

The Nizza Security Architecture

Michael Hohmuth Hermann Härtig

Technische Universität Dresden
Dept. of Computer Science
Operating Systems Group

August 8, 2004

The Nizza security architecture aims at reducing the size of a system's Trusted Computing Base (TCB) by an order of magnitude in comparison to systems based on traditional operating systems such as Linux or Windows. We aim at a complexity of 50 K lines of trusted code, whereas a typical Linux system needs to trust 500 K lines of code for the kernel alone (in a typical x86 configuration).

Nizza uses a second-generation L4 microkernel as its security kernel. It offers secure booting and attestation. The TCB is kept small through radical reuse of existing untrusted code through *trusted wrappers*. Depending on an application's security requirements, even untrusted drivers can be used through DMA virtualization. We support legacy applications through L⁴Linux, a paravirtualized version of the Linux kernel running in untrusted mode.

Nizza requires less hardware modifications than Microsoft's Next-Generation Secure Computing Base (NGSCB, neé Palladium) architecture. Isolation is provided through address spaces, and a secure GUI allows secure components to provide overlapping windows without graphics-adaptor modifications. Nizza applications can be built such that they do not depend on functionality of untrusted legacy-OS components to avoid denial-of-service attacks. In comparison to pure virtual-machine-based approaches, Nizza supports fine-grain protection domains that are more light-weight than a virtual machine.

In the WiP talk, we present the Nizza components we are developing or have already developed, and a first Nizza application, a virtual-private-network (VPN) implementation with IPSec support with currently about 58 K lines of trusted code.