



# Safe Binary Device Driver Reuse via User-level Binary Translation

Rong Chen Zhijun Hao Kang Liu Haibo Chen Binyu Zang  
{chenrong, zjhao, liukang, hbchen, byzang}@fudan.edu.cn

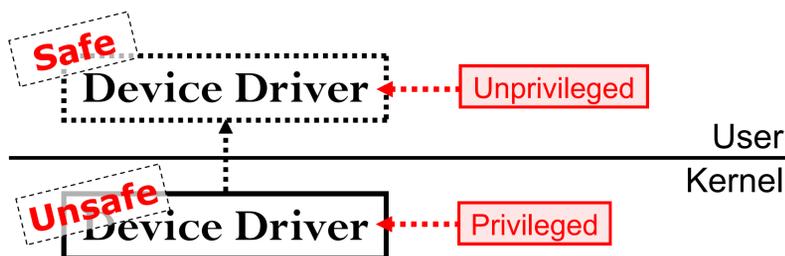
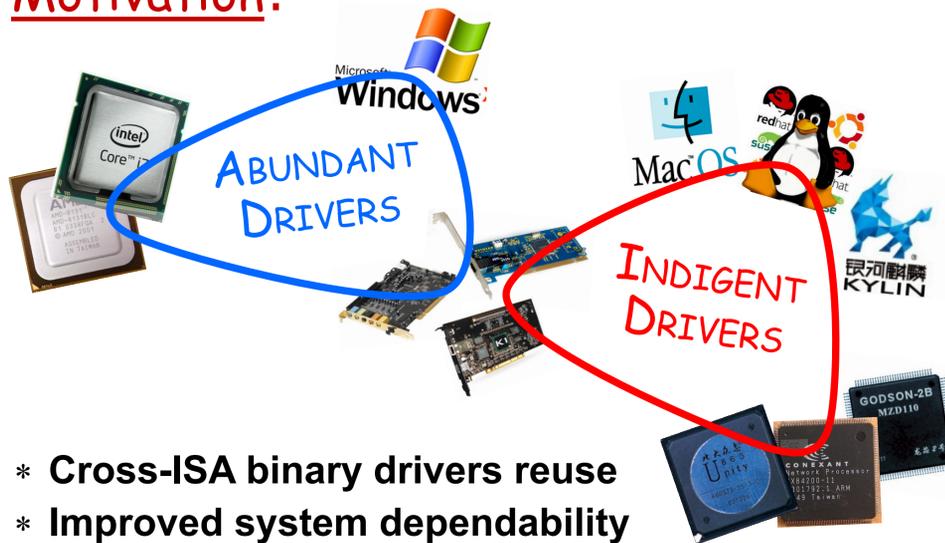
Fudan University

## Abstract:

The maturity of new operating systems heavily depends on the enrichment and diversity of device drivers. The hardware manufacturers, however, usually only provide binary drivers to most commercial OS. Meanwhile, device drivers in commodity OS usually execute in most privileged level and are the majority causes of system failures. Previous techniques either require the modification of source code of drivers or incur large resource overhead, and all of them are not support the reuse of drivers across different ISAs

We propose to use dynamic binary translation to cross-ISA reuse binary device drivers, and improve system dependability. The basic idea is transplanting device drivers at the binary level and using a glue layer to emulate the interfaces of the original OS.

## Motivation:

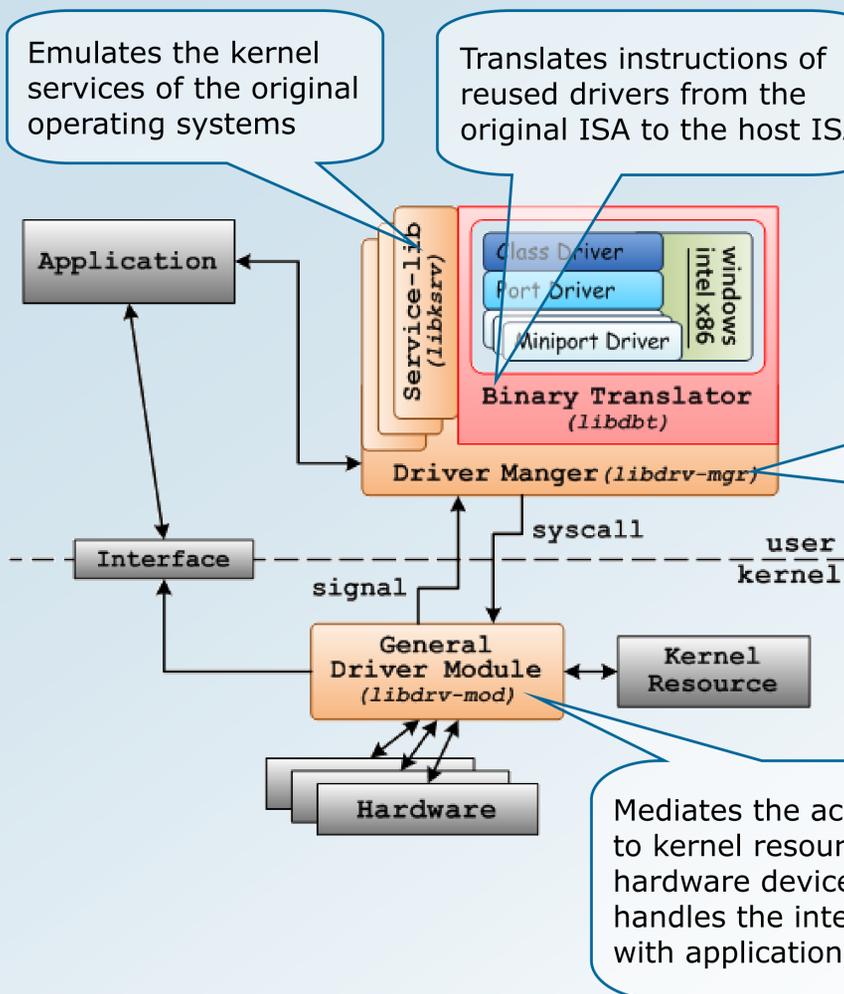


Emulates the kernel services of the original operating systems

Translates instructions of reused drivers from the original ISA to the host ISA

## Our Solution:

Use dynamic binary translation to reuse binary device drivers cross ISAs, and improve system dependability through encapsulating the driver within a user mode process.



Glues the device drivers and the service libraries, and communicates with the module within kernel

Mediates the accesses to kernel resources and hardware devices, and handles the interactions with applications

## early-stage prototype

- \* **Source ISA:** Intel x86
- \* **Target ISA:** Utiy(arm-like)
- \* **Source OS:** Windows XP
- \* **Target OS:** Linux 2.6
- \* **DBT:** based on qemu-0.11.0
- \* **Driver:** network and sound
- \* **Libksrv:** 43/168 interfaces
- \* **Libdrv-mgt:** driver boot
- \* **Libdrv-mod:** driver boot