity published by United State Patent and Trade Mark Office (USPTO), and he published more than 20 papers on main journals and conferences including IEEE transactions and Springer journals. He participated as PI, Co PI, and senior personnel in 6 research projects funded by NSF, DHS, Italian Government, COIA, and QNRF. His research interests include Cybersecurity and SCADA systems security, distributed and high performance systems, and big data.