Cloud Computing: Threat as a Service?

Prof. Dr.-Ing.
André Miede
University of Applied Sciences Saarbrücken

André Miede is Professor of Computer Science and Business Information Systems at the University of Applied Sciences Saarbrücken (Hochschule für Technik und Wirtschaft des Saarlandes). From 2007 to 2010, he was part of the E-Finance Lab's co-operative PhD program and received a PhD from TU Darmstadt. In addition to his research activities, he worked in the financial services sector as an IT and management consultant for several years.

"The E-Finance Lab facilitates the unique connection of high-class academic research with leading companies in the IT and financial services sector. For years now and hopefully many more to come, this proves the beneficial combination of research approaches with industry experience in order to solve important and difficult problems in the field."

Cloud Computing, initially considered by many to be only a temporary hype, has evolved into an accepted and mature architectural paradigm and service delivery model. It realizes the vision of service-orientation, where service providers offer pools of configurable computing resources and service consumers can dynamically use (or release) resources as their business needs require. Thus, computing is envisioned to become a utility such as electricity or water, ready-to-use right from the network and billed on a pay-as-you-go basis.

Underneath this general concept are three well-known basic service models according to the National Institute of Standards and Technology: Software-as-a-Service (SaaS, complete applications are provided via the Cloud), Platform-as-a-Service (PaaS, consumers deploy their own applications on a platform provided in the Cloud), and Infrastructure-as-a-Service (IaaS, provision of basic computing needs such as processing power, storage, etc. in the Cloud). For the financial services industry, service-orientation in general and Cloud Computing in particular is of great interest, e.g., in order to reduce IT infrastructure costs or to increase business flexibility for rapidly changing markets. This has been continuously shown by E-Finance Lab researchers together with business and IT experts from the industry.

However, serious security and privacy concerns have been and still are a huge obstacle for adopting Cloud Computing, especially in the financial services industry. The responsibles' concerns are that, together with beneficial services as described above, new security threats will arise as additional "services" from the Cloud as well. Of particular interest are the classic "CIA" security goals: Confidentiality (hinder non-authorized access to and disclosure of data), Integrity (protection of data against unauthorized and unnoticed manipulation), and Availability (authenticated and authorized subjects can access and use an IT resource upon demand).

Past research of the E-Finance Lab in this area has investigated serious threatening side-effects of service-orientation and Cloud Computing with respect to revealing sensitive business information of service consumers (see EFL Quarterly 02/2012). In addition, one of Cloud Computing's core concepts and benefits, virtualization, leads to difficult security challenges. Virtualization means that one physical high-performance machine can act like and host multiple virtual ones to its users. This enables fast resource provision as any required machine can be deployed nearly instantly as a Virtual Machine (VM), featuring the attributes requested by the service consumer (operating system, performance, etc.). Because virtualization is a concept that is older than Cloud Computing, many of the arising security challenges are not completely new. However, the circumstances in which they may arise are not always well understood and have to be addressed for a successful adoption of Cloud Computing, e.g., in the financial services industry, where strict and increasing regulatory requirements have to be met.

Two selected security challenges of virtualization are VM Hopping and VM Diversity. With VM Hopping, an attacker on a VM gains access to another VM running on the same physical machine. This threatens all of the above "CIA" goals, especially in the service models PaaS and IaaS. On the other hand, VM Diversity means that a variety of different (virtual) operating systems leads to a configuration nightmare of having a current, secure, and robust system available on the network. These security challenges, among many others, have to be addressed explicitly by the service provider's security management in order to avoid offering new threats as an additional "service".

The research described here is based on a cooperation between the E-Finance Lab and National Chiao Tung University, Taiwan, published, e.g., as Tsai, H.-Y.; Siebenhaar, M.; Miede, A.; Huang, Y.-L. & Steinmetz, R.: Threat as a Service? Virtualization's Impact on Cloud Security. In: IEEE IT Professional, 14 (2012), pp. 32-37.