Securely Launching Virtual Machines on Trustworthy Platforms in a Public Cloud

An Enterprise's Perspective

Mudassar Aslam[1], Christian Gehrmann[1], Lars Rasmusson[1], Mats Björkman[2]
[1]Swedish Institute of Computer Science, Isafjordsgatan 22, Box 1263, SE-164 29 Kista, Sweden
[2]Mälardalens Högskola, Box 883, SE-721 23 Västerås, Sweden
(mudassar, chrisg, lra)@sics.se, mats.bjorkman@mdh.se

In recent years, there has been a tendency to migrate IT services like email, storage, and other applications into the clouds due to cost and maintenance benefits. Several different cloud sourcing models exist like Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). We consider the IaaS cloud model which allows cloud users to run their own virtual machines (VMs) on available cloud computing resources. IaaS gives enterprises the possibility to outsource their process workloads with minimal effort and expense. However, one major problem with existing approaches of cloud leasing, is that the users can only get contractual guarantees regarding the integrity of the offered platforms. The fact that the IaaS user himself or herself cannot verify the provider promised cloud platform integrity, is a security risk which threatens to prevent the IaaS business in general. We address this issue and propose a novel secure VM launch protocol using Trusted Computing techniques. This protocol allows the cloud IaaS users to securely bind the VM to a trusted computer configuration such that the clear text VM only will run on a platform that has been booted into a trustworthy state. This capability builds user confidence and can serve as an important enabler for creating trust in public clouds. We evaluate the feasibility of our proposed protocol via a full scale system implementation and perform a system security analysis.