MEMORY SHARING REVISITED

Work in Progress

4th EuroSys Conference
Nuremberg, Germany
2 April 2009

Jorrit N. Herder <jnherder@cs.vu.nl>
Dept. of Computer Science
VU University Amsterdam

THE NEED FOR DRIVER ISOLATION

- **Memory corruption is major crash cause**
- **Device drivers need access to memory**
  - OS data structures
  - Application memory

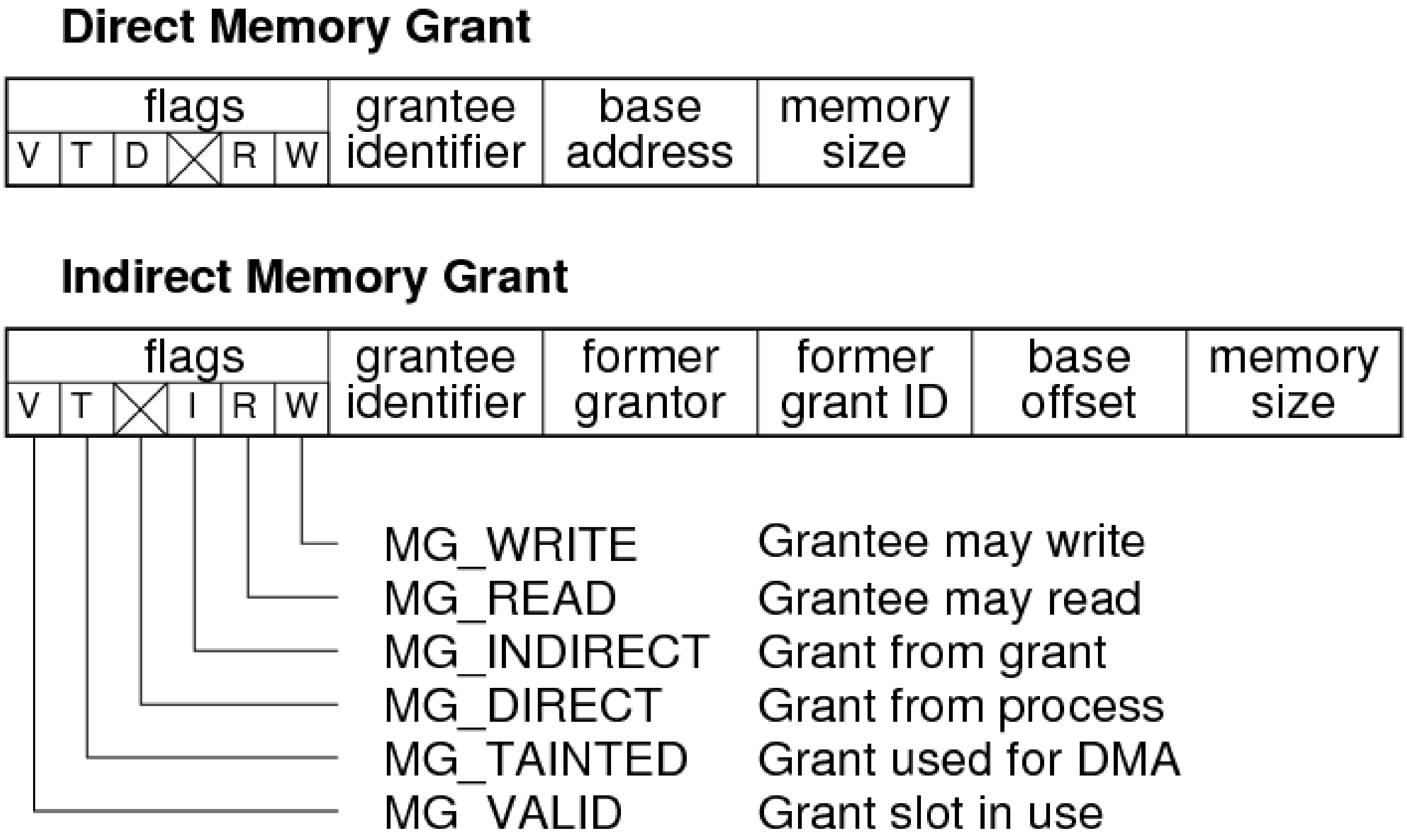
EXISTING PROTECTION SCHEMES

- **System V IPC and POSIX Shared Memory**
- **Not suitable for low-level device drivers**
  - Coarse-grained, page-based protection
  - Protection based on UID, not on process
  - Access rights cannot be delegated
  - No seamless integration for safe DMA
  - No automatic cleanup after driver crash

MEMORY GRANTS

- **Safe memory access based on least authority**
  - Precise, byte-granularity memory area
  - Fine-grained, per-process access rights
- **Privileged grant operations mediated by kernel**
  - Memory copying
  - Memory mapping
  - Direct memory access
- **Delegation supported via indirect grants**

GRANT STRUCTURE



Direct Memory Grant

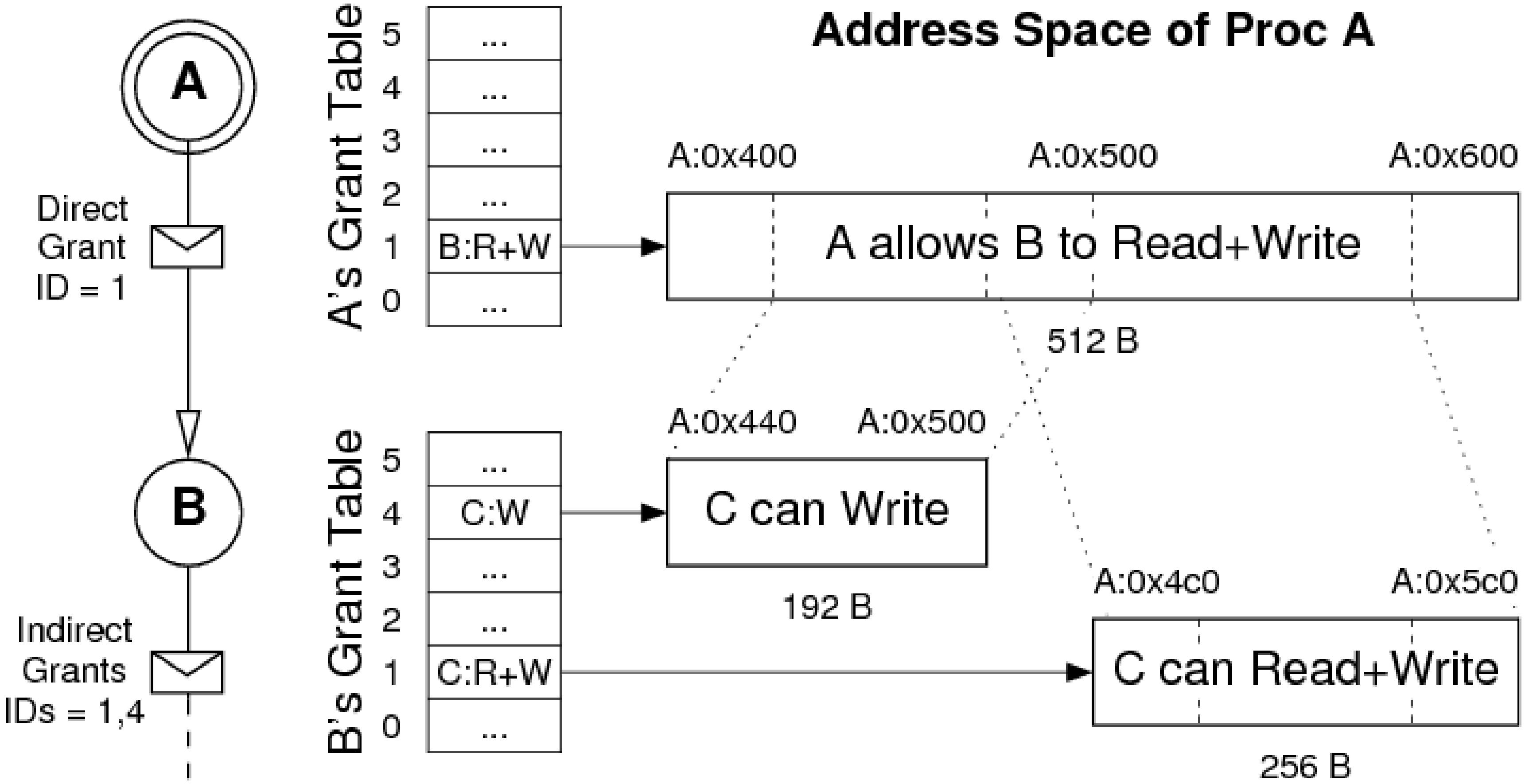
flags						grantee identifier	base address	memory size
V	T	D	☒	R	W			

Indirect Memory Grant

flags						grantee identifier	former grantor	former grant ID	base offset	memory size
V	T	☒	I	R	W					

MG_WRITE	Grantee may write
MG_READ	Grantee may read
MG_INDIRECT	Grant from grant
MG_DIRECT	Grant from process
MG_TAINTED	Grant used for DMA
MG VALID	Grant slot in use

GRANT STRUCTURE



A's Grant Table

5	...
4	...
3	...
2	...
1	B:R+W
0	...

B's Grant Table

5	...
4	C:W
3	...
2	...
1	C:R+W
0	...

THANK YOU

- **Download WIP paper from EuroSys website**
- **Visit me during EuroSys poster session**

Are you a student, love to hack systems, and have some spare time?

MINIX 3 takes part in GSOC 2009 ... pick up the flyer for more info!