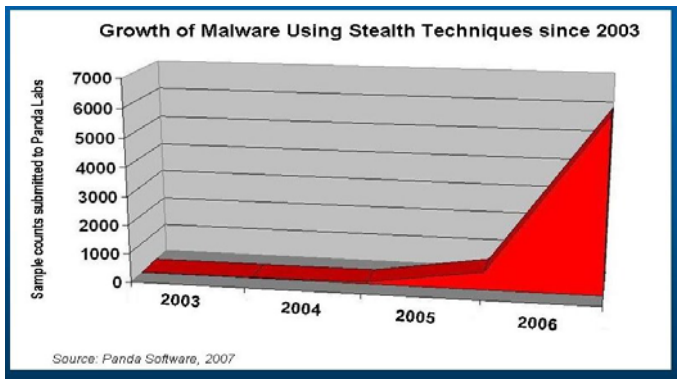
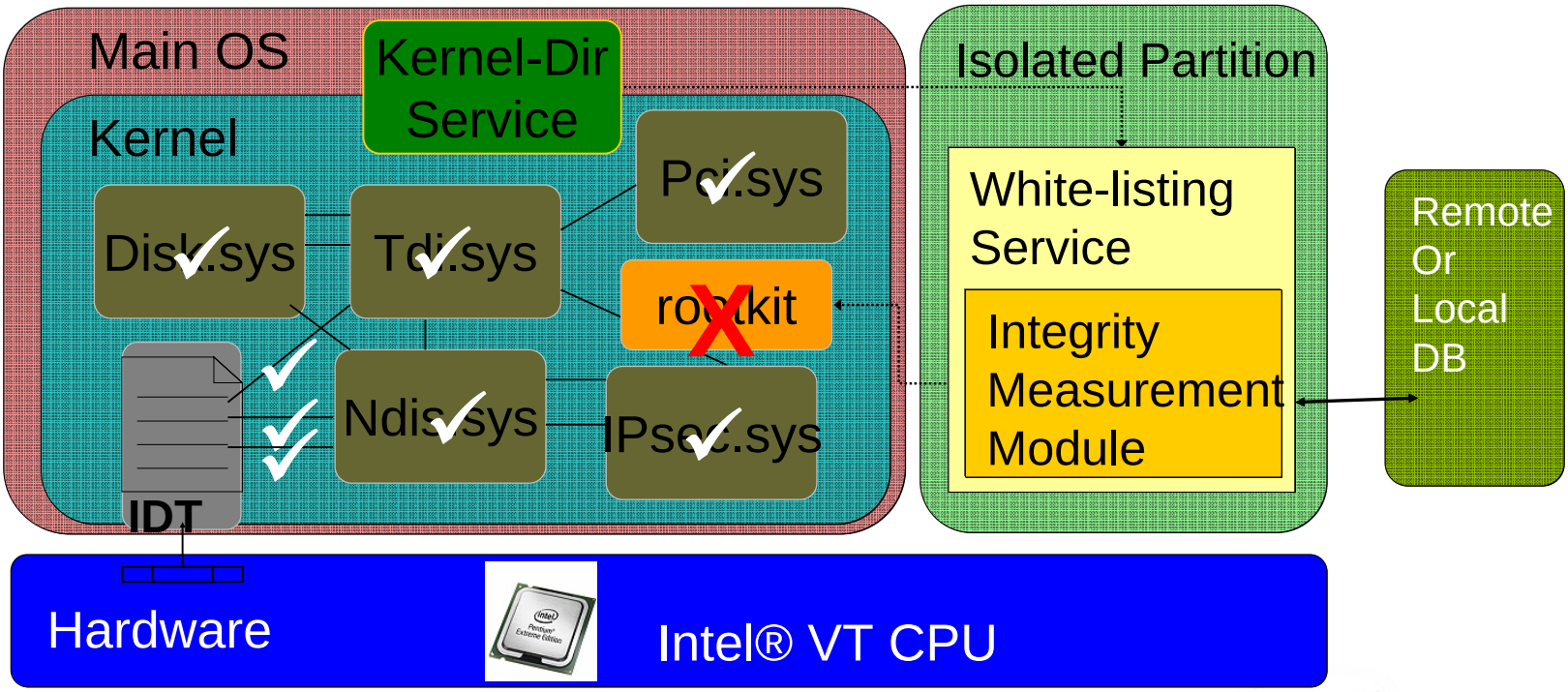
Runtime Kernel Rootkit Detection Technology

Use of rootkits and stealth attacks increased exponentially in 2006.

- Rootkits help malicious software hide
- Many rootkits currently go undetected
- Rootkits propagate through user action and unpatched vulnerabilities
- Rootkits enable botnets





- Runtime memory verification of known kernel software from an isolated secure platform partition
- Monitoring of CPU registers and correlation of system tables (such as IDT, SSDT)
- Offline Tool to generate software manifests available via database

Research at Intel

www.intel.com/research