Putting Trust in Malicious Systems

Jon Giffin
Georgia Tech

giffin@cc.gatech.edu

Issues

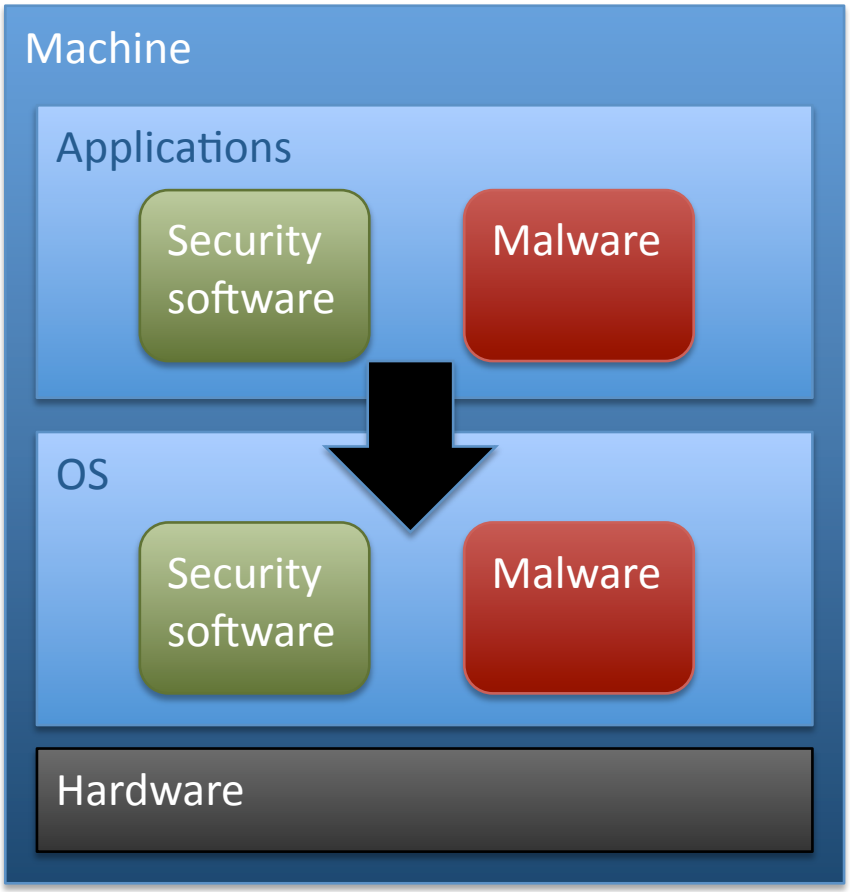
Defense: can security software reliably use virtual environments?

Design: what will hypervisors look like in five years?

Traditional trust

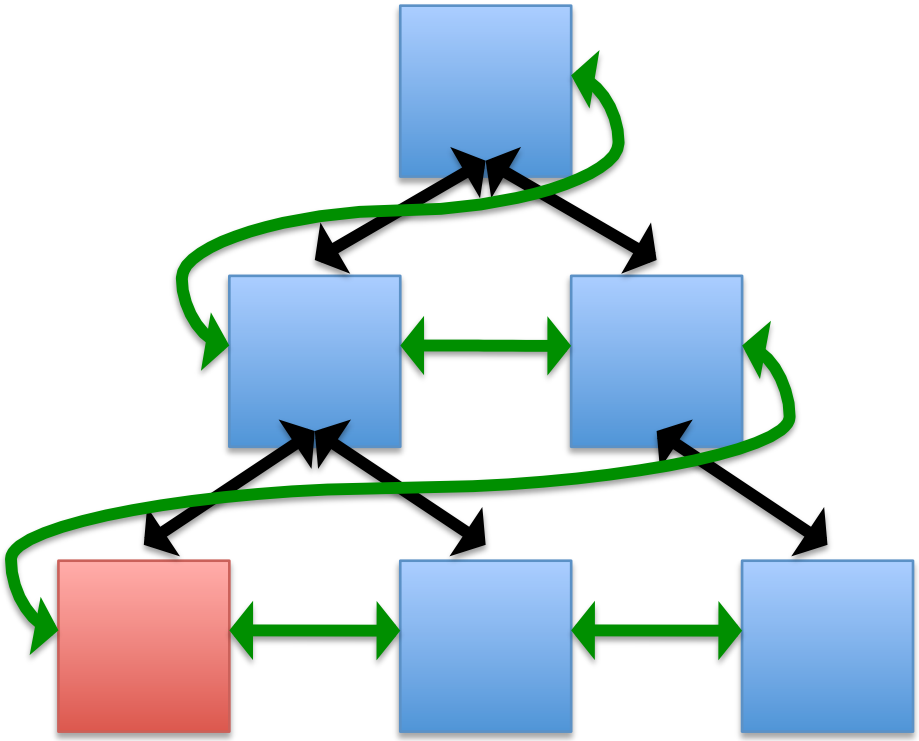
Truism: Whoever controls the lowest layer wins

Traditional software security architectures rely on unsafe trust relationship



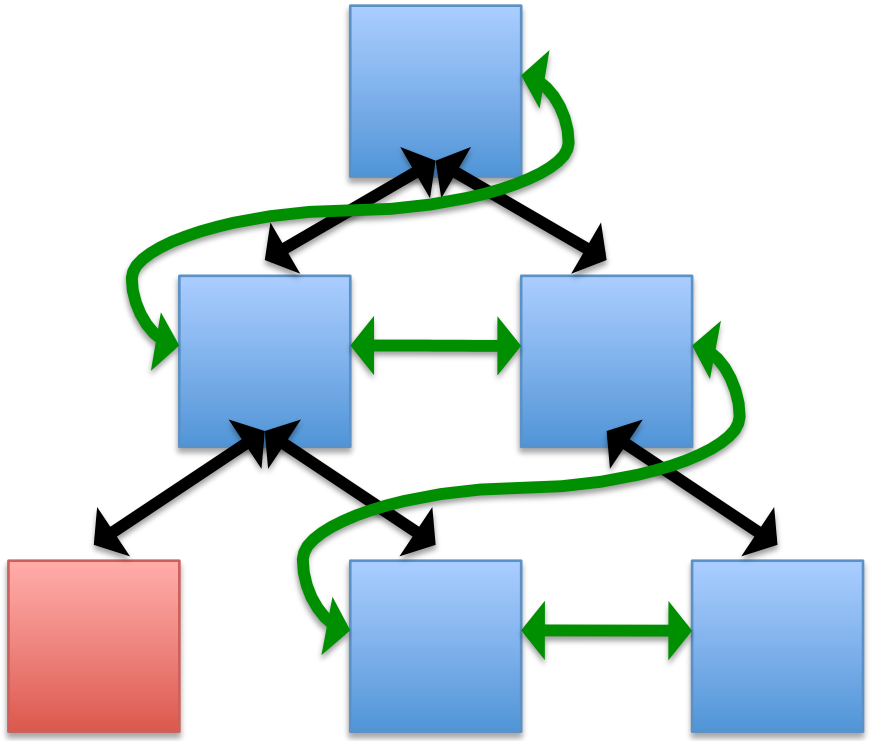
Kernel-level malware

Unhook process from accounting list

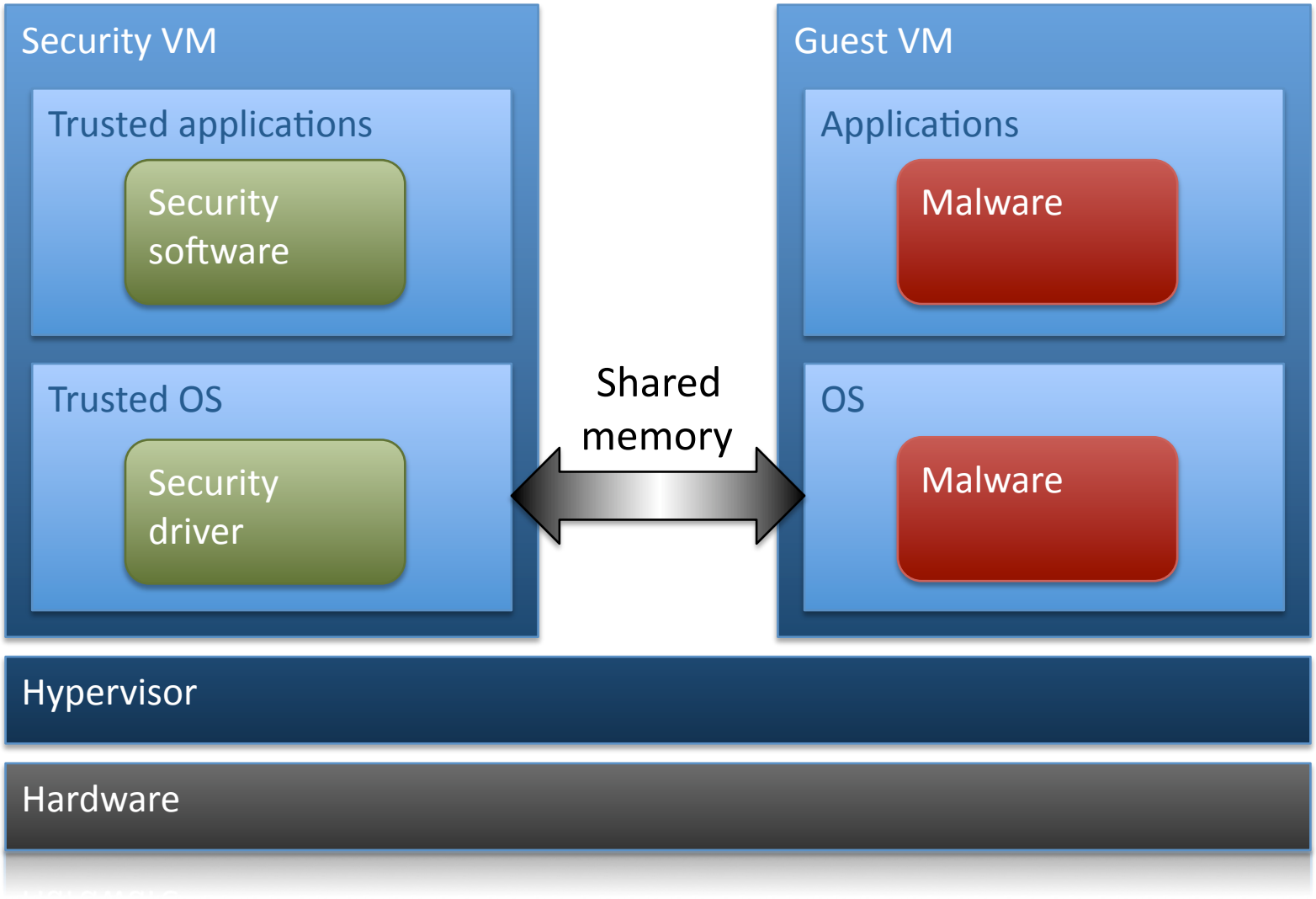


Kernel-level malware

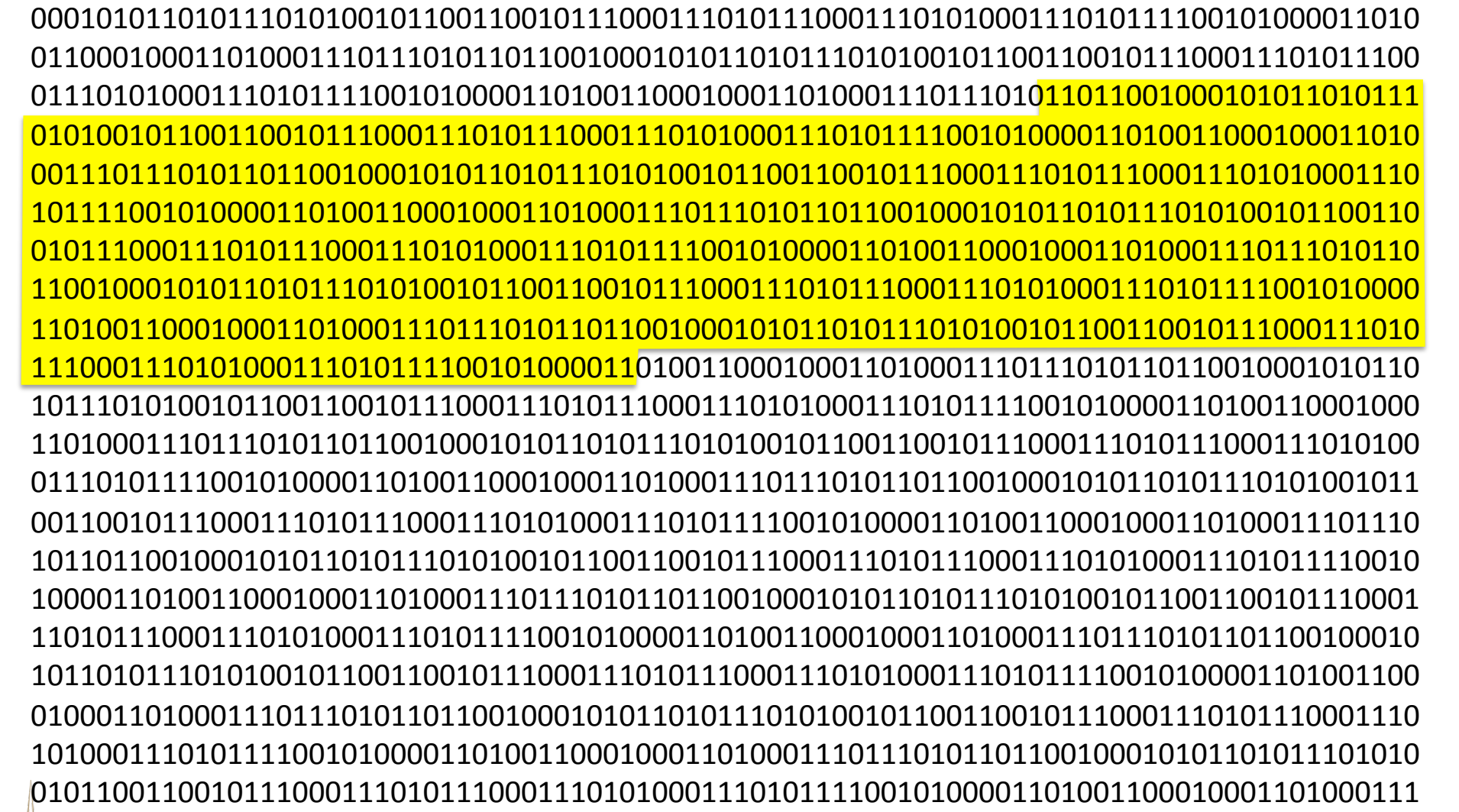
Unhook process from accounting list



Modern architecture

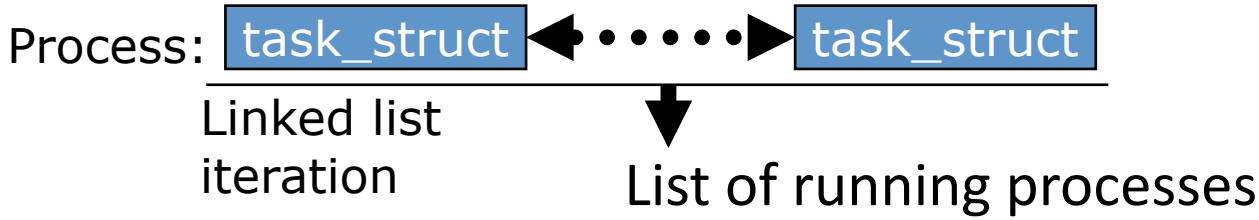


Virtual machine introspection



Virtual machine introspection

- Assign semantic meaning to raw memory bytes
  - Exported symbols
  - Predefined knowledge of kernel data types



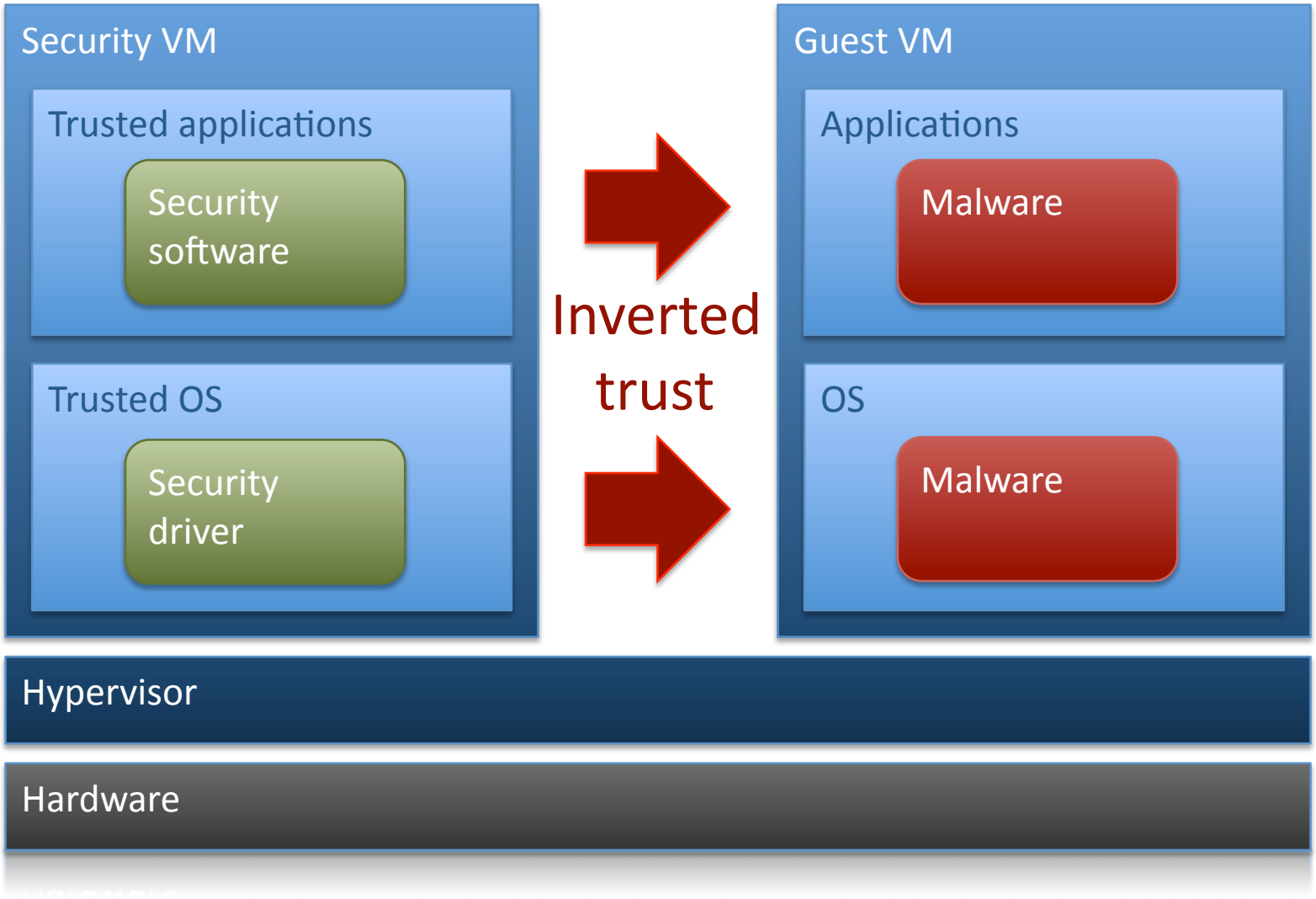
Virtual machine introspection

So… attackers can alter kernel dynamic data structures…

… and VMI-based utilities will build the incorrect view of victim VM…

… in the same way they would have had they been executing directly on the victim machine.

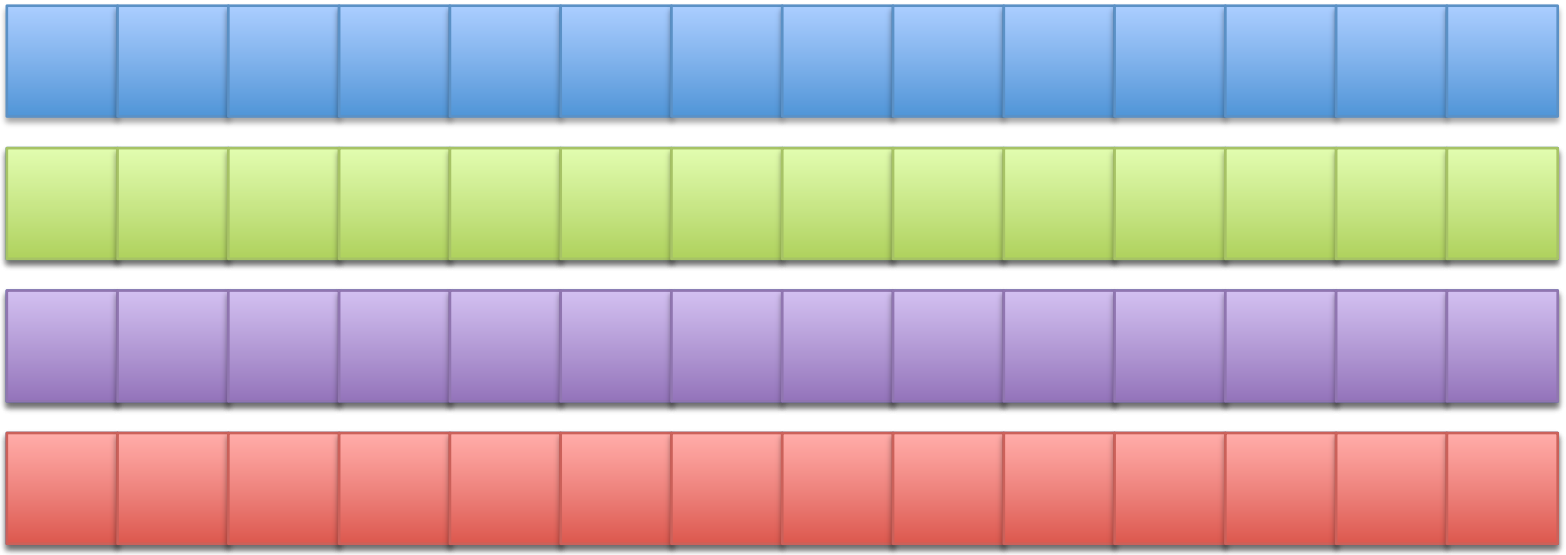
Trust inversion



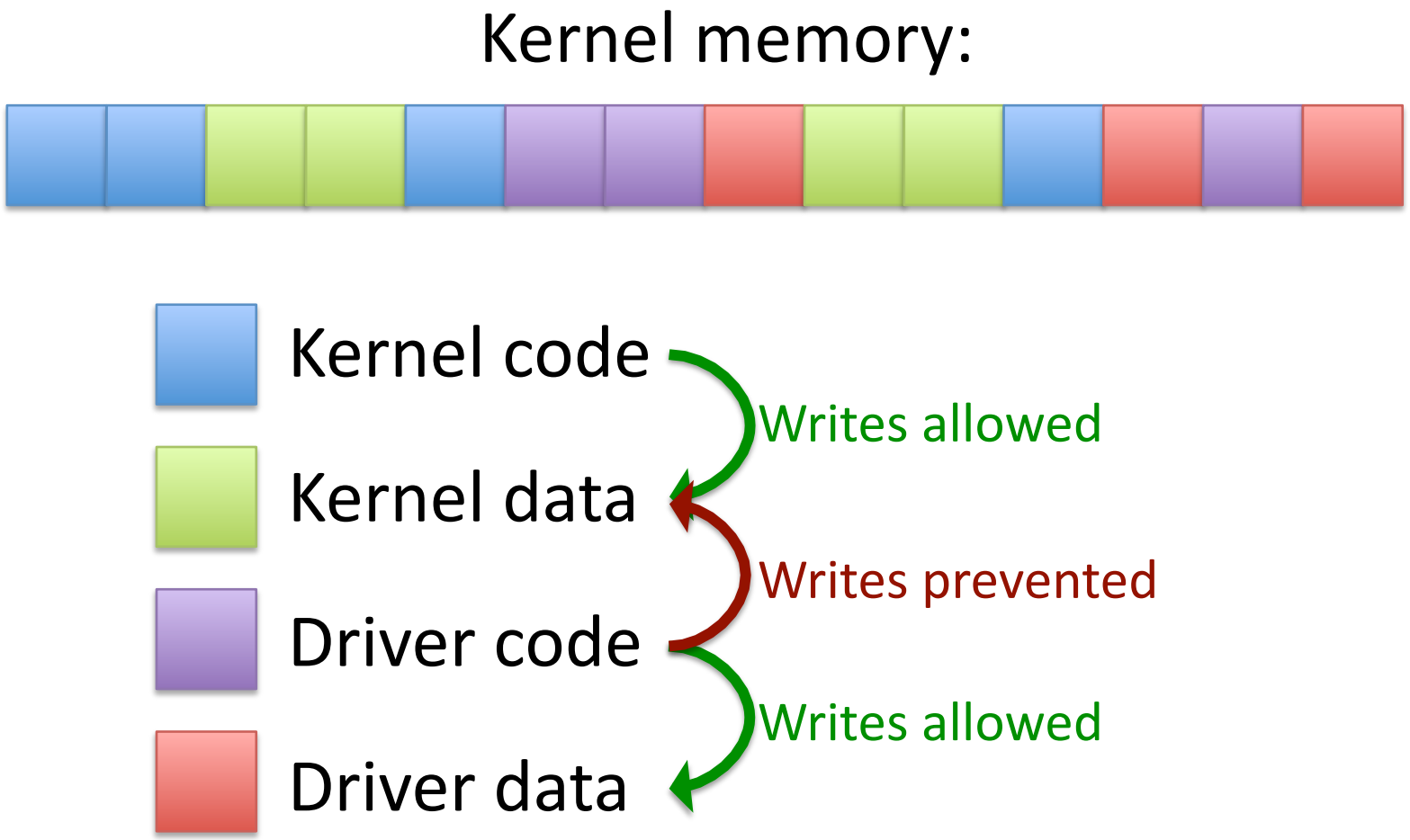
Memory protection

Kernel memory:

Process memory:



Memory protection

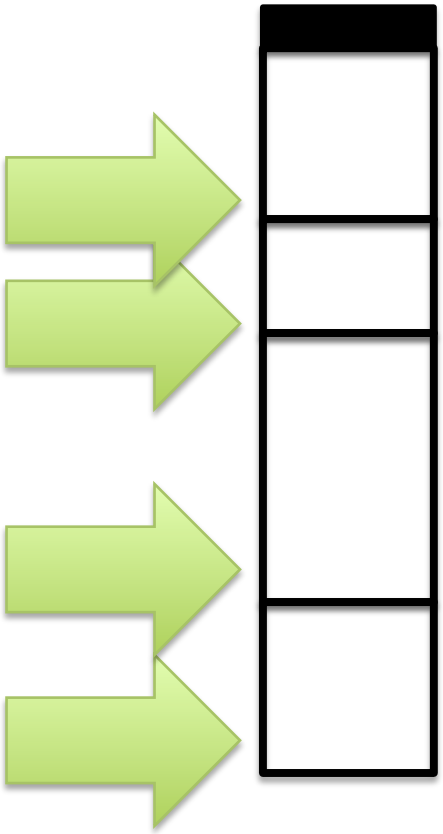


Kernel memory access control

Kernel memory:

- Hypervisor & security VM enforce access control policy on kernel memory
- Policy: security-critical kernel data can be written only by core (non-driver) kernel code

Policy enforcement

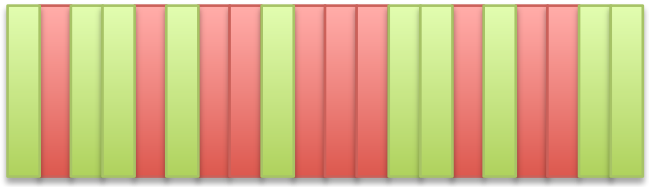


- How is provenance of write determined?
  - Stackwalk (pray for frame pointers)
  - Other techniques for corner cases

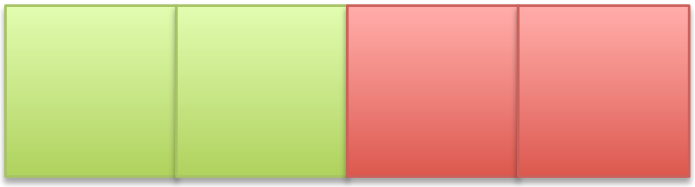
Policy enforcement

- Reducing performance cost
  - Kernel data structure layout optimizations
  - Kernel memory allocation optimizations

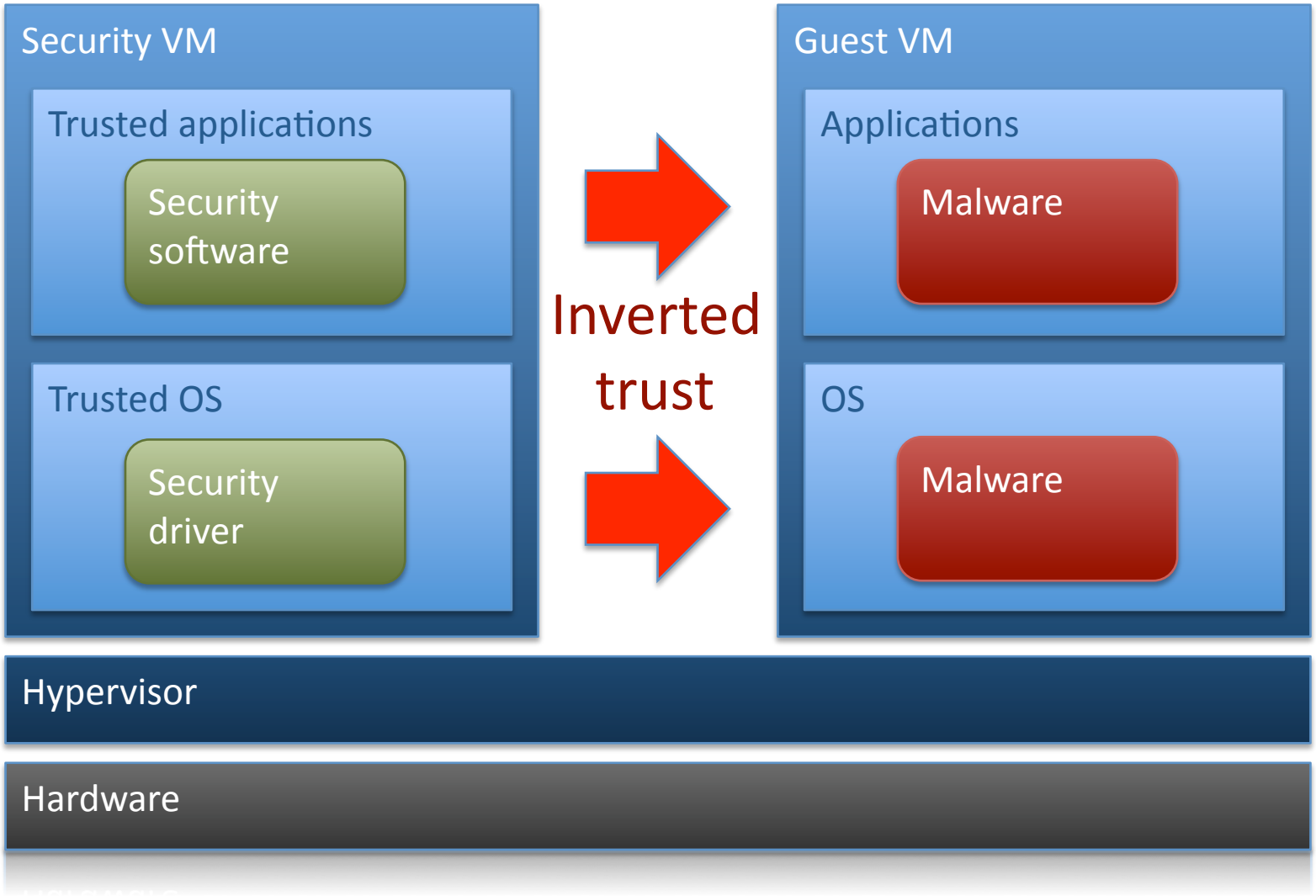
Make this:



Look like this:



Kernel memory access control



Conclusions

Trust assumptions made by VMI-based software require consideration

Hypervisors becoming kernels…
kernels becoming libraries

Kernel-style memory protection restores trust in guest memory views

Questions?

Jon Giffin
Georgia Tech

giffin@cc.gatech.edu