Trabajo Fin de Grado
Grado en Ingeniería en Tecnología de Telecomunicación

Antikörper

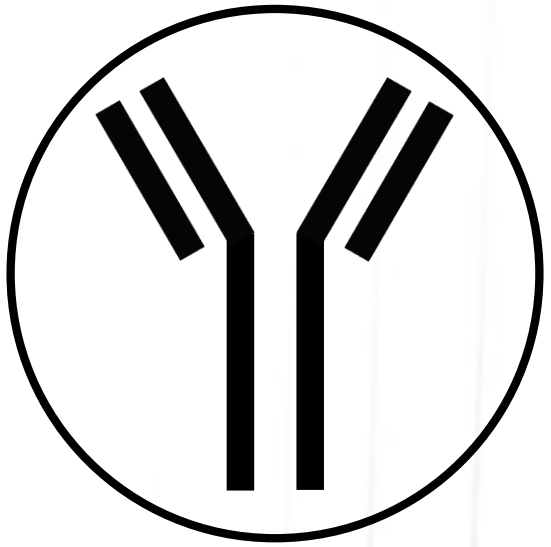
Diseño e Implementación de un Sistema de Detección de Intrusos Inalámbrico basado en Network IDS

AUTOR: Josu Barrientos Bahamonde
DIRECTOR: Luis Zabala Alberdi

BILBAO, 3 DE MARZO DE 2015

Índice

- Introducción
- Objetivos del proyecto
- Diseño de Antikörper
- Resultados de pruebas de rendimiento
- Conclusión y trabajo futuro



Introducción

La seguridad informática se está convirtiendo en un tema de interés mundial.

Con el fin de reducir los ataques en la redes, se hace necesario el uso e implementación de distintas herramientas de seguridad.

Este proyecto contribuye en el diseño y la implementación de un Sistema de Detección de Intrusiones Inalámbrico/Wireless Intrusion Detection System (WIDS).

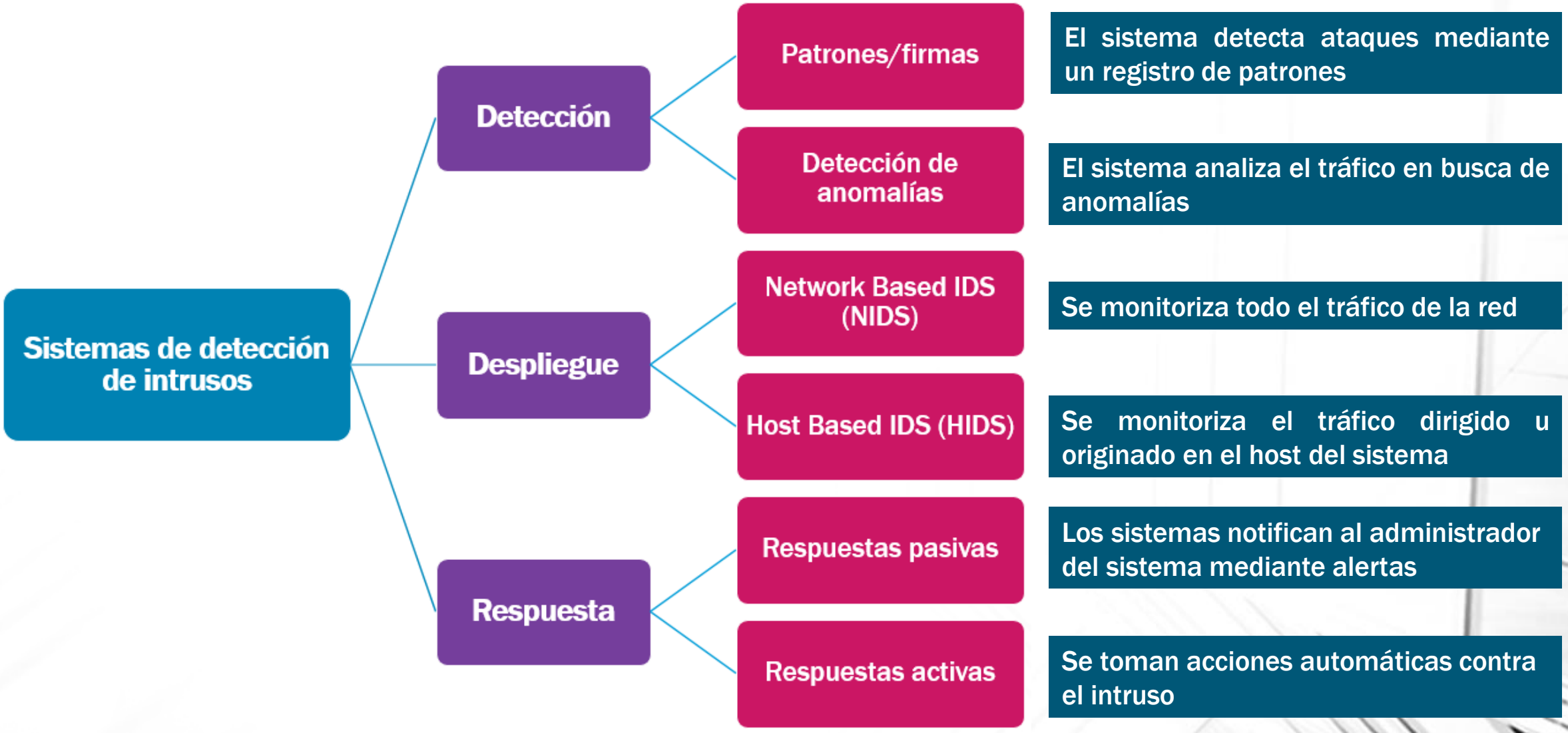
Introducción | Sistemas de detección de intrusos (IDS)

Conjunto de herramientas software y hardware encargadas de monitorizar los eventos que ocurren en un sistema informático en busca de intentos de intrusión.

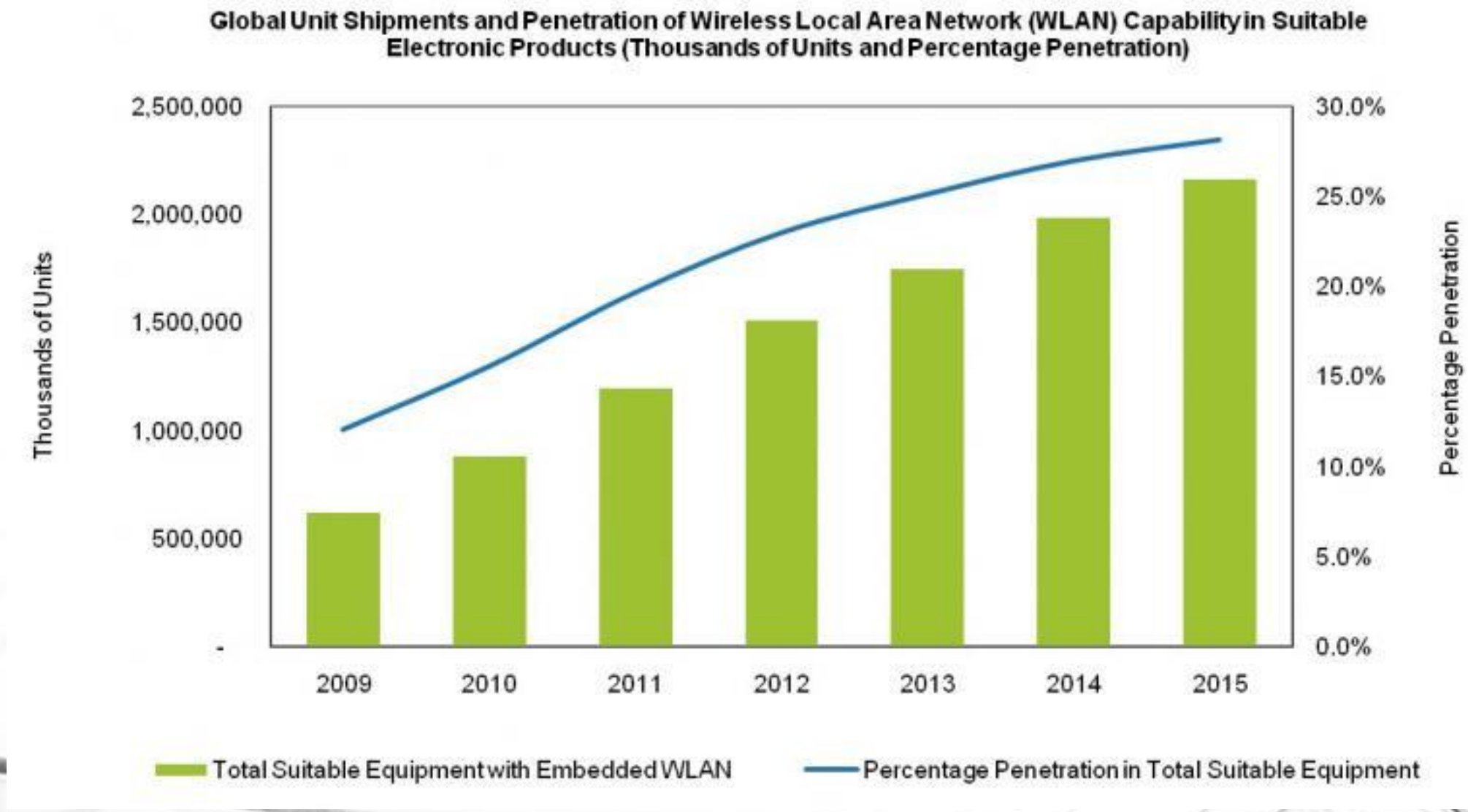
Razones por las que usar un IDS:

- Prevenir problemas al disuadir al atacante.
- Detectar ataques y otras violaciones de seguridad que no son prevenidas por otras medidas de seguridad.
- Detección de preámbulos de ataque.

Introducción | Sistemas de detección de intrusos (IDS) (I)



Introducción | Wireless Local Area Network (WLAN)



Objetivos del proyecto

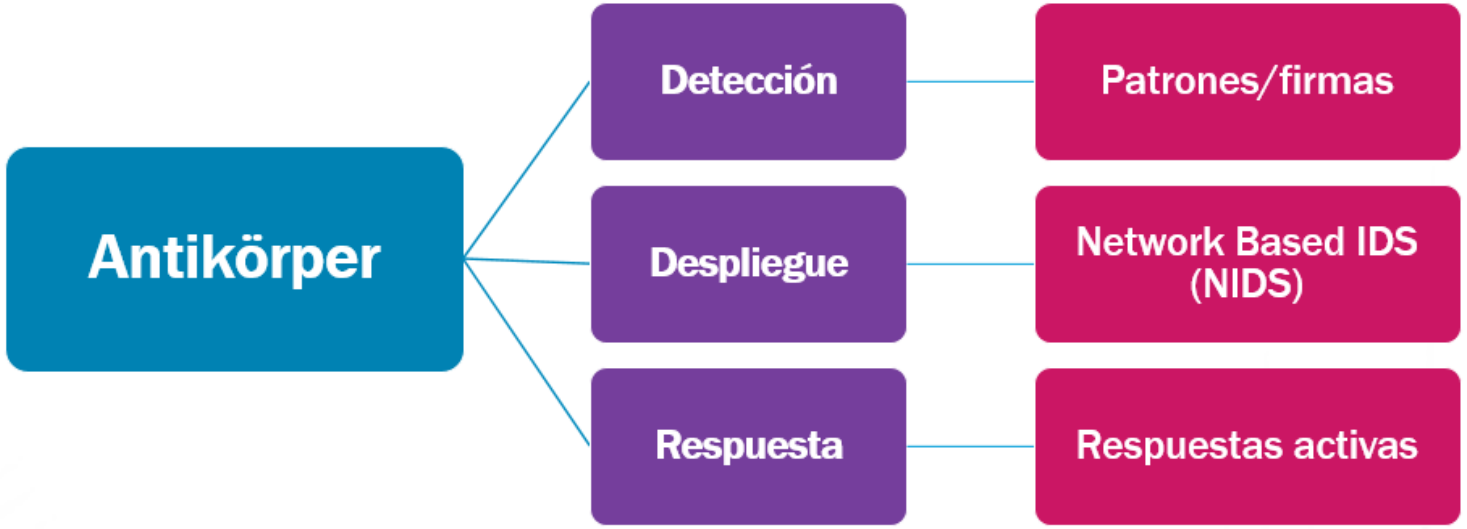
Objetivo principal:

- Diseño e implementación de un Sistema de Detección de Intrusiones Inalámbrico.

Objetivos parciales:

- Estudio del estándar IEEE 802.11 referente a las redes WLAN, arquitecturas de IDS y distintas soluciones y herramientas de seguridad.
- Diseño de un arquitectura WIDS genérica.
- Implementación y validación del sistema.

Diseño de Antikörper | Visión global

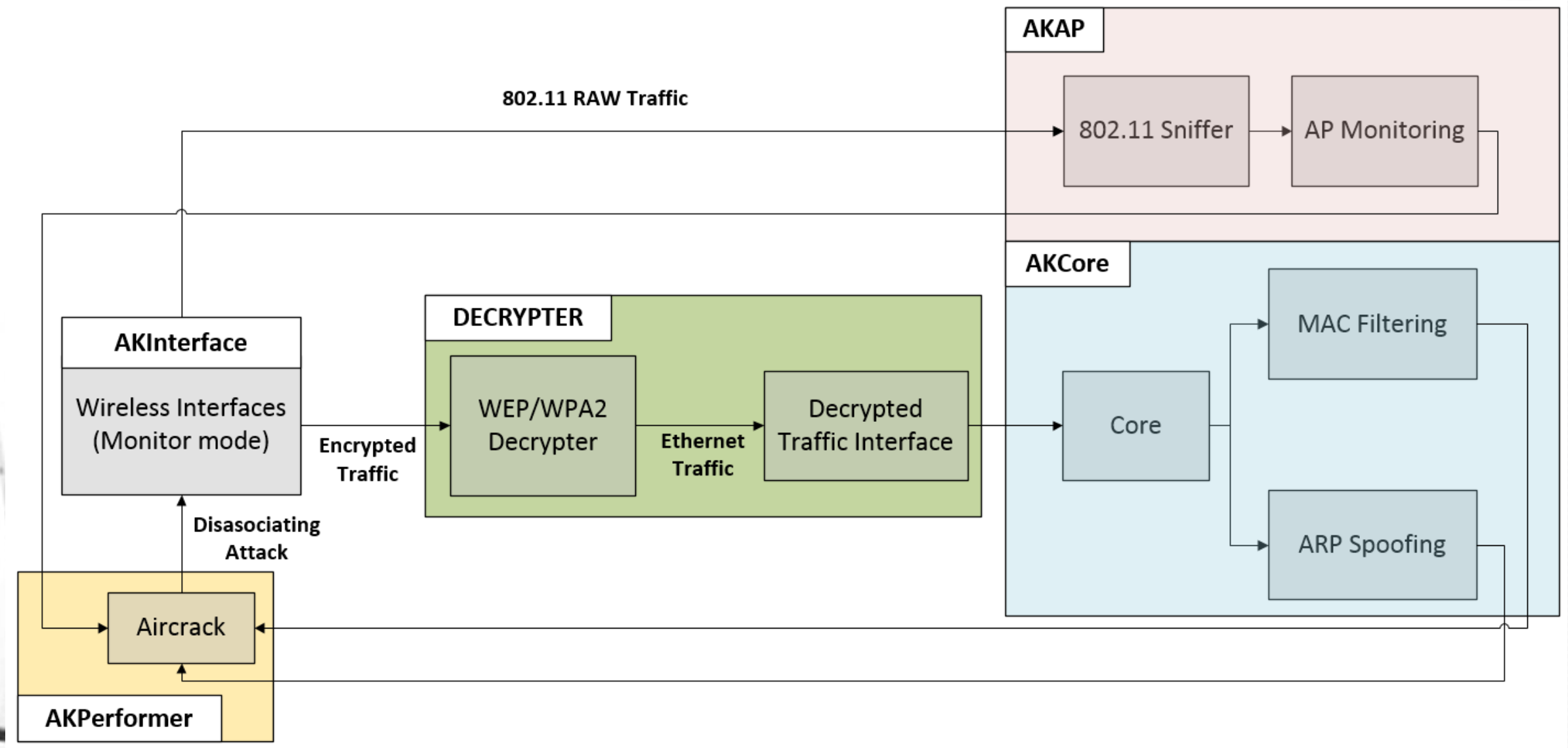


Antikörper es un IDS inalámbrico basado en Network IDS, con detección de intrusiones mediante patrones de ataque y actuación activa frente a diferentes anomalías.

Ventajas del diseño:

- Implementación sencilla de firmas/patrones de ataque.
- Rango de detección mucho mas amplio y eficiente.
- Actuación rápida y eficiente frente a las amenazas.

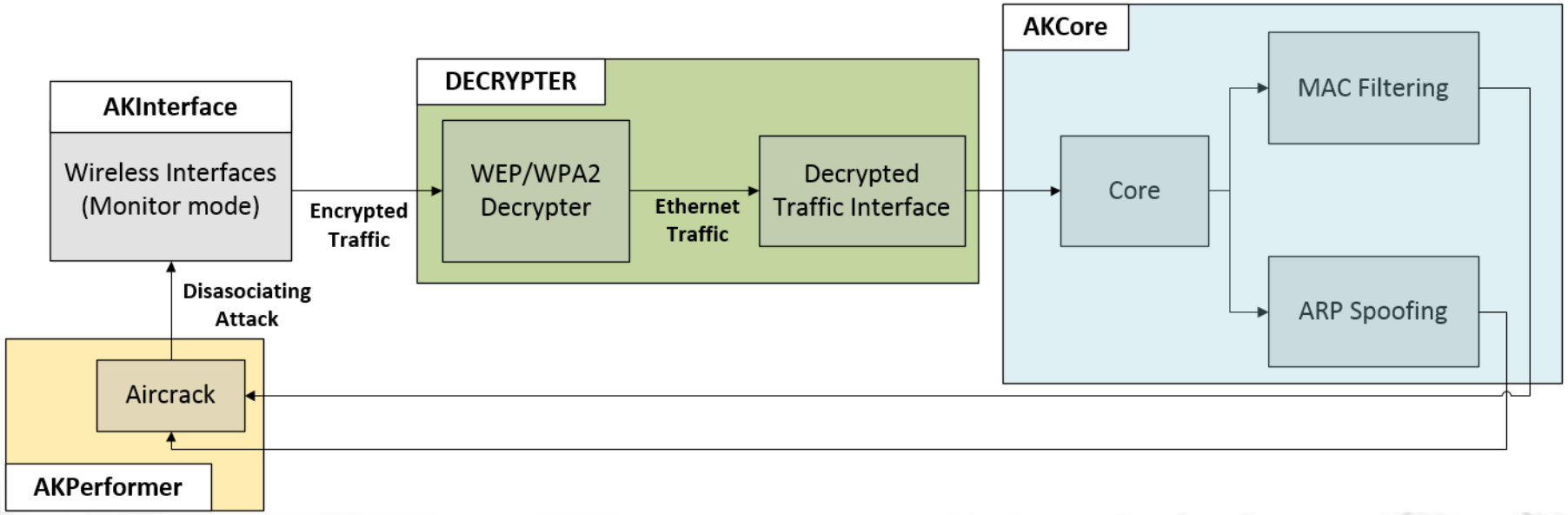
Diseño de Antikörper | Arquitectura



Diseño de Antikörper | AntikörperCore

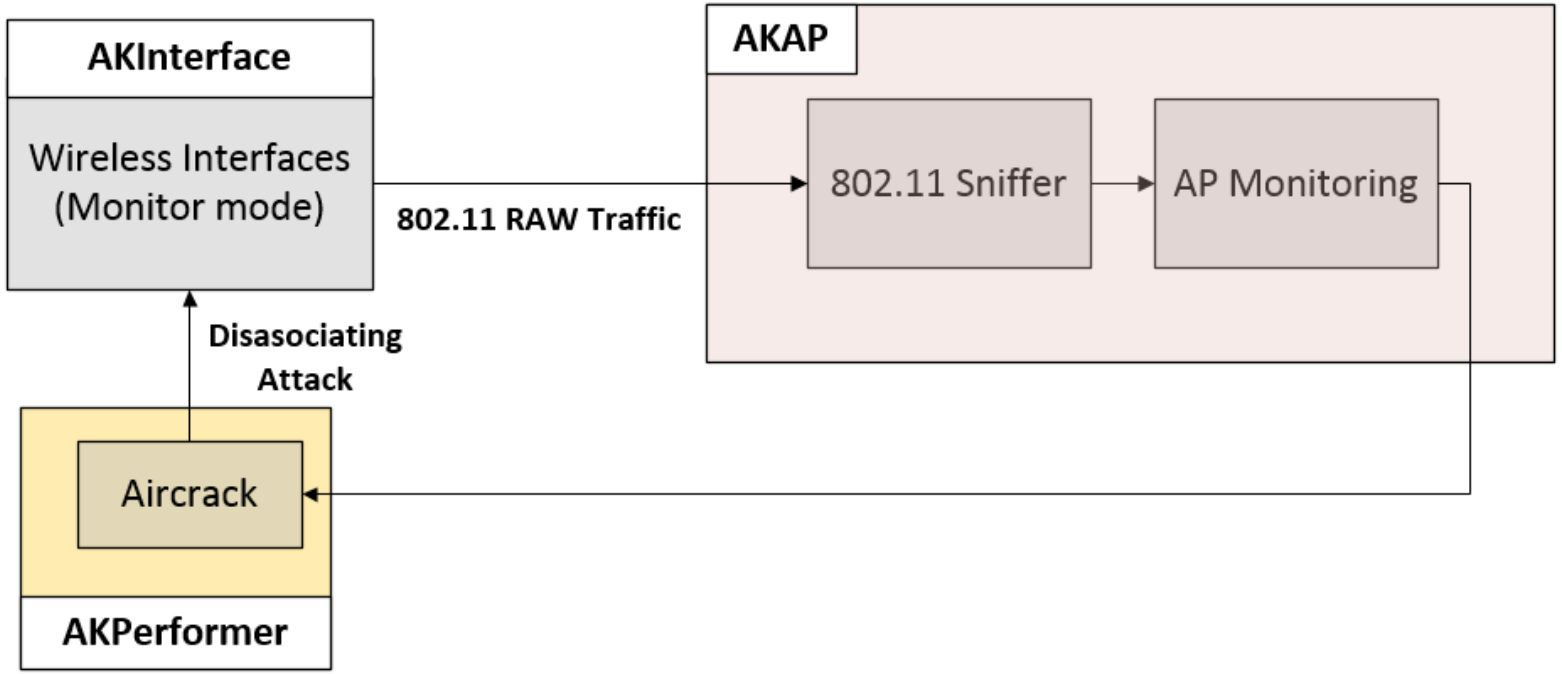
El funcionamiento del sistema está separado en dos programas independientes:

- **AntikörperCore** detecta intrusos en el interior de la red en base al tráfico capturado y desencriptado.
  - Filtrado MAC.
  - Análisis de paquetes ARP (Address Resolution Protocol).
  - Respuesta frente a intrusos.



Diseño de Antikörper | AntikörperAP

- **AntikörperAP** detecta Puntos de Acceso Maliciosos en base al trafico RAW 802.11 de WLAN.
  - Análisis de las tramas Beacon.
  - Deshabilitación de Puntos de Acceso Maliciosos.



Resultados de pruebas de rendimiento

Prueba	Medidas	
Tráfico recibido	Tramas 802.11 en red	14.789 tramas
	Tramas capturadas	14.765 ±15 tramas
	Rendimiento	99,83 %
Intrusiones detectadas	Ataques generados	500
	Ataques detectados	500
	Rendimiento	100 %
Respuestas generadas	Intrusos en red	500
	Intrusos expulsados	500
	Rendimiento	100 %

Conclusiones y trabajo futuro

- Implementación de un sistema IDS inalámbrico basado en Network IDS completamente funcional.
- Potencia, fiabilidad y estabilidad probada.
- Innovador y uno de los pocos en su especie.

Trabajo futuro:

- Implementación e integración de complementos que amplíen las funcionalidades del sistema.
- Añadir funciones de medición **QoS** (**Q**uality **o**f **S**ervice) en el sistema.
- Paradigma de sistema distribuido.
- Integrar en el sistema una base de firmas más extensa y fácilmente ampliable, junto con un procesador de tráfico heurístico.

Trabajo Fin de Grado
Grado en Ingeniería en Tecnología de Telecomunicación

Antikörper

Diseño e Implementación de un Sistema de Detección de Intrusos Inalámbrico basado en Network IDS

AUTOR: Josu Barrientos Bahamonde
DIRECTOR: Luis Zabala Alberdi

BILBAO, 3 DE MARZO DE 2015