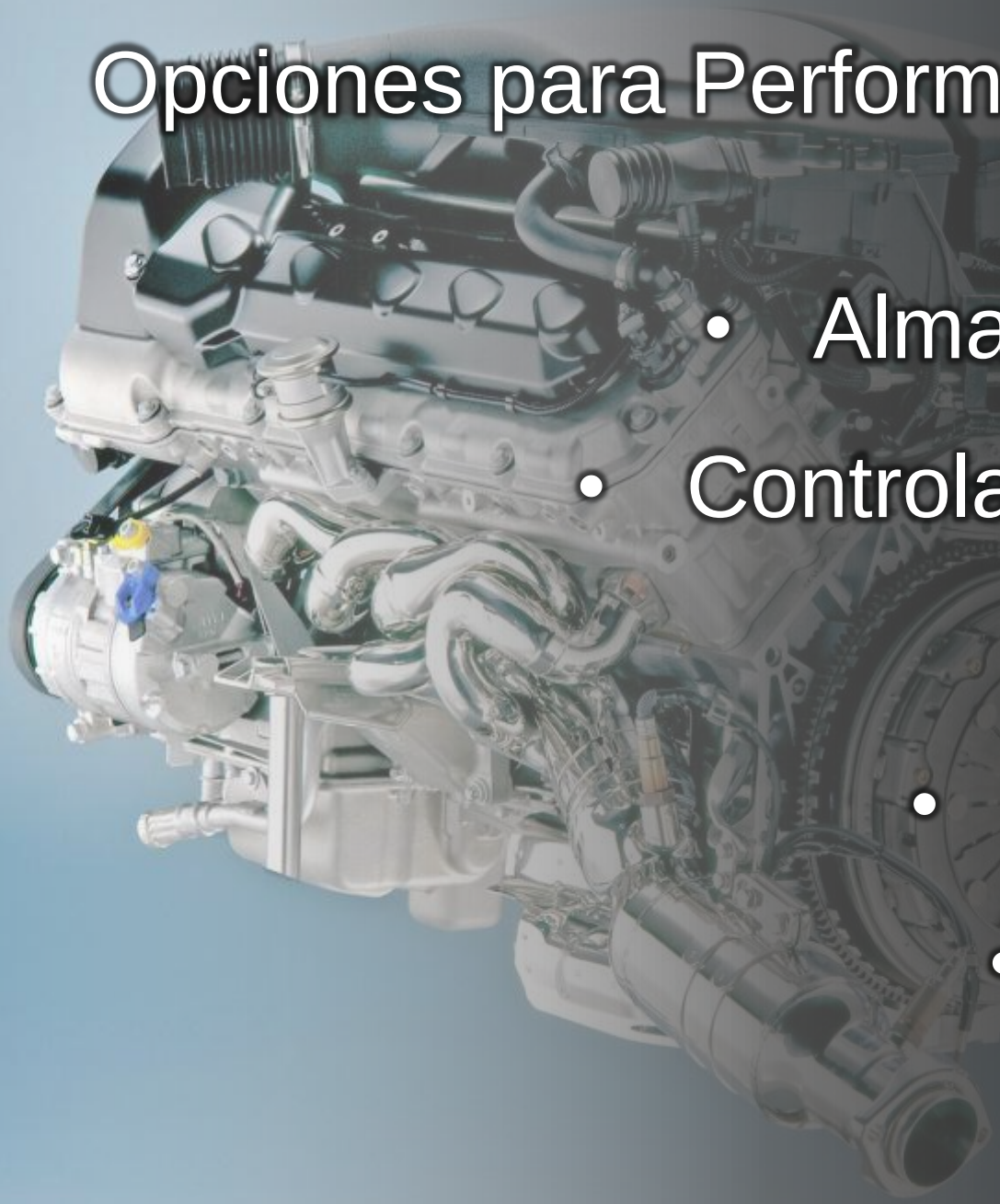
Maximizar el performance de las soluciones de una manera segura

Rafael Díaz-Barriga

ESS Agosto 2012

Opciones para Performance Tuning :



- Almacenamiento
- Controladora de red
- Servidor
- Procesador
- Software

Almacenamiento de estado sólido: SSD

Intel 10Gb Ethernet

“Offloads” para cargas de trabajo virtualizadas

Servidor: Opciones del BIOS

Procesador

Microarquitectura

GHz

Multi-core

Cache size

Optimización del software

Herramientas para hacer un mejor uso del hardware

… y la seguridad?

1
Vulnerabilidad

100M
Identidades perdidas

1
Ataque planeado

34
Compañias comprometidas

1
Worm

7M
PC’s Zombies

Situación 1: Protección de los datos

Encripción (cifrado)

- Aún cuando los datos puedan ser perdidos o
robados, no podrán ser usados
- Protege la confidencialidad en usos donde el aislamiento físico es imposible
- Estándares de la industria y leyes específicas

INTEL AES-NI

USOS

Transmisión

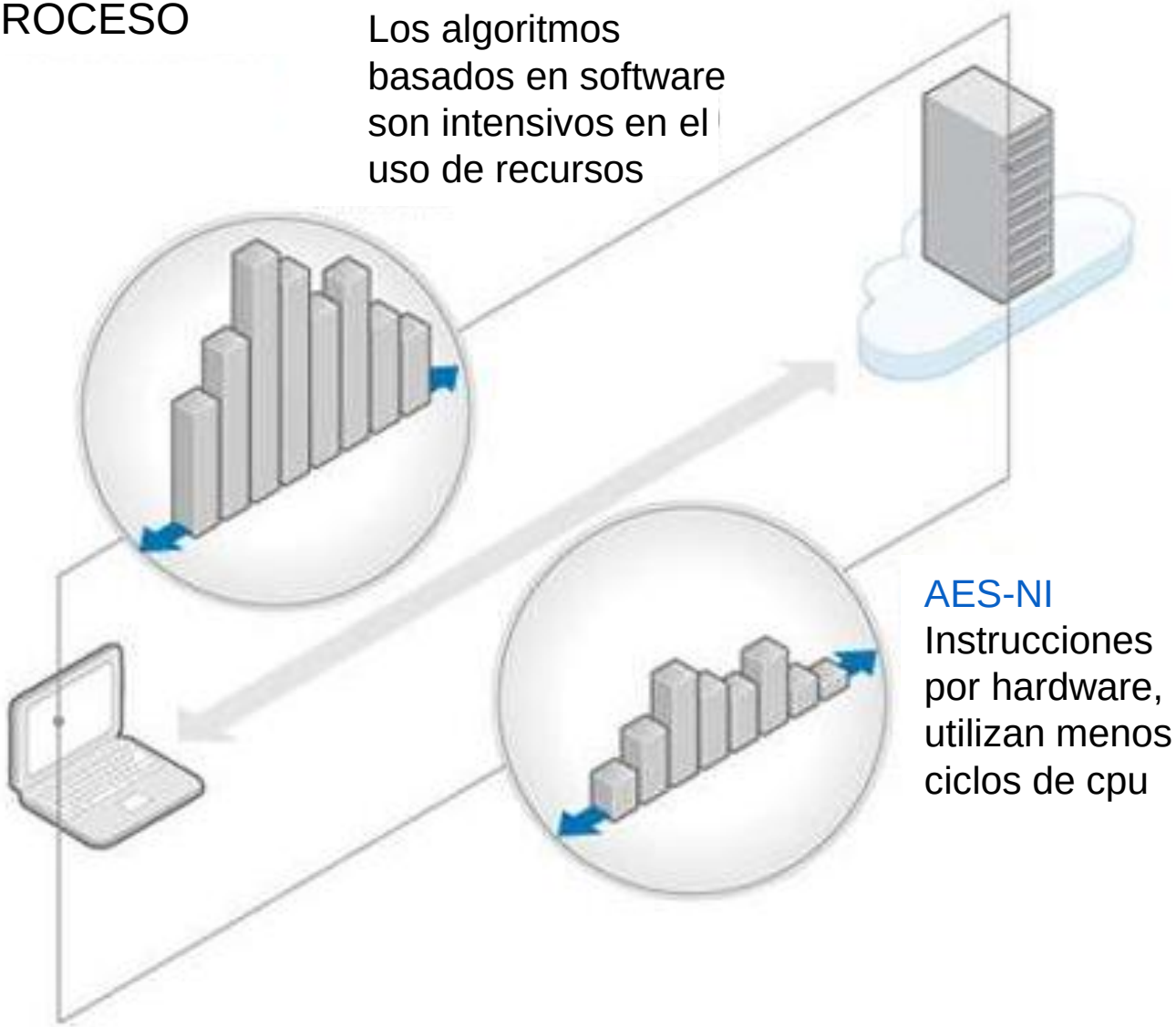
Almacenamiento

Aplicaciones

PROCESO

AES

Los algoritmos basados en software son intensivos en el uso de recursos



AES-NI

Instrucciones por hardware, utilizan menos ciclos de cpu

Situación 2: Protección de la plataforma

Objetivos del Malware

- Corromper sistemas
- Interrumpir el negocio
- Robar datos
- Tomar control

Puntos que los atacantes buscan

- Aquellos con menores defensas
- Dificiles de detectar y de recuperar

Componentes amenazados

- BIOS, Firmware
- Hypervisor

Intel Trusted eXecution Technology (TXT)

Tecnología de ejecución confiable

Método reactivo

Las tecnologías actuales usan una lista “negra”

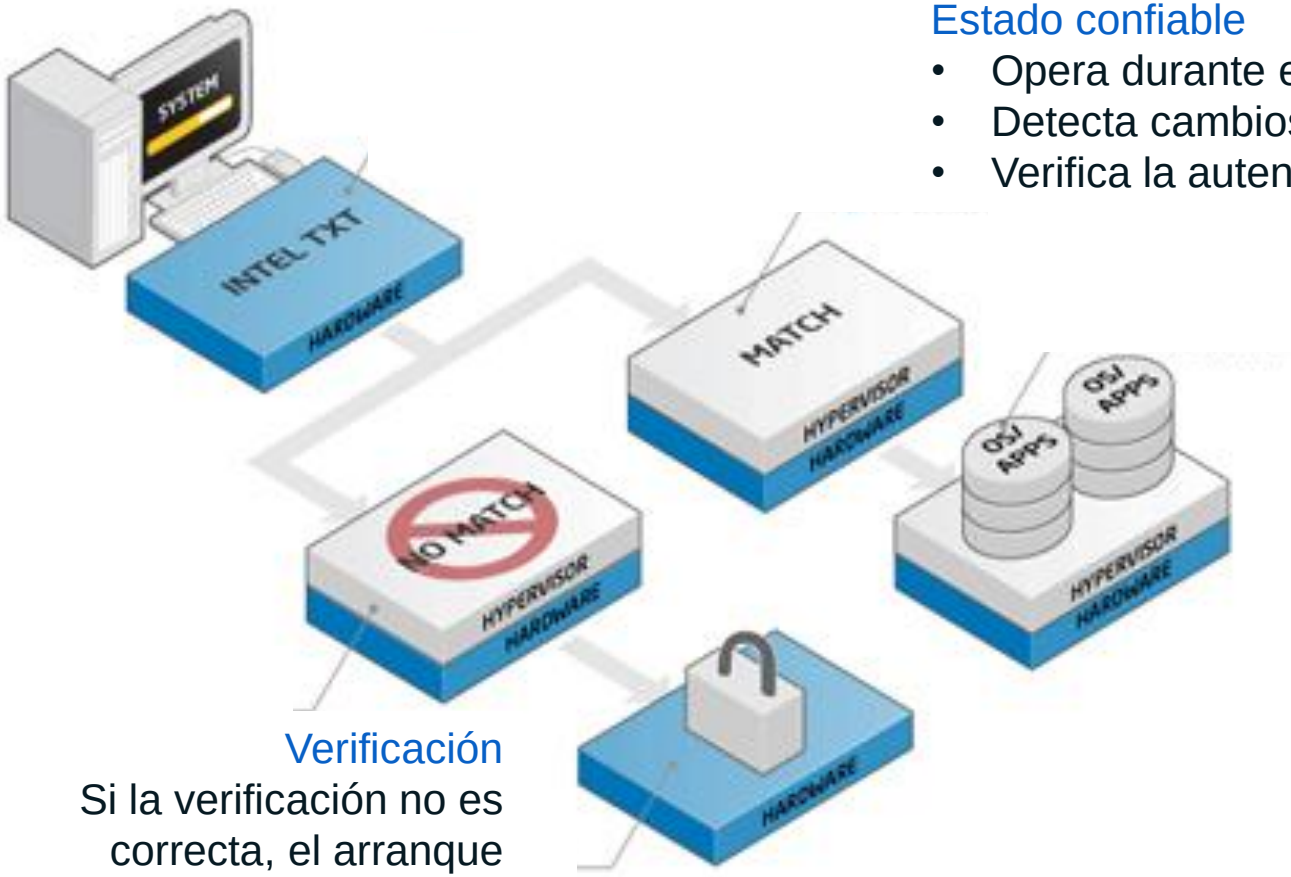
- La lista “negra” crece cada vez con el tiempo
- La identificación ocurre en respuesta al ataque

Método proactivo

Lista “confiable” para código de identidad conocida

- TxT – Tecnología basada en hardware
- Verifica software dañino antes de que arranque

Uso 1- Verificación del arranque a un estado confiable



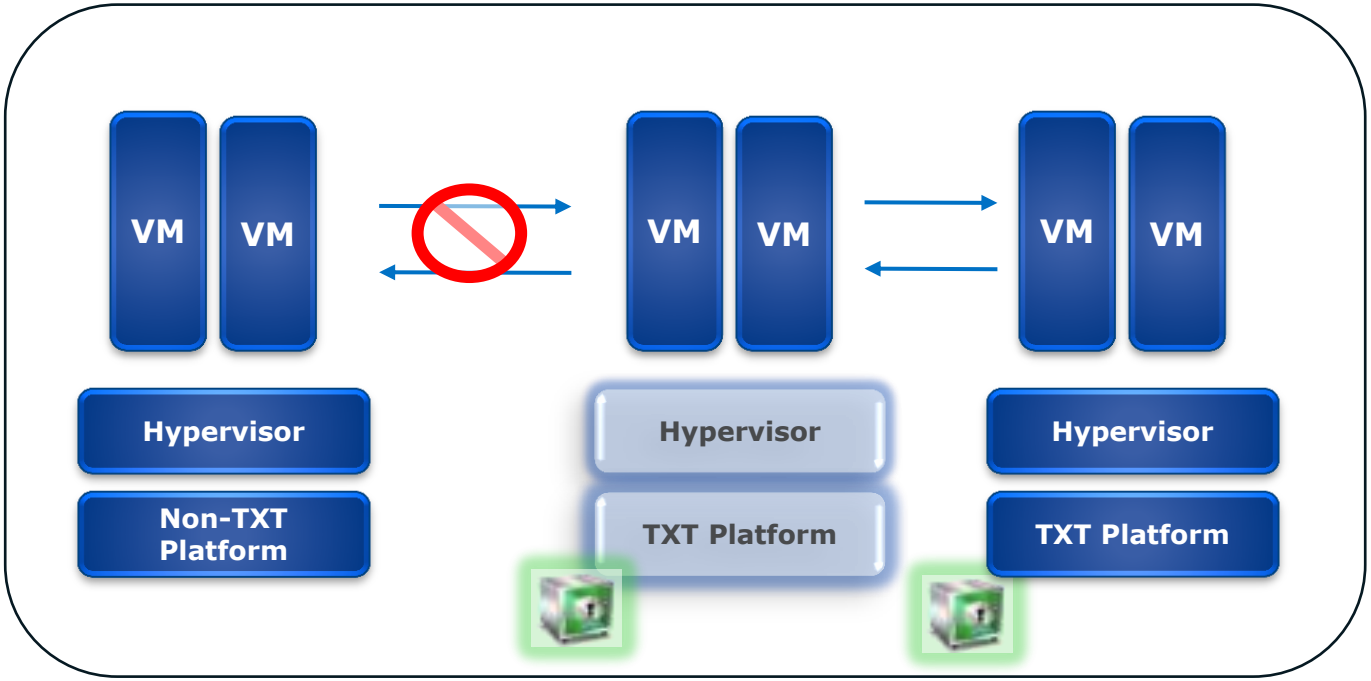
Estado confiable

- Opera durante el arranque
- Detecta cambios en el BIOS/FW
- Verifica la autenticidad del SO

Verificación

Si la verificación no es correcta, el arranque puede bloquearse

Uso 2 - Grupos de recursos confiables (Trusted Pools)



- **Grupos de recursos virtuales confiables**
- **Migración dinámica de VM basada en politicas**
- **Solo “hosts” confiables**
- **Previene ciertas applicaciones de migrar a recursos no verificados**

Comentarios finales

Diferentes factores afectan el desempeño

Herramientas de desarrollo

Almacenamiento de estado sólido

Adaptadores de red de 10Gb

Tecnologías de seguridad basadas en hardware

AES-NI, TxT

Gracias

rafael.diaz.barriga@intel.com