

COMPUTER SCIENCE COLLOQUIUM

Department of Computer Science
City University of Hong Kong

L4/Nizza and VPFS, its Secure Storage Component

Prof Hermann Härtig
Professor for Operating Systems
Faculty of Computer Science
Dresden University of Technology
Germany

Date :

15 February 2008 (Friday)

Time :

10:30am - 11:30am (Refreshment will be served at 10:15am)

Venue

CS Seminar Room, Rm Y6405, 6th Floor Yellow Zone, Academic Building,
City University of Hong Kong, Tat Chee Avenue, Kowloon Tong.

Abstract

The L4/Nizza security architecture is designed to support security-sensitive applications by drastically reducing the sizes of such applications' Trusted Computing Base (TCB). We achieve this by splitting an application into an untrusted and a security-sensitive part. The untrusted part runs on a legacy operating system in a virtual machine (for example on L4Linux, a paravirtualized implementation of the Linux kernel). The sensitive part relies only on a small set of components that are relevant for its security goals. These components and the sensitive part of the application form the TCB of that application.

VPFS, a Virtual Private File System, is the secure storage component of L4/Nizza. Its security goals are confidentiality, integrity (discovery of unauthorized modifications) and recoverability of data. Following L4/Nizza's general approach, VPFS is split into two components. The untrusted component reuses an existing file-system implementation for data storage, whereas a small trusted component protects the data using cryptographic algorithms and some hardware support. If an application needs such secure storage, our VPFS prototype adds less than 5000 lines of code to that application's TCB.

Biography

Prof. Härtig obtained his Diploma and PhD from Education in Karlsruhe. From 1984-1994, he worked at German National Research Center for Computer Science. He joined Dresden University of Technology (TU Dresden) in 1994 where he is currently a full professor of Computer Science. He has held visiting positions in numerous research labs and Universities including UC Berkeley, MIT, Hebrew Univ., UNSW and Intel Microprocessor research labs.

Prof. Härtig's research focuses on micro-kernel and virtualization technology applied to systems security and real-time systems. In real-time, Prof. Härtig's team has ten-year experience in devising the DROPS architecture and in building components, including small real-time micro-kernels and real-time managers for disks, communication and windowing systems. In systems security, Prof. Härtig's team has devised the L4/Nizza architecture that supports legacy software together with applications with very high security requirements. More details about Prof. Härtig's work can be found at <http://tudos.org/>.

* * * * *

*In case of questions, please contact Dr Guoliang Xing at Tel: 2788 7525, E-mail: glxing@cs.cityu.edu.hk,
or visit the CS Departmental Seminar Web at <http://www.cs.cityu.edu.hk/>.*