CERIAS

The Center for Education and Research in Information Assurance and Security

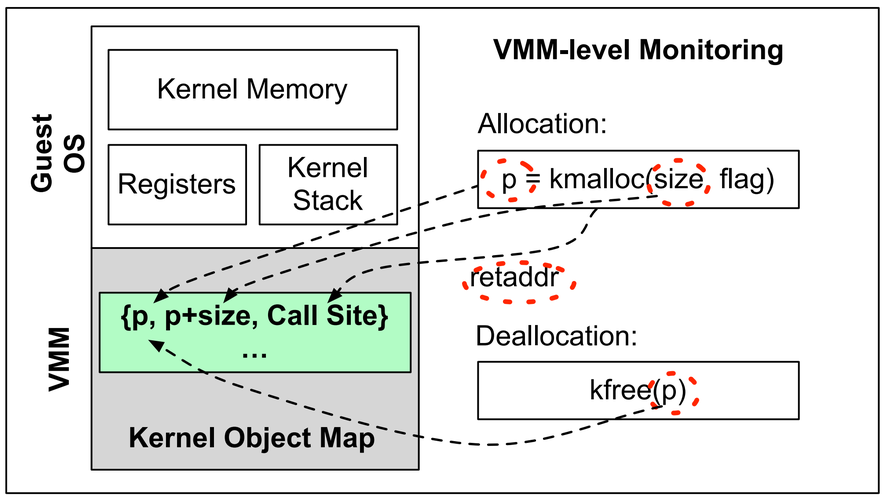
KMAG: VMM-level Malware Detection via Kernel Data Access Profiling

Chung Hwan Kim[*], Dannie Stanley[*], Rick Porter[+], Dongyan Xu[*]

[*]Purdue University and CERIAS, [+]Applied Communication Sciences

Monitoring Kernel Object [De]allocations

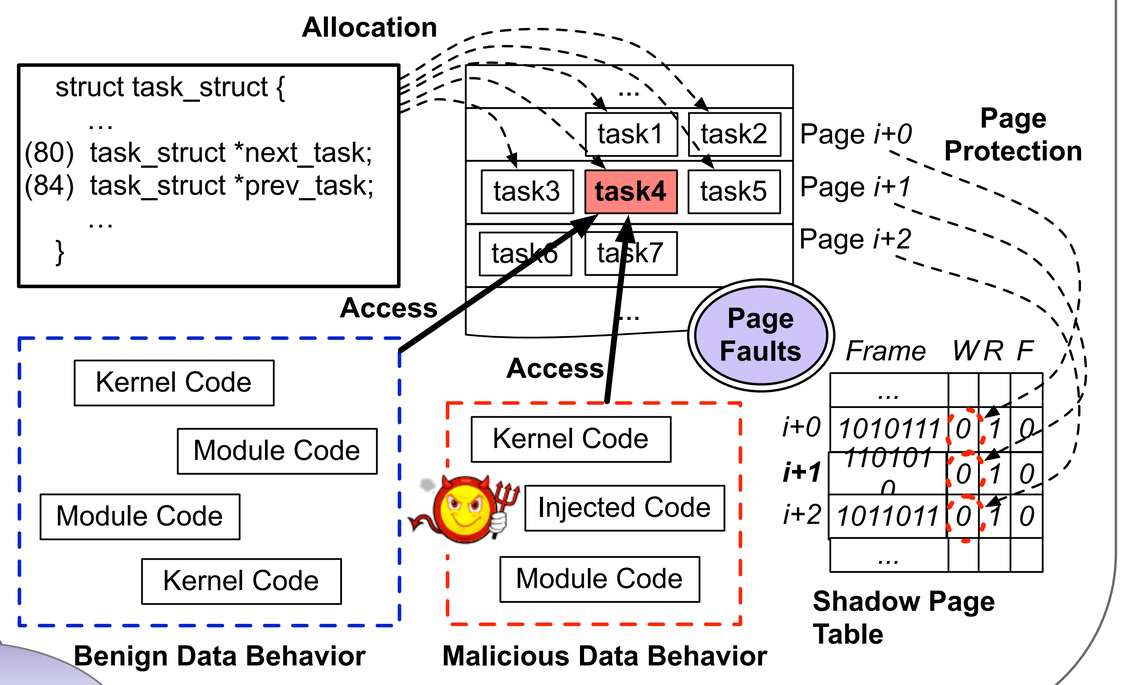
- Static objects are identified using kernel-exported mapping information.
- Dynamic object [de]allocations are reported by annotated kernel memory functions with hypercalls.
- Memory ranges are extracted from function arguments and return values.
- Call stack information is used to derive data types.



Key Idea: Allocation call sites can be used as constant kernel object identifiers.

Page-level Kernel Data Access Monitoring

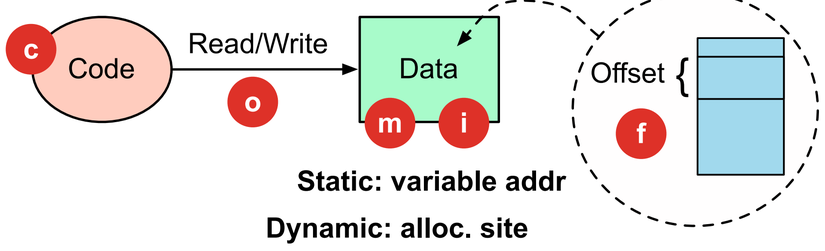
- Pages that contain allocated kernel objects are protected in the shadow page table.
- Accesses to kernel objects are recorded or examined when shadow page faults occur.
- Pages are unprotected, and protected back after faulting instructions are executed, if benign accesses.



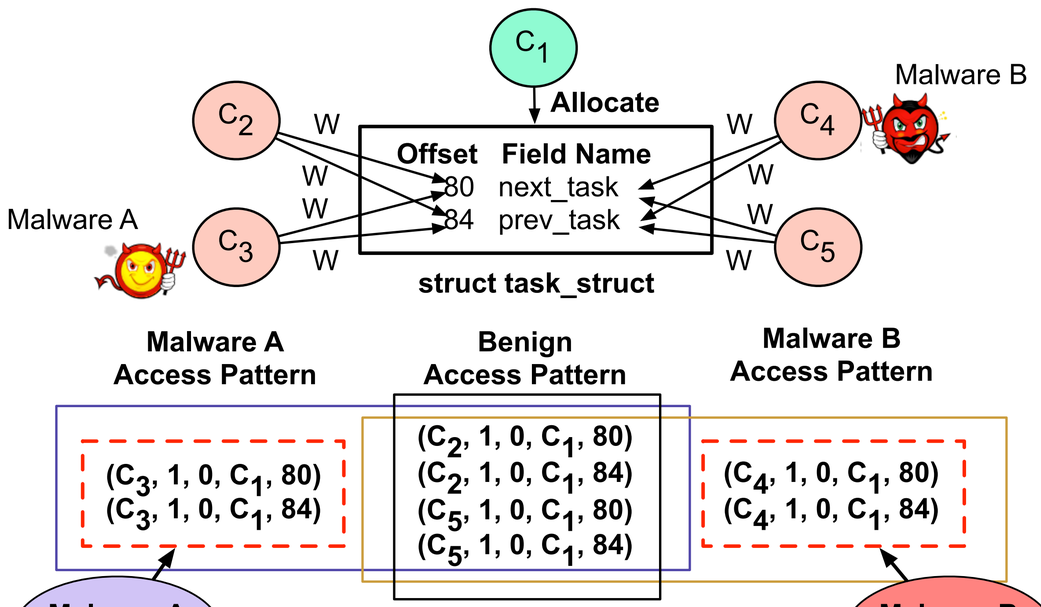
KMAG: Kernel Memory Access Guard

Access Pattern Training & Malware Detection

- Encoding a memory access pattern



- Summary of kernel memory accesses (data access profile)



Similar or same malware can be detected by matching signatures during runtime.

Detection of Kernel Exploits & Conclusion

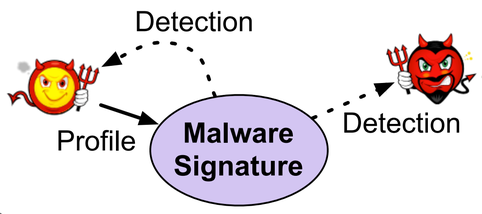
Exploit Name	# of Manipulated Objects	Manipulated Data		Attack Vector
		Type	Field	
hp	# of hidden processes	task_struct	next_task, prev_task	LKM
dr-rootkit	1	task_struct	uid, euid, gid, egid	LKM
linux-sendpage	1	task_struct	uid, euid, gid, egid	Kernel
adore-ng	1	module	list.next, list.prev	LKM

Conclusion

- Most malware attacks involve kernel data accesses; *Kernel Rootkit Profiling [Eurosys '09], [RAID '09]*.
- Data access patterns can match malware variants with common data targets.
- Data-centric kernel malware analysis can be performed transparently and effectively at VMM level.

Research Status

- Working on further evaluations and optimizations.



Demo

Author

CERIAS

PURDUE UNIVERSITY