Master's Thesis: Adaptive Security Policy Management in Distributed Clouds

Background

Recently emerging concepts like Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) in future will allow service providers offering their customers new ways of service supply – essentially, by adopting Cloud Computing concepts. Datacenter architectures do not only facilitate provisioning of common software as a service, but also infrastructure- and platform-level components in a highly scalable manner.

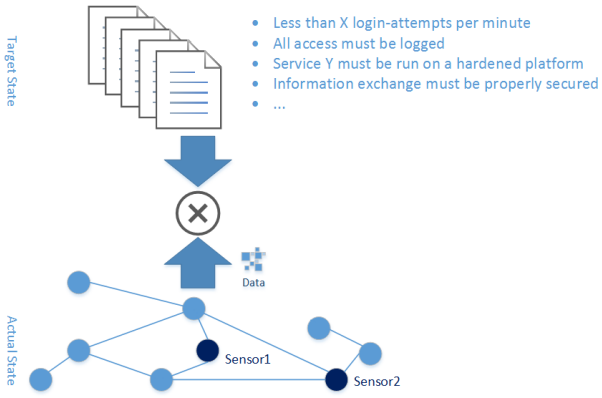

Figure 1

Just as a Cloud's flexibility leverages a quicker and user-friendly service supply, it also brings several challenges for security management in such an environment.

Conventionally, a technical approach for security management in a computer network environment is partially implemented through the alignment of, on the one hand, data which describes the systems' current state (acquired from sensors which are placed at crucial spots on different layers like physical and virtual platforms, operating systems, software and the network), and, on the other hand, predefined conditions agreed among customers and service providers, which are uniformly described via static security policies (cf. Figure 1). However, due to the dynamic nature of Cloud systems and services, continuous changes in risk management and consequently, in the security configuration are required. Manually adapted, static security policies cannot perfectly meet the highly dynamic requirements of a Cloud based service environment. In particular, real-time information about security configuration, events, and emerging threats, demands for a much more dynamic and automated approach for security management. Such policy adaptions, amongst others, encompass threshold modifications, the application of existing policies to new systems as well as condition-refinement.

Designated use cases, for instance, include the relocation of a specific service (i.e., system-migration), handling yet unknown security events, modification of access control rules and automated security incident response.

Task

In this work, the focus of your task is especially on the development of a concept for a security policy management, which provides adaption mechanisms – for instance by application of heuristic methods like pattern matching. The initial step will be the examination of requirements and the selection of a suitable, commonly used security policy description language according to its expressiveness and global acceptance. Further elaboration includes the research of adaption mechanisms respectively to occuring events, the integration into and basic proof-of-concept implementation of approaches in a test environment.

Requirements

- Advanced comprehension of networking and network security
- Basic knowledge of Linux and virtualization technology
- Fundamental programming skills

Organizational

This project originated and is being performed in collaboration with **NOKIA Bell Labs**, which will take part in your assistance. You will have a time limit of **5 month** to perform this work in **German** or **English** language.

Your advisors for this topic are **Michael Steinke** (UniBW), **Iris Adam** (NOKIA) and **Manfred Schäfer** (NOKIA) under supervision of **Prof. Dr. Wolfgang Hommel**.

Contact: **michael.steinke@unibw.de**

der Bundeswehr Universität München

NOKIA Bell Labs