Security Assurance in Virtualized Environments

Virtualized infrastructures and clouds form complex and rapidly evolving environments that can be impacted by a variety of security problems. Manual configuration as well as security checks often cannot keep up with these ever-changing complex systems. The need for automated security assurance analysis is immediate. Given the volatility of virtualized infrastructure configurations as well as the diversity of desired security goals, specialized analysis tools – even though having performance advantages – have limited benefits.

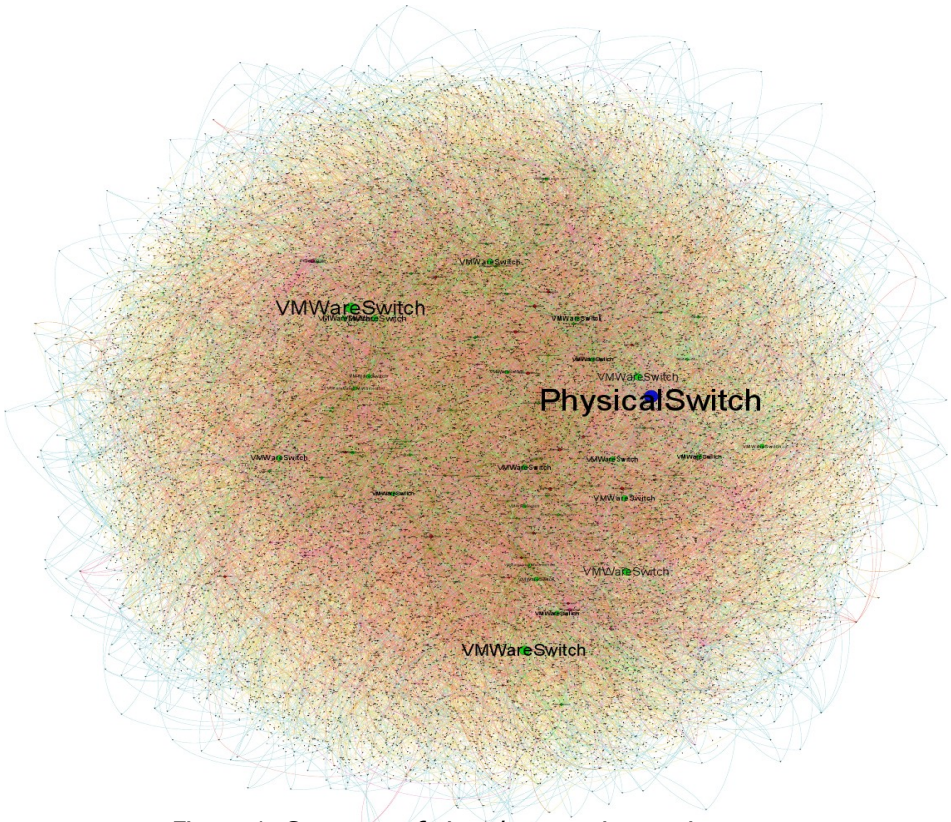

Figure 1: Structure of virtual computing environment

Desired vs. Actual Security State

As a general approach, we first specify abstract security goals as *desired state* for a virtualized infrastructure in a formal language, modeling virtual machines and their connections (VM). For instance, goals can be in the areas *operational correctness* (e.g., "Are all VMs deployed on their intended clusters?"), *failure resilience* (e.g., "Does the infrastructure provide enough redundancy for critical components?") or *isolation* (e.g., "Are VMs of different security zones isolated from each other?").

Second, we employ a generic analysis tool to evaluate the *actual state*, i.e., the virtualized infrastructure configuration, against this desired state. Thus, we obtain an automated analysis mechanism that can check the configuration – and configuration changes – against the high-level security policy.

From engagements with customers running large-scale virtualized infrastructures, we learned that they are interested in a broad range of security goals. Specialized tools can be applied to a subset of these security goals, as we already demonstrated in previous research (cf. [2]) for security zone isolation. However, a general approach is desired that can cover this broad range of security requirements.

Analysis of Static and Dynamic Environments

Such an automated analysis can cover two scopes: in the static case, we analyze a single state of a virtualized infrastructure against the desired properties. In the dynamic case, we consider the actual configuration as a start state and consider transitions that can change this configuration. In our example, we consider particularly changes that an intruder can make to the network (within the limits of his access rights), e.g., by migrating VMs to other security zones. The question is whether we can reach an attack state in this way, i.e., a current configuration of the system that violates the required security properties. The dynamic

SECURITY ASSURANCE IN VIRTUALIZED ENVIRONMENTS

Figure 2: Cloud data centre

case is a generalization of the static case that can only be handled by the model-checking tools.

A Platform for Automated Security Verification

Our goal is to establish general-purpose verification methods as an automated tool for security assurance of virtualized infrastructures. We present a platform that connects declarative and expressive description languages with state-of-the art verification methods. As desired state specification, we take security assurance goals in the formal language VALID [1] as inputs. As actual state, we lift the configuration of a heterogeneous virtualized infrastructure to a unified graph model. For this, we employ a security assurance analysis tool called SAVE [2], which also computes graph coloring overlays, that model, e.g., information flow. We develop a translator that connects these descriptions with the various state-of-the art verification tools. The translation involves adapting the verification problem to the domain of the respective tool, and property-preserving simplifications and abstractions to support the verification. In particular, the translation does not add false positives or false negatives to the model.

References

[1] Bleikertz, S., and Groß, T. A Virtualization Assurance Language for Isolation and Deployment. In IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY) 2011.

[2] Bleikertz, S., Groß, T., Schunter, M., and Eriksson, K. Automated information flow analysis of virtualized infrastructures. In 16th European Symposium on Research in Computer Security (ESORICS) 2011.

Disclaimer

The TClouds project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement number ICT-257243.

Where To Find Security Assurance Technology?

Parts of this technology have been included in the product IBM PowerSC Trusted Surveyor.

Further Information

More information about the Security Assurance in Virtualized Environments technology can be found under Deliverable "D2.3.2 - Components and Architecture of Security Configuration and Privacy Management."

TClouds at a glance

Project number:
257243

TClouds mission:

- Develop an advanced cloud infrastructure that delivers computing and storage with a new level of security, privacy, and resilience.
- Change the perceptions of cloud computing by demonstrating the prototype infrastructure in socially significant application areas.

Project start:
01.10.2010

Project duration:
3 years

Total costs:
EUR 10.536.129

EC contribution:
EUR 7.500.000

Consortium:
14 partners from 7 different countries.

Project Coordinator:
Dr. Klaus-Michael Koch
coordination@tclouds-project.eu

Technical Leader:
Dr. Christian Cachin
cca@zurich.ibm.com

Project website:
www.tclouds-project.eu