Hostile environment detection with Timing measures

Gaël Delalleau
gael.delalleau+csx@m4x.org

CancSecWest 2005
Vancouver – May 4-6
Detecting kernel rootkits from userland and uid>0

The idea: measuring the execution time of syscalls

- Unprivileged CPU instructions used to get ticks count
  - rdtsc on Intel
  - %tick on Sparc...
- A change in the execution time means the syscall has been changed => ALERT

The problem: IRQs, cache effects... => execution time is always different!

The solution: doing many measures then some statistical analysis
Timing can also be used for...

- Detecting userland rootkits and backdoors
  - Static ELF injection
  - Dynamic ELF injection (library call hijacking)
- Detecting Virtual Machines (honeypots? ;)
  - Tested on VMware, UML, QEmu...
- Detecting a debugging environment
  - Tested on strace, truss...
Time for Demo

- And don't forget to get up early tomorrow

- I speak at 9:00am

- Wake me at room 1630 if I don't show up :)