# Modeling virtualized infrastructures under security constraints

Muhammad Ali
University of Passau
Innstr.43 94032
Passau, Germany
muhammad.ali@uni-passau.de

Michael Niedermeier
University of Passau
Innstr.43 94032
Passau, Germany
michael.niedermeier@uni-passau.de

Hermann de Meer
University of Passau
Innstr.43 94032
Passau, Germany
hermann.demeer@uni-passau.de

## ABSTRACT

As virtualization is among the current key enabling technologies for both energy-efficient operation as well as reduction of hardware costs, many companies are trying to take advantage by virtualizing their hardware infrastructures. While these advantages make the usage of virtualized infrastructures very appealing, the impact on security is a problem that still needs to be researched. This position paper focuses on the problem of mapping virtual resources onto physical ones while restricting the mapping scheme under security constraints. While proposing a mapping scheme is not a new idea, the main novelty in our work is to take into account the security requirements of virtual resources into the resource mapping equations.

## 1. INTRODUCTION

Pertaining to virtualization, an interesting question for us was the impact of such a new paradigm on the security of the infrastructure. Traditional security solutions are mostly applied as they stand to virtualized resources. There have been surveys to identify new risks and threats pertaining to virtualized environments like [6] where the authors listed several attack efforts to compromise hypervisors. Hyperjacking [3] was yet another effort where programmers were able to successfully install a rootkit. Such efforts arose concerns across the community about the security of this new technology.

In this position paper, we present our initial work to develop a novel solution towards the modeling of virtualized infrastructures constrained under security considerations. The primary question we like to answer is that, given a set of available physical and virtual resources, how can a mapping scheme for these resources under certain security constraints be achieved. The general trend we find today is to reduce the number of physical resources by trying to put as many virtual resources on the same physical hardware, as long as this is possible due to performance and capacity constraints. However, we believe that security is yet another constraint which needs to be carefully considered. In addition, it is also not enough to apply the same traditional security processes on virtualized environments as the requirements and paradigms are different. Examples here are hypervisor vulnerabilities, communication between virtual machines on one physical server or side-channel attacks. The wider perspective is to develop a formal virtual resource security requirements expression language and a corresponding set of ontologies to capture wider range of security requirements. Finally, all the efforts will converge towards the realization of a complete modeling and simulation tool.

## 2. RELATED WORK

A considerable amount of work has already been done within the area of expressing security requirements in different domains. Many approaches have been made to feasibly integrate security requirements in a modeling language. Additional approaches like standalone security expression languages or extending existing standards like UML or MDA have also been proposed in the past. Well-known examples extending UML are e.g. SecureUML [4] or UMLSec [2]. Menzel et.al. [5] give an overview of the creation of security modeling languages and their integration into existing modeling languages. This approach is complimentary to our work.

General security analysis of virtualization has also been done already, for example by [6]. While pinpointing the weak spots of virtualization is an important task on its own, the qualitative results of possible attack vectors is not enough for usage in a security model. However, these existing set of results are complimentary to our work and will serve as an input to our model.

The mapping of virtual onto physical resources has also been researched in the past [1] which investigates the usage of a virtual machine placement system. The most recent effort in this direction can be found in the project EU FP7 "PASSIVE"[1], which started in September 2010. Its goal is to develop a security architecture that helps managing security in a virtualized environment. While there is no published work that originated from the project until now, the importance of this topic becomes clear by the extensive funding of PASSIVE through the EU.

[1]Policy-Assessed system-level Security of Sensitive Information processing in Virtualised Environments

## 3. OUR APPROACH

We define $P$ as a set of, 1 to n, available physical resources. Each of the physical resources $p_n \in P$ can be expressed as a tuple $(A_{p_n}, c_{p_n})$ where $A_{p_n}$ is the set of attributes with $|A_{p_n}| \geq 0$ and $c_{p_n}$ is the max available capacity in units, $c_{p_n} \geq 0$. Each of the attributes can be considered as a name-value pair.

Additionally, we define a set of, 1 to m, virtual resources $V$ which need to be mapped on the available physical resources. Here we are not taking into consideration the mapping of offered services onto virtual resources and assume an equal mutually exclusive set of services assigned to each virtual resource. A virtual resource $\vartheta_m \in V$ can be represented by a tuple $(A_{\vartheta_m}, \lambda_{\vartheta_m})$ where $A_{\vartheta_m}$ is the set of attributes each represented as a name value pair while $\lambda_{\vartheta_m}$ is the set of, 1 to n, tuples $(p_n^{\vartheta_m}, c_n^{\vartheta_m})$ where $p_n^{\vartheta_m}$ is a $n^{th}$ physical resource on which the $\vartheta_m$ is dependent upon and $c_n^{\vartheta_m}$ is the respective required capacity. $c_n^{\vartheta_m} = 0$ implies that $\vartheta_m$ is not dependent on $n^{th}$ physical resource (or $p_n$).

Thus, the condition $\forall p_n^{\vartheta_m} \in \lambda_{\vartheta_m} \; \exists \; p_n \in P \mid p_n = p_n^{\vartheta_m}$, ensures that the required physical resources must be available; otherwise the virtual resource can not be mapped. In addition, $\forall p_i^{\vartheta_m}, p_j^{\vartheta_m} \in \lambda_{\vartheta_m}, \; p_i^{\vartheta_m} \neq p_j^{\vartheta_m}$, implies that each virtual resource must only specify a certain physical resource only once.

Generally, the mapping problem here is to design a mapping function $f: V \rightarrow P^*$ under the simple constraint that the required capacities must not exceed the available capacity for any individual physical resource $\Rightarrow \forall p_n \in P, c_{p_n} \geq \sum c_n^{\vartheta_m}$.

We now extend the above model to incorporate security requirements. We assume that each virtual resource may need a certain set of security requirements and thus we now represent $\lambda_{\vartheta_m}$ by a tuple $(p_n^{\vartheta_m}, c_n^{\vartheta_m}, \omega_n^{\vartheta_m})$ where $\omega_n^{\vartheta_m}$ is the set of security constraints[2] which must be preserved when mapping virtual resource $\vartheta_m$ onto physical resource $p_n$.

Furthermore, we extend the representation of physical resource by incorporating an additional element $\Delta_{p_n}$ within the previously defined tuple and thus a physical resource $p_n$ will now be expressed as a tuple $(A_{p_n}, c_{p_n}, \Delta_{p_n})$. We term $\Delta_{p_n}$ as a security context represented as a collection of context variables and supported actions. This collection as a whole present a state of the security context at any time instant. We term *"security context"* as a logical entity spanning the context of physical resource plus any virtual resources already occupying it.

The extended mapping problem will now include an additional constraint to map security requirements of the virtual resource to the security context of the physical resource. We define the relation "$\lhd_D$" as *compatible with the degree* $D$ where $0 \leq D \leq 1$ is the threshold variable which can be varied to fine tune the system. This relation between the requirements and security context is being evaluated to map virtual resources onto physical ones.

[2]We use the terms *requirements* and *constraints* interchangeably in the text

Mathematically:

$$f: V \rightarrow P^* \text{such that} \tag{1}$$

$$\forall p_n \in P, c_{p_n} \geq \sum c_n^{\vartheta_m} \tag{2}$$

$$\forall p_n \in P, \vartheta_m \in V, \omega_n^{\vartheta_m} \lhd_D \Delta_{p_n} \tag{3}$$

We specifically focus on the Equation 3 in our work which pertains to resolving security constraints and security context capabilities. The representation of $\omega_n^{\vartheta_m}$ and $\Delta_{p_n}$ is the current focus of our work. Both entities are interrelated, as virtual resource requirements are being mapped onto the target security context. They both could contain expressions spanning from very simple to very complex forms and our goal is to formalize such statements.

Summing up, it has to be noted that, although virtualization is one of the most noticeably rising technologies, there are currently no modeling and simulation techniques available that have the ability to express the security requirements that come along when trying to co-locate different virtual resources onto physical ones.

## 4. ACKNOWLEDGMENTS

The research leading to the results presented in this paper has been jointly funded by EuroNF SJRP.44 SPEC project and "Ausbau der Kompetenzpartnerschaft zum Themenschwerpunkt 'IT-Sicherheit' an den Standorten Passau und Regensburg" which is co-funded by the European Union's European Regional Development Funds - Regional Competitiveness and Employment (in German: Europaeischer Fonds fuer regionale Entwicklung - Regionale Wettbewerbsfaehigkeit und Beschaeftigung).

## 5. REFERENCES

[1] C. Hyser, B. McKee, R. Gardner, and B. J. Watson. Autonomic virtual machine placement in the data center. Technical report, HP Laboratories, February 2008.

[2] J. Juerjens. Umlsec: Extending uml for secure systems development. In *Proceedings of the 5th International Conference on The Unified Modeling Language*, pages 412–425, 2002.

[3] S. T. King, P. M. Chen, Y. Wang, C. Verbowski, H. J. Wang, and J. R. Lorch. Subvirt: Implementing malware with virtual machines. In *In IEEE Symposium on Security and Privacy*, pages 314–327, March 2006.

[4] T. Lodderstedt, D. Basin, and J. Doser. Secureuml: A uml-based modeling language for model-driven security. In *UML 2002 - The Unified Modeling Language. Model Engineering, Languages, Concepts, and Tools. 5th International Conference*, volume 2460, pages 426–441, Dresden, Germany, September/October 2002.

[5] M. Menzel and C. Meinel. Securesoa - modelling security requirements for service-oriented architectures. In *2010 IEEE International Conference on Services Computing*, 2010.

[6] E. Ray and E. Schultz. Virtualization security. *CSIIRW '09: Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research*, pages 1–5, 2009.