Nominee: secunet Security Networks AG

Nomination title: SecuStack: A security-hardened Cloud infrastructure for sensitive data and processes

Although companies are outsourcing more and more computing power to the cloud, there is still mistrust in Public Cloud offerings: According to a study by Intel Security, 50% of all companies surveyed say they are suspicious of these solutions (source: https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/#5b2df0918483)

One of the reasons for vulnerability in data centers is the often enormous amount of work involved in encrypting data to be transferred into the cloud. In order to achieve this, companies need to tie up enormous human resources expertise. This is where cloud providers should use their capabilities to help businesses make the cloud a safe place for them.

But the moment, there is still an enormous need for action in this context if cloud providers want to be perceived as trustworthy partners for the secure storage and processing of data in the future.

This is why secunet Security Networks AG, one of the leading German providers of advanced IT security, in cooperation with Cloud&Heat Technologies GmbH, a provider of OpenStack-based public and private cloud solutions, has set itself the goal of making OpenStack more secure. OpenStack is the de facto standard for open source cloud computing and cloud data centers, on which global players also rely on for their public cloud offerings.

Unfortunately, open source solutions are often equipped with different levels of quality regarding security implementations due to the large number of independent developers involved. Many cloud platforms do not yet provide encryption of user images or dedicated encryption of networks in multi-tenant systems. For example, the current cryptographic solutions provided by OpenStack are often rather basic in nature. However, in order to develop a more trustworthy and appealing solution for users with very high security requirements (such as public authorities or banks) in the long term, secunet and Cloud&Heat wanted to use their expertise in the software OpenStack to launch a joint development effort to establish a security-hardened Cloud platform for critical processes and data.

As part of the SecuStack project, an OpenStack-based distribution for public cloud solutions was designed, documented and prototypically implemented, which addresses the necessary security measures to create a secure and trustworthy cloud environment.

The objectives of the project can be summarized in this way:

1. **encryption of sensitive information inside and outside the cloud**
2. **control of key material by the user and optional end-to-end encryption for the transfer and strictly temporary storage and usage of keys**
3. **protecting user data in the cloud while guaranteeing privacy (encryption) as well as integrity (signature)**
4. **hardening of the cloud infrastructure**
5. **network separation and tenant separation with access control**

The innovation and added value of the project is to give the user complete control over his key material, within the bounds of what is currently technically possible. In addition, cryptographic measures and systematic hardening result in a significantly higher degree of separation ("client separation") in the software.

secunet and Cloud&Heat are developing under the condition that with regard to the access to encrypted data (i. e.: images, key material, virtual machine runtime data, persistent block storage, network traffic), a potential attacker or third-party software is technically prevented from accessing this data.

Why nominee should win

The genuine innovations and special features of the project SecuStack provide the ideal solution for industries with extremely high security requirements and policies, such as financial institutions, public authorities, health care, R&D and many more

This secure cloud solution opens up completely new markets for organizations, institutions and private individuals who have previously decided not to enter the cloud for security, cost or human resource reasons.

If entirely new segments of users would declare a Public Cloud as trustworthy, also the providers of innovative cloud solutions and thus the entire IT-industry would participate