

# Sicherheit, Virtualisierung und Einbruchstoleranz: Herausforderungen für zukünftige Systemsoftware

Hans P. Reiser

LaSIGE, University of Lisboa

Während bei der Hardware weiterhin eine rasante Entwicklung beobachtet werden kann, ist bei der Sicherheit von Systemsoftware immer noch ein eklatantes Defizit festzustellen. Beispielsweise werden in der National Vulnerabilities Database<sup>1</sup> jährlich tausende Schwachstellen in Standardsoftware dokumentiert, und einem Angreifer ist es heutzutage problemlos möglich, Schwachstellen von Rechnern so auszunützen, dass er Botnets mit Millionen von fremden Rechnern bilden kann<sup>2</sup>. Tendentiell sind diese Probleme in den letzten Jahren eher größer geworden, als dass sie durch geeignete Konzepte gelöst oder zumindest gemildert werden konnten.

Bei der Systemsoftware müssen künftige Entwicklungen also nicht nur die Herausforderungen neuer Hardwarearchitekturen lösen, sondern dabei auch die zentrale Frage der Sicherheit adressieren. Mit diesem Beitrag möchte ich zwei Konzepte zur Diskussion stellen, die in den nächsten Jahren bei der Entwicklung von Systemsoftware für sichere und vertrauenswürdige Dienst-Infrastrukturen eine bedeutende Rolle spielen werden:

## 1. Virtualisierung als Chance

Im Desktop- und Serverbereich haben marktübliche Betriebssysteme eine Komplexität erreicht, die es in absehbarer Zeit unmöglich macht, deren Sicherheit und Korrektheit zu garantieren. Virtualisierung bietet nun die Chance, unterhalb des (möglicherweise unsicheren) Betriebssystems eine *vertrauenswürdige Komponente* zu etablieren. Hierzu darf sich die Entwicklung von Virtualisierungslösungen nicht allein auf Ressourcenverwaltung und Vereinfachung der Administration fokussieren. Neue Konzepte zur Entwicklung von Systemsoftware müssen vielmehr den Aspekt Sicherheit in den Mittelpunkt stellen. Eine derartige sichere und vertrauenswürdige Infrastruktur ist auch eine Grundvoraussetzung, dass Entwicklungen wie „Cloud Computing“ eine erfolgreiche Zukunft haben.

## 2. Einbruchstoleranz

Die Komplexität heutiger IT-Systeme macht es notwendig, bei der Sicherheit nicht nur die *Vorbeugung* zu betrachten, sondern auch Konzepte für die *Tolerierung von Fehlern und Einbrüchen* zu entwickeln. Ziel der Forschung in diesem Bereich sollte es sein, System-Infrastruktur so zu entwickeln, dass mit möglichst geringem Aufwand eine möglichst gute Einbruchstoleranz erreicht wird. Der Einsatz von durchgehender *N-Versionen-Programmierung* ist dabei aus Aufwands- und Kostengründen oft kaum realistisch. Hier kann die Ausnützung von Heterogenität von Standardsoftware (z.B. von Betriebssystemen) vorteilhaft sein.

Mein Forschungsprojekt „**VM-FIT**“ (Virtual Machine based Fault and Intrusion Tolerance)<sup>3</sup> beschäftigt sich mit der Kombination von Virtualisierung und Einbruchstoleranz. Es konnte darin gezeigt werden, dass unter der Annahme einer vertrauenswürdigen Virtualisierungsschicht eine wesentlich einfachere Realisierung von Einbruchstoleranz möglich ist. Zwei wesentliche Vorteile sind, dass die Anzahl der erforderlichen Replika-te gegenüber traditionellen Ansätzen verringert werden kann sowie die Replikationskosten (insbesondere der Kommunikationsaufwand) reduziert werden können. Auch eine proaktive Systemwiederherstellung zur Korrektur von fehlerhaften Rechnern lässt sich mit Hilfe von Virtualisierung signifikant einfacher und effizienter realisieren.

Abschließend lässt sich beobachten, dass Entwicklungen im Hardwarebereich (z.B. omnipräsente Internet-Konnektivität, heterogene vernetzte Kleinstgeräte) dazu führen, dass Dienst-Infrastrukturen zukünftig Adaptivität, Interoperabilität, Skalierbarkeit und dynamische Komposition von Diensten bieten müssen. Bei diesen zukünftigen Entwicklungen stellt die Sicherheit der System-Infrastruktur die zentrale Herausforderung dar. Dabei ist diese als integraler Bestandteil der Systementwicklung zu begreifen, nicht als „Add-On“, das später nachträglich hinzugefügt wird. □

<sup>1</sup>National Vulnerability Database, NIST, <http://nvd.nist.gov/>

<sup>2</sup>Peter Gutmann (31. August 2007). „World's most powerful supercomputer goes online“. Full Disclosure. <http://seclists.org/fulldisclosure/2007/Aug/0520.html>. Abgerufen 2009-08-31

<sup>3</sup>Hans P. Reiser, Rüdiger Kapitza: Hypervisor-based Efficient Proactive Recovery Proc. of the 26th IEEE Symp.on Reliable Distributed Systems - SRDS'07