Respond to Attacks in the Cloud

Yu-Sung Wu

Assistant Professor, Department of Computer Science
National Chiao Tung University, Taiwan
Tel: +886-3-5712121-56635, Fax: +886-3-572-1490
Email: hankwu@g2.nctu.edu.tw

ABSTRACT

The process of IT consolidation in cloud computing has made the cloud a de facto magnet for security attacks. Incidents such as Facebook plagued by social spamming attacks and Amazon EC2 being used as a stepping-stone in the Sony PSN attack all indicate that security attacks targeting the cloud are now a reality.

Traditionally, protecting IT infrastructure from attack is through the deployment of network intrusion detection system (NIDS) and end-point security protection systems. The approach now faces new challenges in the cloud computing environment. First, the network topology in a cloud environment can change due to dynamic resource consolidation or load balancing. Second, the multi-tenant nature of cloud computing environment means that attack can very possibly originate from a compromised system within the cloud. The distinction between external network and internal network is also blurred in the cloud making it difficult to identify a fixed vantage point in the network for the deployment of network intrusion detection systems. Third, the multi-tenant nature greatly complicates the use of end-point security protection solutions as the deployment requires cooperation from individual tenants and is thereby hard to enforce in practice. Fourth, the resource consumed by individual end-point protection software is not amortized across systems and poses a barrier on the path to resource consolidation as pursued by cloud computing.

In this talk, we will discuss the issues on responding to security attacks in cloud computing environment. The talk will cover the challenges of applying traditional security monitoring systems in an IaaS cloud computing environment. We will continue to discuss a new architecture for building security monitoring and attack response systems for the cloud. The proposed architecture enables unified security monitoring and protection in a multi-tenant cloud environment. It also allows the consolidation of security monitoring resource and helps reduce the cost to defend security attacks in the cloud environment. A prototype system based on a modified Xen hypervisor is built to provide unified and cost-effective anti-virus protection for systems in an IaaS cloud as a proof of concept of the proposed architecture. The system does not require guest components to be pre-installed in individual hosted systems and can attain reasonable performance under the constraint of today's hardware virtualization technologies.

BIOGRAPHY

Yu-Sung Wu received B.S. in electrical engineering from National Tsing Hua University, Hsinchu, Taiwan in 2002, M.S. and Ph.D. in electrical and computer engineering from Purdue University, West Lafayette, Indiana in 2004 and 2009.

In 2009, he joined National Chiao Tung University in Hsinchu, Taiwan, where he is in charge of the Laboratory of SEcurity aNd SytEms (SENSE) in the computer science department. Previously, he had worked at Purdue CERIAS research center conducting research on the design of automated response system for distributed applications and had also worked at Avaya Labs in New Jersey developing intrusion detection solutions for VoIP systems.