Sistema Colaborativo de Detección y Reacción ante Intrusiones basado en Intel vPro

Ana Nieto, Gerardo Fernández

Nics Lab - Universidad de Málaga

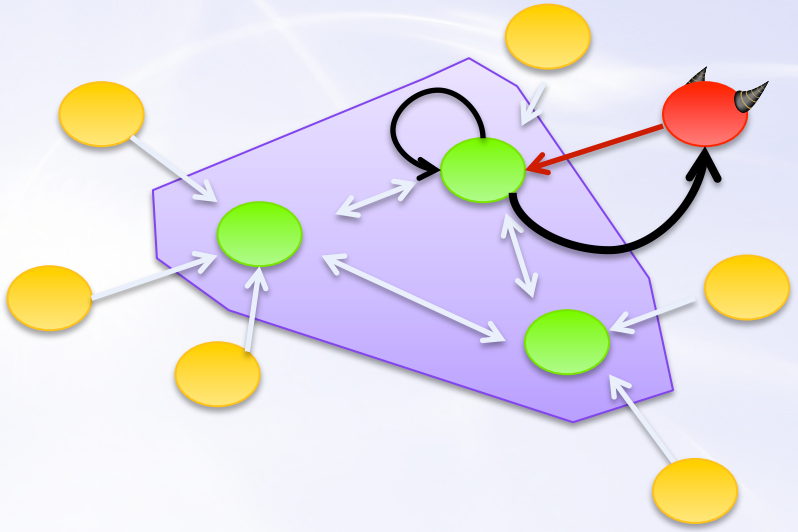
www.nics.uma.es

NICS

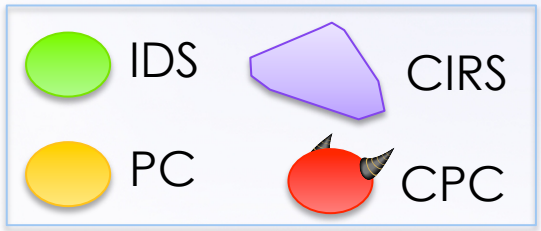
Sistemas Colaborativos de Detección y Reacción frente a Intrusiones (CIRS)

- Permiten la definición de políticas de actuación frente amenazas detectadas

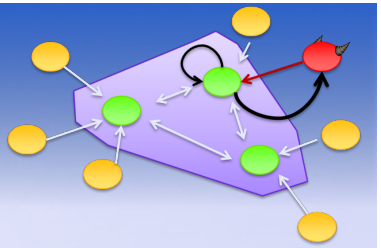
- Enfoques habituales:
  - Listas blancas/negras
  - Seguimiento del ataque
  - Obtención de evidencias
  - Aislamiento del tráfico de ataque



- *Sistemas de Alerta Temprana*
  - Agentes distribuidos por la red
  - Informan de la incidencia lo antes posible



Problemas abiertos



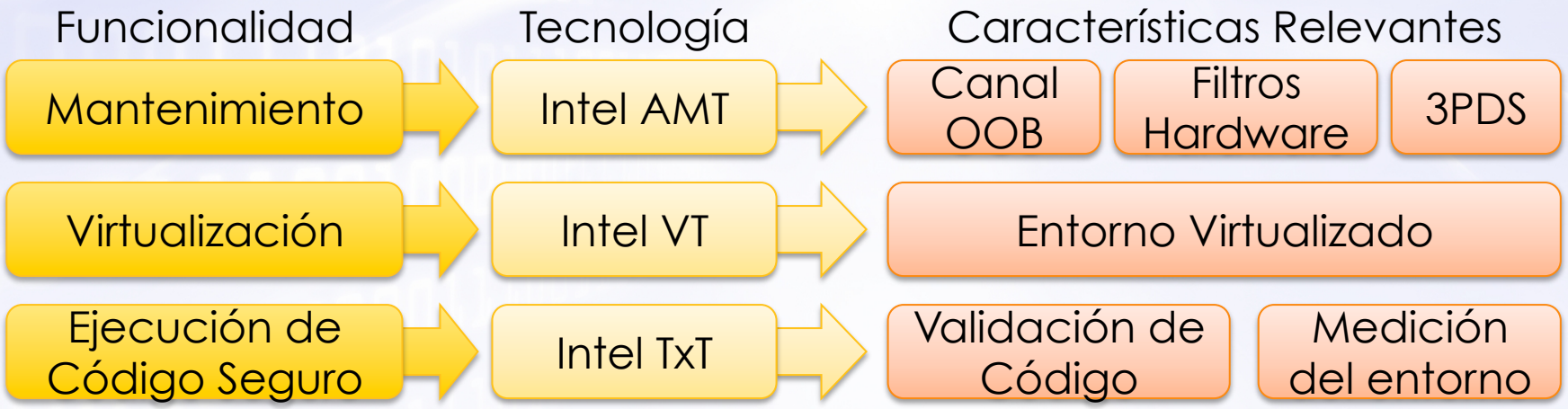
- ¿Podemos **confiar** en todos los agentes?
  - Complejos esquemas de confianza que afectan al rendimiento

- ¿Es **segura la comunicación** entre los agentes?
  - El intercambio de información es un punto crítico en el que el atacante podría
    - adquirir información sensible,
    - alterar dichos datos o
    - incomunicar el canal de comunicaciones entre dos o más agentes.

Sistema Colaborativo de Detección y Reacción ante Intrusiones basado en **Intel vPro**

Intel vPro

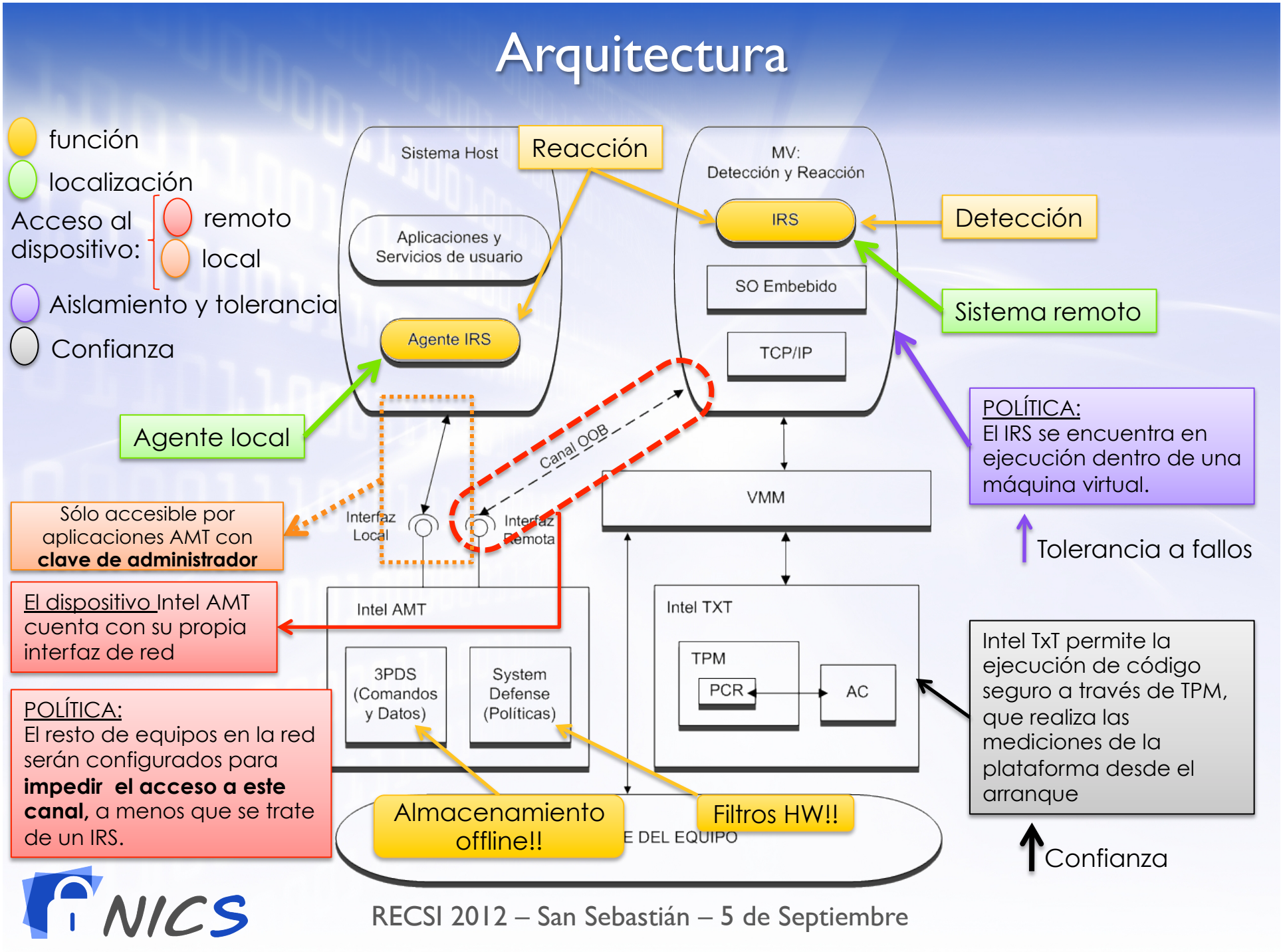
- Agrupa un conjunto de tecnologías relacionadas con el **mantenimiento** remoto (Intel AMT), la **virtualización** (Intel VT) y la **ejecución de código seguro** (Intel TxT).
- Combina elementos HW y SW para incrementar la seguridad de la plataforma y su rendimiento



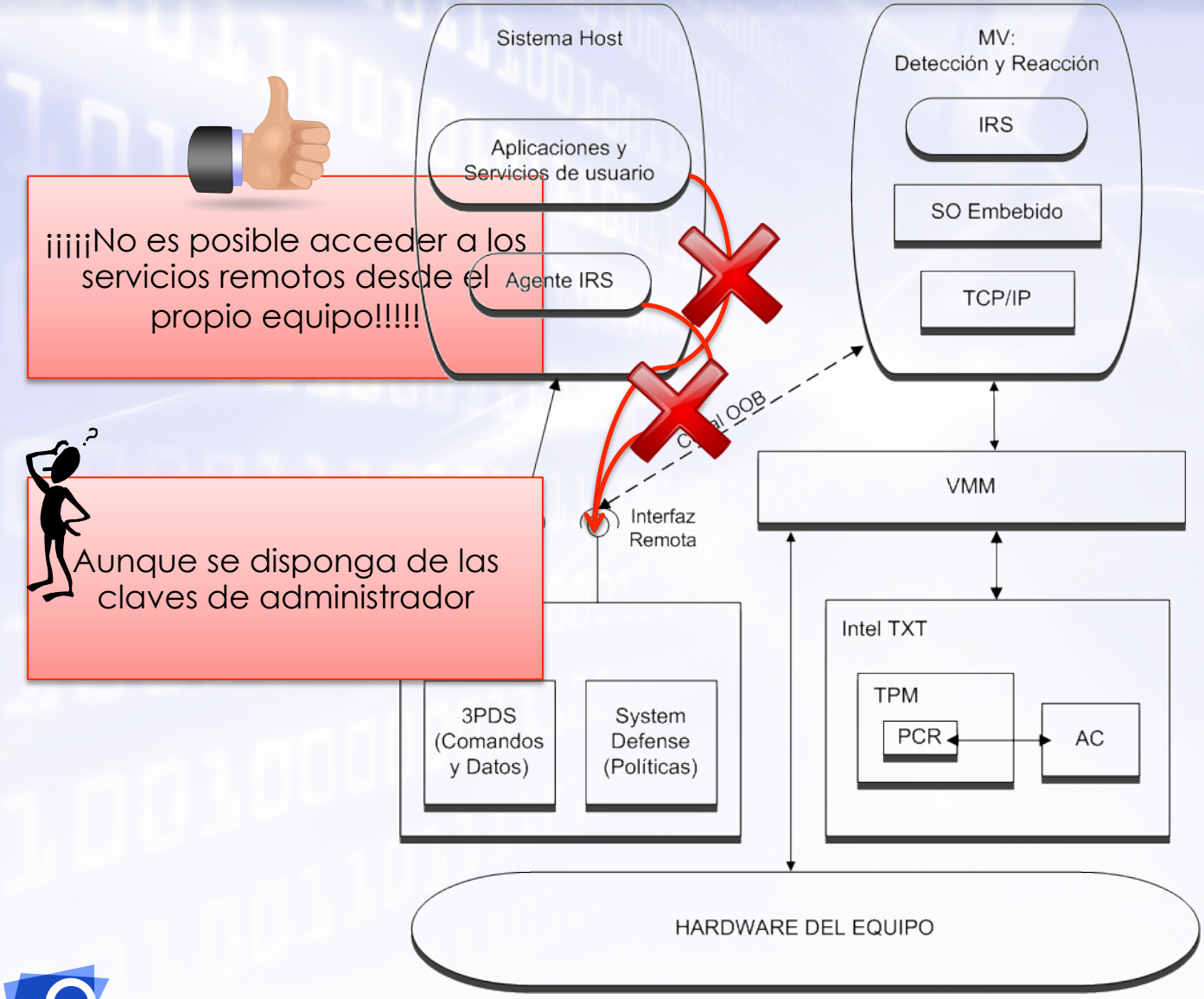
Sistema Colaborativo de Detección y Reacción ante Intrusiones basado en Intel vPro

- Añade **componentes HW** embebidos en los equipos IRS para aumentar la **confianza** del entorno
  - Ejecución de código confiable usando TPM
- Emplea **canales de comunicación fuera de banda** (OOB) para la comunicación entre los componentes del sistema de detección y reacción y reglas de filtrado HW
- Define el **formato de los mensajes** y la **secuencia de control** necesarias para el envío de código móvil interpretado por el agente nativo
- Componentes:
  - Mecanismo de detección
  - Mecanismo de reacción
  - Agente local
- Contexto:
  - Red en la que todos los equipos cuentan con tecnología Intel vPro
- Arquitectura y funcionamiento…

Arquitectura

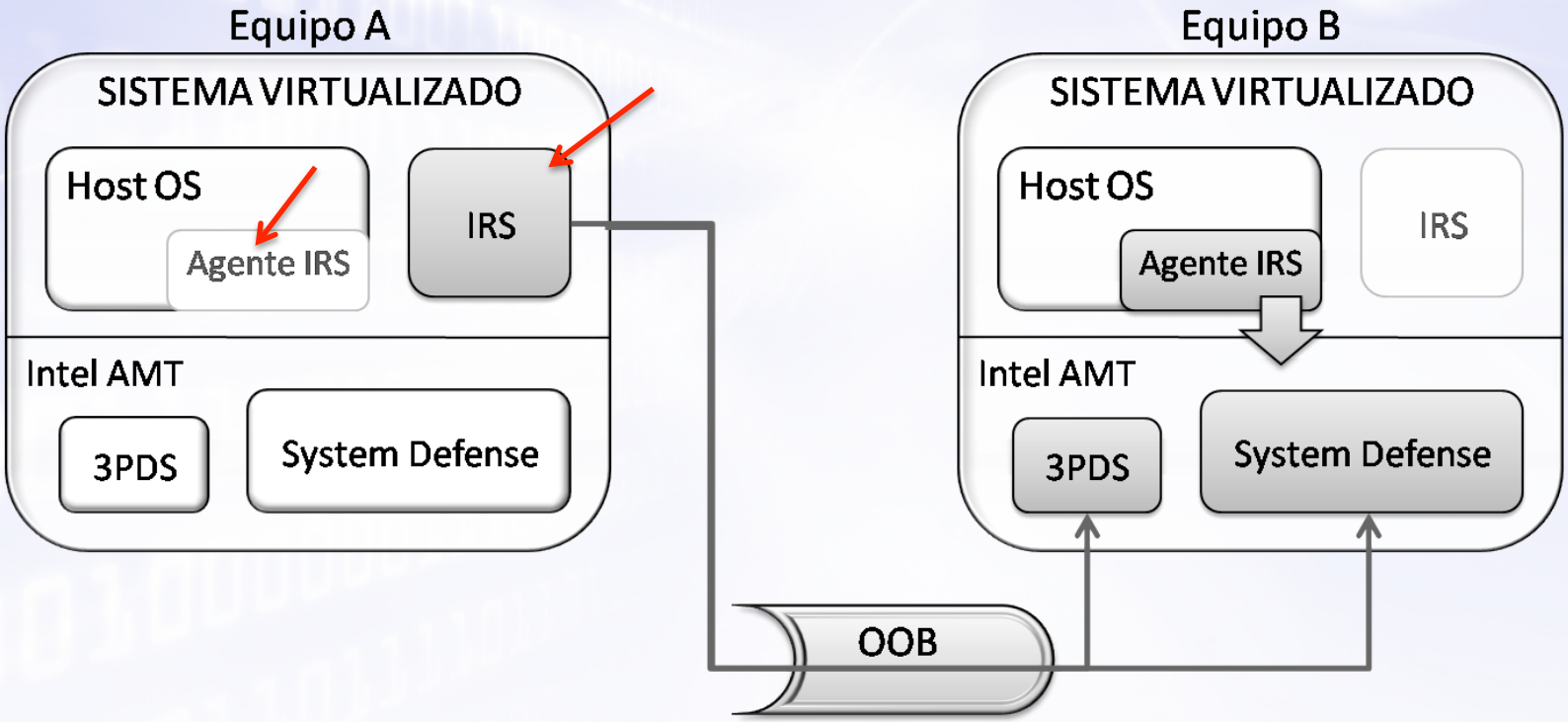


Arquitectura



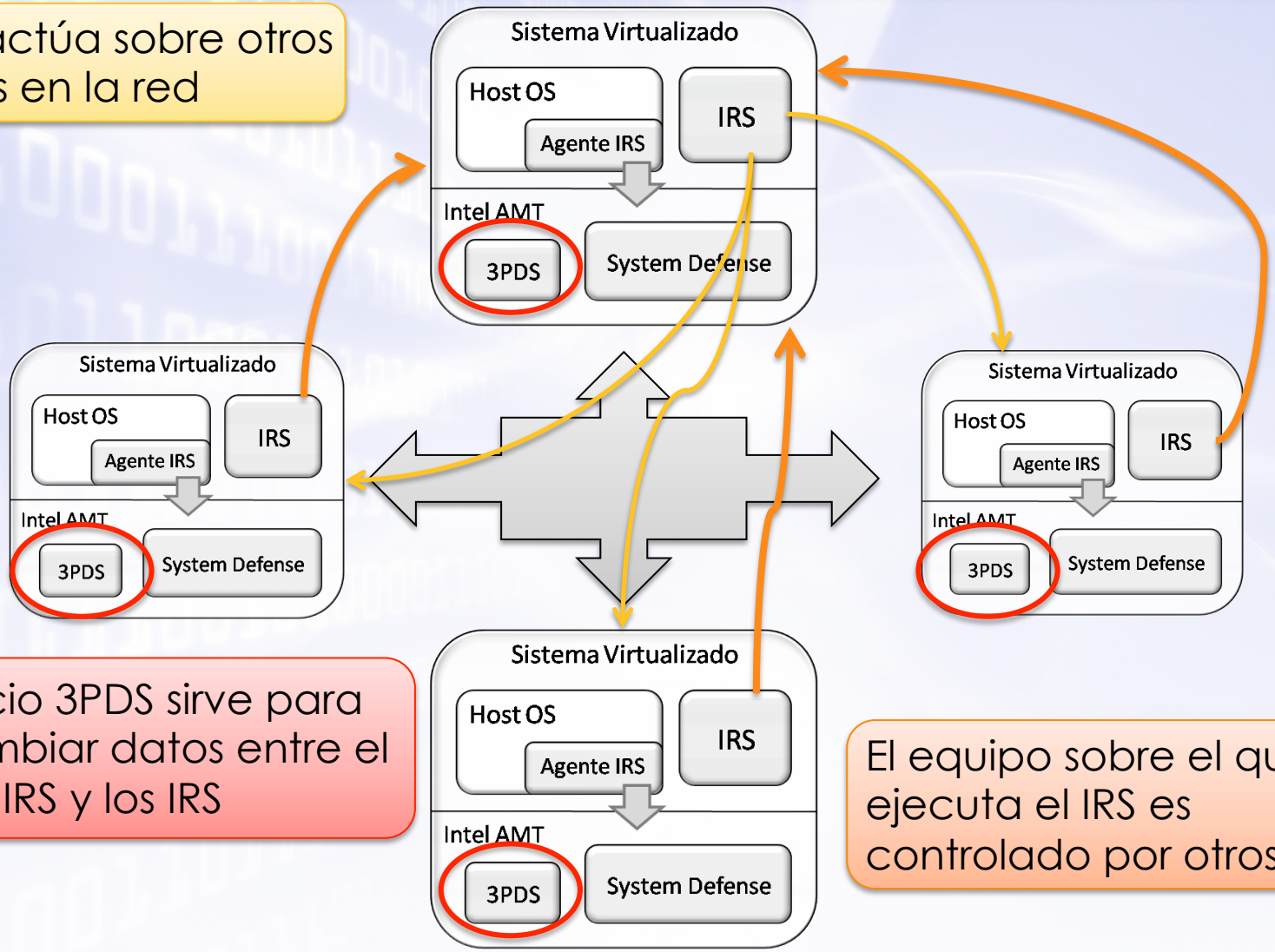
Arquitectura

- Un equipo de la red puede tener ambos componentes integrados, funcionando como IRS y a la vez contando con un agente



Funcionamiento

Un IRS actúa sobre otros equipos en la red

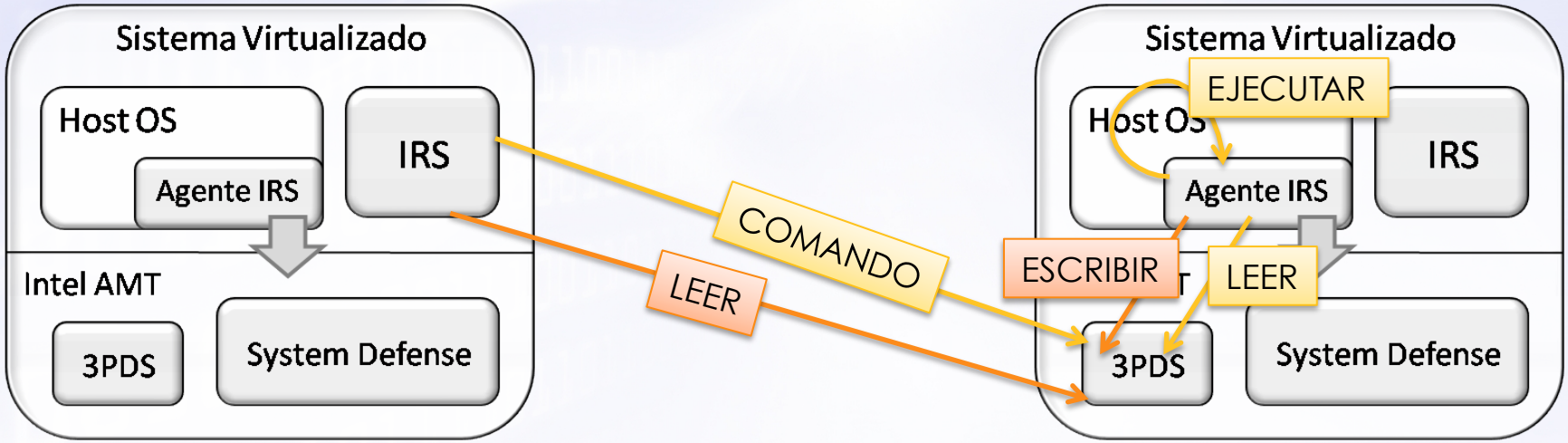


El espacio 3PDS sirve para intercambiar datos entre el Agente IRS y los IRS

El equipo sobre el que se ejecuta el IRS es controlado por otros IRS

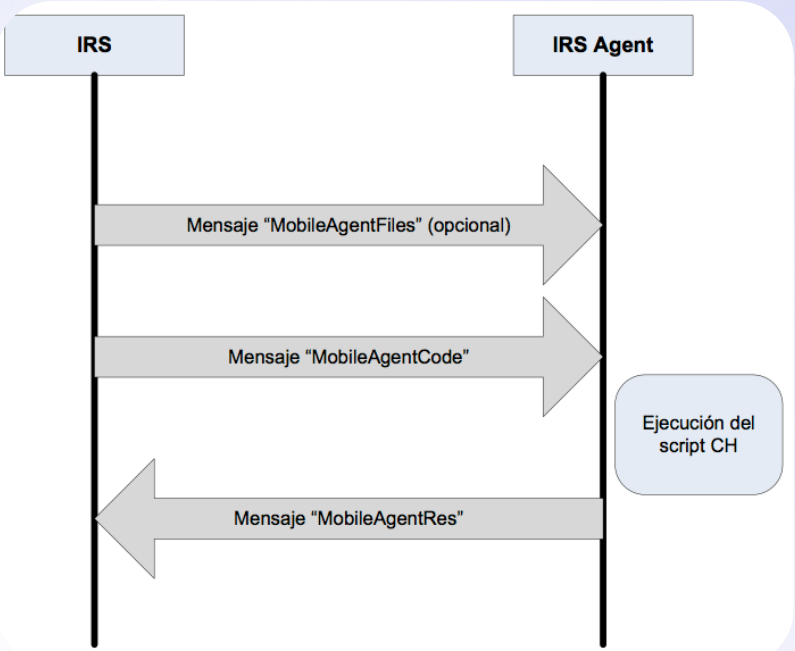
Funcionamiento

- Acciones sobre el equipo comprometido:
  - Aquellas propias de AMT: configurar filtros HW (ej. aislar el equipo),
  - Escribir/Leer del espacio 3PDS conforme a la estructura definida
  - Ejecutar código móvil (e.j. listar procesos) -- Intérprete CH



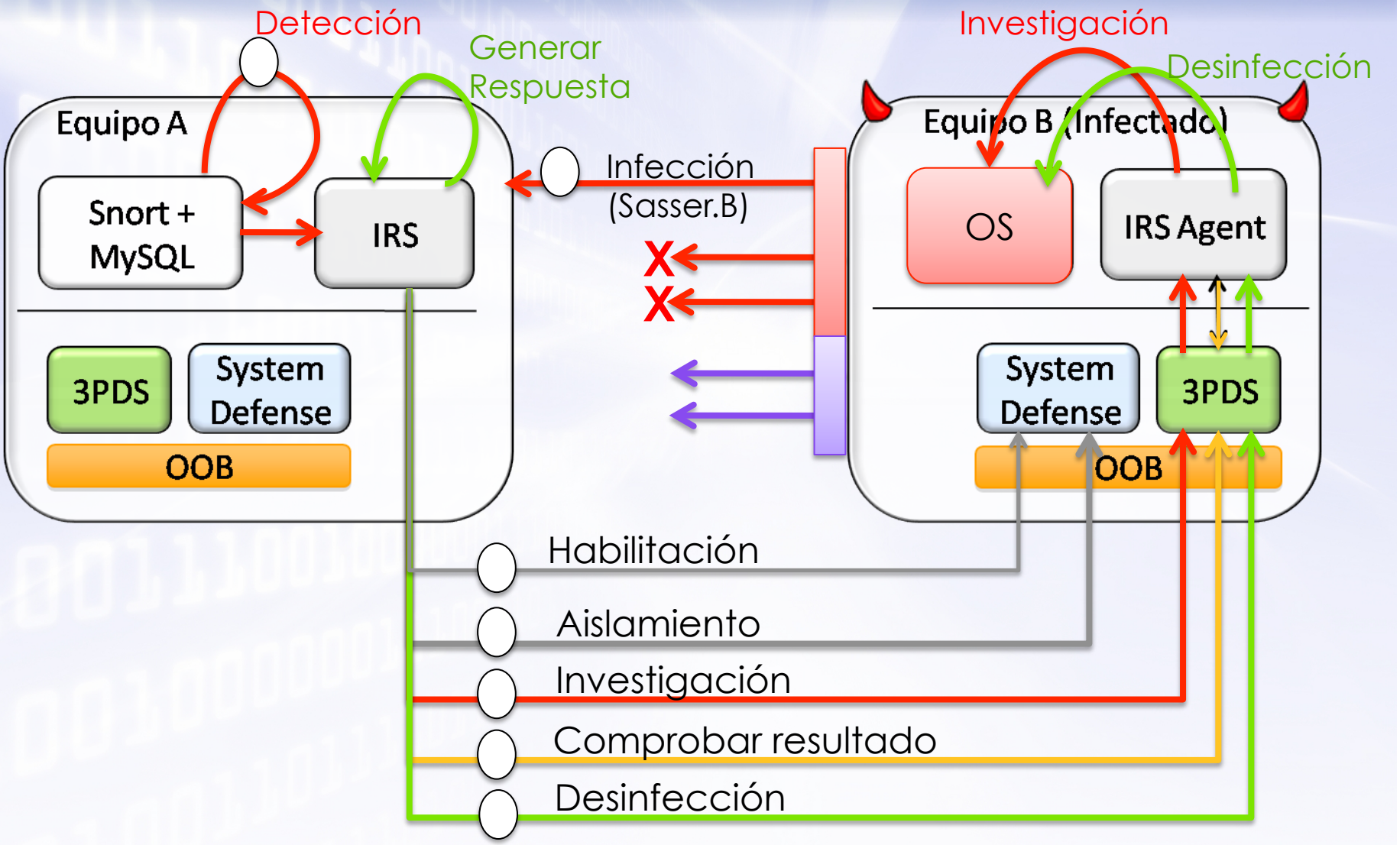
Prototipo

- Versiones 2.6, 3.0 y 6.0 de Intel AMT
- Intel AMT SDK para el desarrollo de código que use los servicios de Intel AMT
- Usamos el **Intérprete CH** de **Mobile C**
- Definición de funciones:
  - obtener lista de procesos,
  - finalizar proceso,
  - obtener valores del registro,
  - ejecutar un proceso,
  - obtener ficheros.
- Definición del
  - **Formato** de los mensajes y
  - La **secuencia de control**



- Snort para la detección de ataques
- El entorno se compone de dos equipos en una red cableada tal que:
  - Hay un equipo infectado que intenta propagar un virus (sasser)
  - El otro equipo detecta esta amenaza y reacciona para frenar el contagio

Prototipo (Demo)



Prototipo (Demo)

- Vídeo

Conclusiones y Trabajo Futuro

- Sistema colaborativo para la detección y reacción ante intrusiones, empleando como ase las tecnologías presentes en Intel vPro
  - Intercambio de datos aun cuando el equipo destino se encuentra inoperativo, suspendido o en otro estado donde el sistema operativo está inhabilitado.
- Comunicación OOB entre los IRS
- Agente IRS en los equipos para evaluar localmente los daños
- Permite la virtualización del IRS
- Problemas:
  - Virtualización & Intel AMT
  - Carencia de emuladores que permitan validar virtualmente la solución
- Cuestiones abiertas:
  - Evaluación del riesgo de colisión en el acceso al espacio 3PDS y el tiempo de retardo por escritura en éste.