



Livegrid™



# Lack of System Registers

## and two simple anti-forensic attacks

Tsukasa Ooi <[li@livegrid.org](mailto:li@livegrid.org)>  
Lead Analyst, Livegrid Incorporated



## Related Topics

- Live Memory Forensics
- Anti-forensics
- Rootkits



## What is “anti-forensics”?

- The way to prevent forensics
- Not only attackers!
  - Anti-forensics is also useful for bad guys to prevent OWN MACHINE to be forensically analyzed
- But forget it.
  - I’m not talking about this...



## I will be Taking at:

- PacSec 2009

Stealthy Rootkit – How bad guy fools live memory forensics?



## Live Memory Forensics/Imaging

- Forensics based on memory of running machine
- Done by Memory Acquisition Tools
  - EnCase
  - dd
  - ...



# What Physical Memory Acquisition Tools Do?

- Acquire contents of Physical Memory
- **Acquire System Registers (optional)**

Really, “optional”?



## What rootkits can do?

- Can fake forensics software without acquiring contents of System Registers.



## Really?

- Many software does!
  - EnCase
  - (RAW) dd
  - Memoryze
  - WinEN
  - FastDump
  - ...

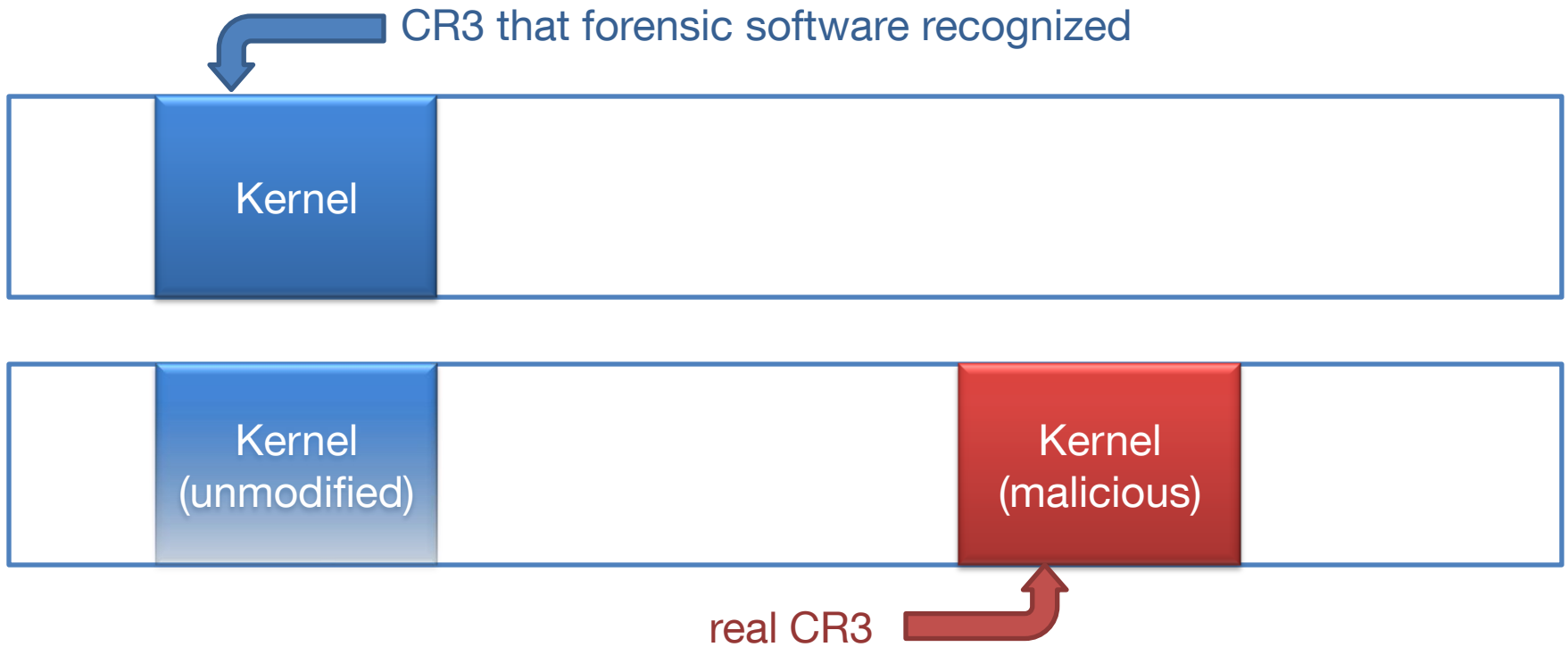


## Way to attack – part one (1)

- Modify CR3 Registers (Pointer to Paging Structure)



## Way to attack – part one (2)





## Way to attack – part one (3)

- If System Registers are missing, forensic software finds signatures of system.
- But these mechanism are very easy to fool.

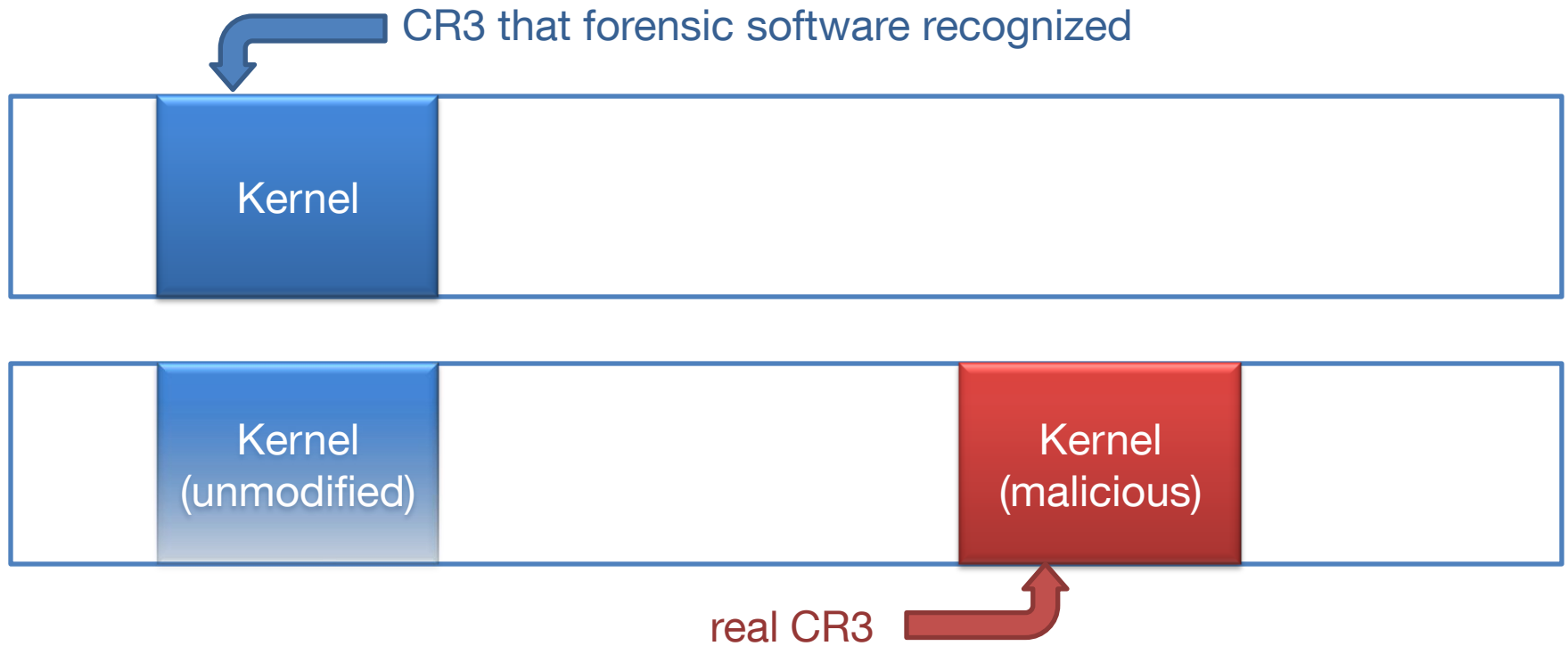


## Way to attack – part one (4)

- Keep system (physical) memory range unmodified
- Create backup region
- Copy part of kernel and patch backup
- Change CR3 to rootkit's one



# Way to attack – part one (5)



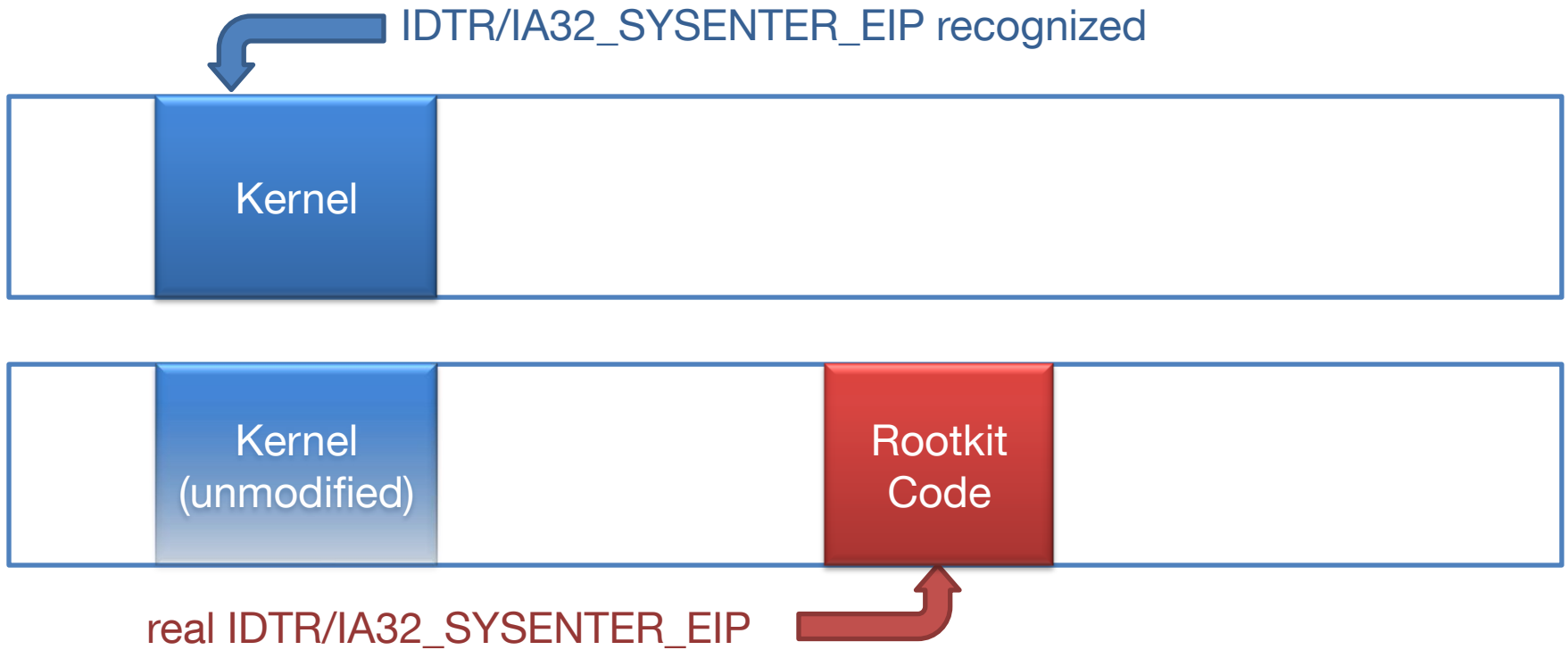


## Way to attack – part one (6)

- But this attack is a bit difficult because rootkit must manage its own page table.
- There is one more way that is very easy!



# Way to attack – part two (1)





## Way to attack – part two (2)

- IDTR is a system register managing interrupts and exceptions
  - Including page faults
- IA32\_SYSENTER\_EIP MSR / LSTAR\_MSR is a pointer to system call entry
  - Can hook/modify system calls



## Way to attack – part two (3)

- Way to implement:  
<Begin> Change these registers <End>  
Very easy right?
- These are widely used by current rootkits  
but also useful for anti-forensics
  - If attacker hide rootkit somewhere in the memory,  
there are no general ways to detect these attacks!



## Way to prevent these attacks (1)

- Acquire these system registers
  - CR3
  - IDTR
  - IA32\_SYSENTER\_EIP MSR
  - LSTAR\_MSR
- (If rootkit use CR3/IDTR)  
Check physical and logical memory layout



## Way to prevent these attacks (2)

- Interrupt Descriptor Table layout and Page Table layout are easy to detect
- So...
  - Find these tables
  - Check if these tables are “malicious”



## Conclusion

- Acquire system registers as possible
- New approach for forensics is needed



Livegrid™



Have any questions?

**THANK YOU**

Tsukasa Ooi <li@livegrid.org>  
Livegrid Incorporated, Lead Analyst



## Technical Articles and Sources

- ... will be available December, 2009
- at <http://a4lg.com/>