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.

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.

Access Pattern Training & Malware Detection
- Encoding a memory access pattern
- Summary of kernel memory accesses (data access profile)

Detection of Kernel Exploits & 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.