Desarrollo y prueba de Políticas de seguridad sobre servidores WEB usando REFEREE

Sustentación del Proyecto

Autores

- Estudiantes:
  - Ing. Antonia Fernandez Segovia
  - Ing. Francis Castellanos Ariza
- Director

  Dr. Wilson Zuñiga

Guia de la presentación

- Objetivos.
- Contexto general.
- REFEREE.
- Políticas de seguridad.
- Implementacion de políticas de seguridad con REFEREE.
- Demostración aplicación desarrollada.
- Proyecciones.

Objetivos

- Realizar la evaluación de la herramienta REFEREE y sus potenciales aplicaciones
- Elaborar un manual para el desarrollo y prueba de políticas de seguridad sobre aplicaciones WEB usando la herramienta REFEREE

Guia de la presentación

- ✓ Objetivos.
- Contexto general.
- REFEREE.
- Políticas de seguridad.
- Implementacion de políticas de seguridad con REFEREE.
- Demostración aplicación desarrollada.
- Proyecciones.

Contexto General

La seguridad en el *Web* se asocia con la criptografía, protocolos y políticas públicas, obscureciendo de esta manera el gran reto de construir aplicaciones *Web* seguras. Como el objetivo del Web es ser un espacio donde la información refleje no solo el conocimiento humano sino también las relaciones humanas, en este pronto se reflejará la gran complejidad de las relaciones de confianza entre la gente, las computadoras y las organizaciones.

Manejo de Confianza

En el marco de la seguridad en computadores; el manejo de confianza surge como una nueva filosofía, para codificar, analizar y manejar decisiones de confianza en sistemas abiertos.

El cambio de modelos cerrados (donde la comunidad de usuarios es conocida) a abiertos (accedidos publicamente) complica el análisis de seguridad en las aplicaciones WEB

Manejo de Confianza (Cont...)

Las tecnologías convencionales de seguridad, aún implantadas perfectamente, no aseguran el manejo de confianza.

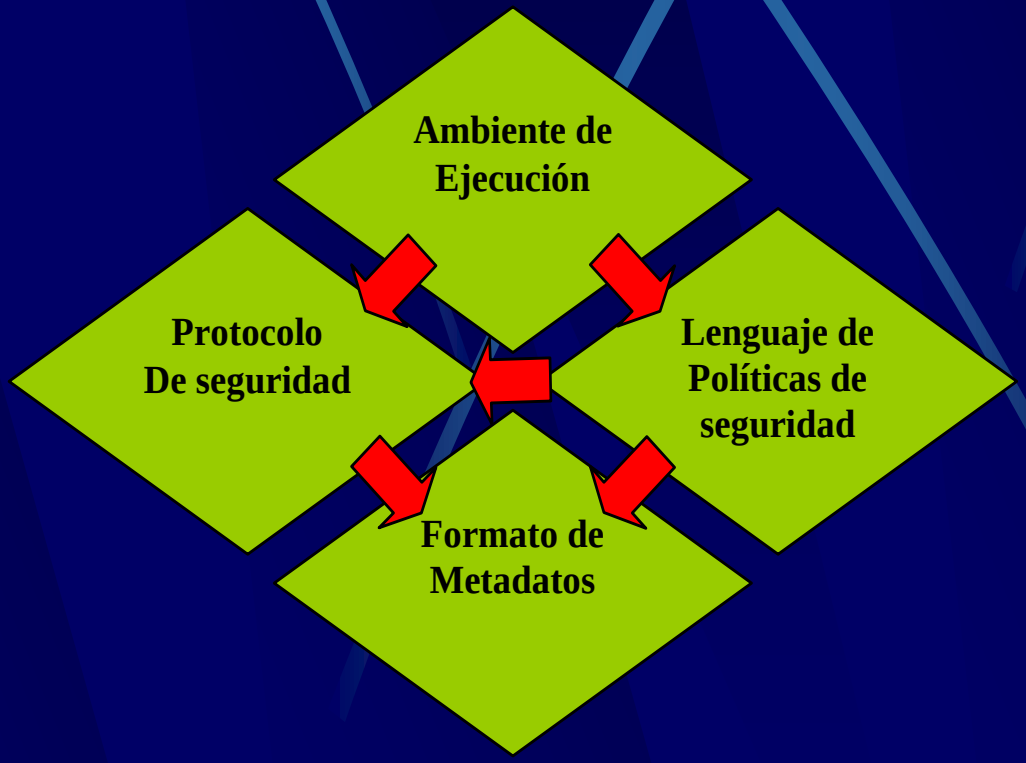
Infraestructura de Manejo de Confianza

- Formato de metadatos: Representan el medio por el cual fluye la confianza de la entidad que lo crea a la aplicación que es la que realiza la decisión de confianza.
- Protocolo de confianza: Obtiene el conjunto apropiado de aserciones para que una petición dada cumpla con una política de confianza.

Infraestructura de Manejo de Confianza (Cont..)

- Lenguaje de políticas: Permite especificar un conjunto de criterios confiables para ejecutar una acción dada.
- Ambiente de ejecución: Es un ambiente que permite interpretar las políticas de seguridad y administrar protocolos de Confianza.

dependencia de componentes de la infraestructura del manejo de confianza .



Ambiente de Ejecución

Es el corazón de un sistema de confianza porque es donde las políticas locales se encuentran con los protocolos de confianza y los formatos de metadatos para realizar las decisiones de confianza.

Ambiente de Ejecución (Cont.)

REFEREE (*Rule-controlled Environment For Evaluation of Rules and Everything Else*) fue diseñado para ser un ambiente de ejecución de propósito general para todas las aplicaciones Web que requieren seguridad, este evalúa las políticas del usuario en respuesta a un requerimiento de una aplicación *host*.

Guia de la presentación

- ✓ Objetivos.
- ✓ Contexto general.
- REFEREE.
- Políticas de seguridad.
- Implementacion de políticas de seguridad con REFEREE.
- Demostración aplicación desarrollada.
- Proyecciones.

REFEREE

Es una aplicación general para expresar y evaluar políticas para el manejo de confianza.

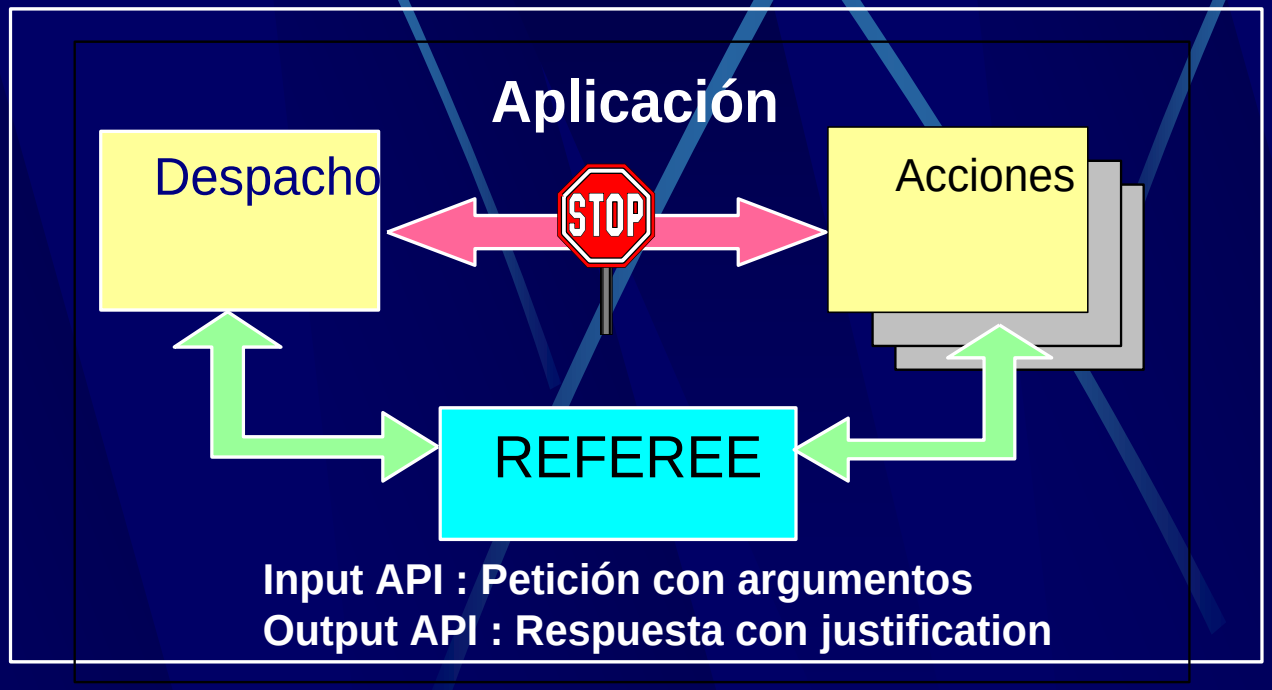
La esencia del sistema de manejo de confianza REFEREE se basa en los siguientes aspectos:

- Una aplicación llama a REFEREE con una pregunta respecto a una acción en particular. REFEREE analiza la acción y envia el resultado a la aplicación que lo llama para que esta lo interprete.

REFEREE (Cont...)

- Para cada posible acción la aplicación puede preguntar si hay una política correspondiente que se responsabilice por determinar si la acción debe ser o no realizada.
- El resultado de una llamada a REFEREE es un par consistente de una tripla lógica y una justificación para ella.

Interface externa para REFEREE



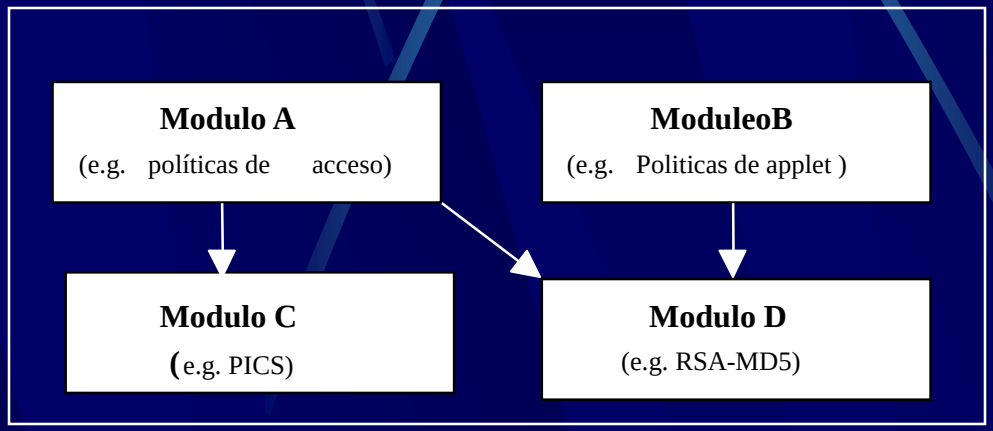
Arquitectura Interna de REFEREE

El componente básico en REFEREE es el módulo.

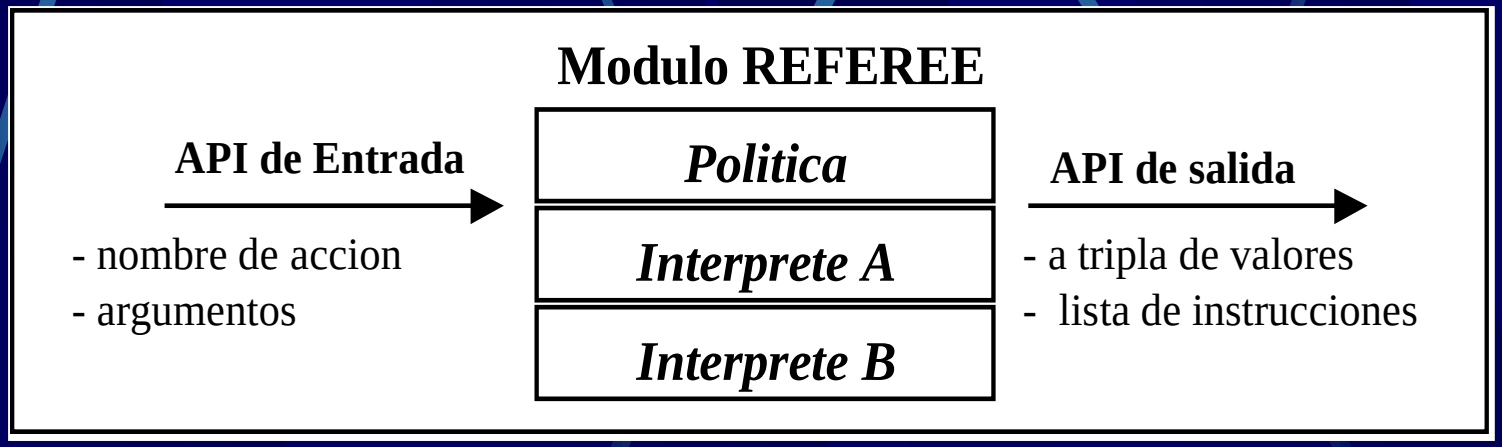
Un módulo REFEREE corresponde a un bloque de código ejecutable que procesa argumentos de entrada e instrucciones adicionales para encadenar otras tareas de diferentes módulos y hacer decisiones de confianza basado en las aserciones retornadas.

Arquitectura Interna de REFEREE (Cont.)

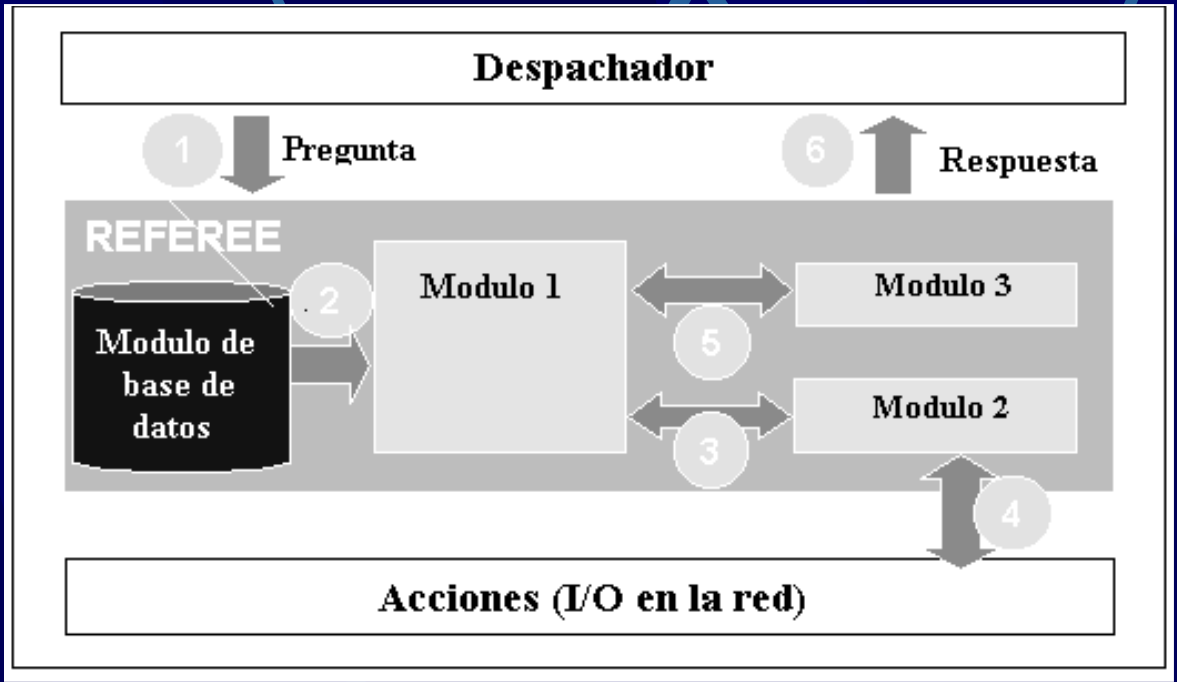
La interconectividad de los módulos de REFEREE hace que pueda procesar requerimientos de una aplicación *host* y producir una recomendación.



Interface de un módulo REFEREE



Pasos para realizar una consulta



Guia de la presentación

- ✓ Objetivos.
- ✓ Contexto general.
- ✓ REFEREE.
- Políticas de seguridad.
- Implementacion de políticas de seguridad con REFEREE.
- Demostración aplicación desarrollada.
- Proyecciones.

Políticas de seguridad

Preguntas como : Perturbarán los intrusos los sistemas internos?, Los datos valiosos de la organización estarán comprometidos (cambiados o leídos) durante cualquier transmisión?, La organización se pondrá en aprietos y perderá toda su información vital?, son muy válidas en estos momentos y las organizaciones deben colocar todo su empeño y esfuerzo en resolverlas.

Políticas de seguridad (Cont.)

El propósito de una política de seguridad en Internet es decidir como una organización se va a proteger por si misma. Las políticas de seguridad usualmente requieren dos partes:

- una política general, establece lo que abarcará la política, la seguridad de Internet.
- reglas específicas, que definen lo que esta o no permitido.

Construcción de políticas de seguridad con REFEREE

Para la construccion de las politicas de seguridad que van a ser utilizadas por REFEREE se utiliza el lenguaje PROFILES 0.92

Es un lenguaje de políticas flexible y modular cuyo objetivo es explotar y mostrar las características importantes de REFEREE en la construcción y definición correcta de las políticas de seguridad.

Funciones de PROFILES 0.92

URL Coincidencia de prefijos

url-match URL (<URL-prefijo>+)

[<prefijo-coincide?>])

Coincidencia de patrones

(match <patrón> <lista de sentencias>)

Funciones de PROFILES 0.92 (Cont.)

Formas de Combinar los *Tri-Value*

(*and* <regla>+)

(*or* <regla>+)

(*threshold-and* <num> <regla>+)

(*not* <regla>)

(*true-if-unknow* <regla>)

(*false-if-unknow* <regla>)

Funciones de PROFILES 0.92 (Cont.)

Invocación

invoke <nombre política>

<lista de sentencias>

<argumentosadicionales>)

Funciones de PROFILES 0.92 (Cont.)

- **Instalación**

(install-policy <lista de sentencias>)

(install-interpreter <lista de sentencias>)

Donde *<lista de sentencias>:*

((<contexto>)

(<identificador>

<fragmento de código>

<nombre del lenguaje>)).

Guia de la presentación

- ✓ Objetivos.
- ✓ Contexto general.
- ✓ REFEREE.
- ✓ Políticas de seguridad.
- Implementacion de políticas de seguridad con REFEREE.
- Demostración aplicación desarrollada.
- Proyecciones.

Implementación de políticas de seguridad con REFEREE

- Aplicación Host:

La aplicación desarrollada fue implementada en Java y funciona como un filtro que restringe o no el acceso a direcciones URL según los archivos de configuración definidos, utilizando a REFEREE como la herramienta para la toma de decisiones de confianza en los sitios definidos por el usuario con base en los archivos de configuración.

Implementación de políticas de seguridad con REFEREE(Cont.)

- Requerimientos:

  * Software REFEREE: Aplicación Java para la verificación y manejo de políticas.

  * Applet Ref1: Applet que utiliza el *software* REFEREE para la verificación del cumplimiento de las políticas de seguridad.

Implementación de políticas de seguridad con REFEREE(Cont.)

- Requerimientos (Cont.)

  * Archivos de configuración de políticas: Archivos de soporte a la verificación de políticas de seguridad que contienen las direcciones sobre las cuales se van a realizar controles de seguridad. Los nombres de estos archivos son: SITCON y SITRES.

Implementación de políticas de seguridad con REFEREE(Cont.)

- Requerimientos (Cont.)

* Plug-in Java: Software que permite que el *browser* corra un applet Java.

* Archivo de Seguridad de Java: Archivo que otorga a la aplicación Java los permisos de acceso a la máquina del usuario.

Implementación de políticas de seguridad con REFEREE(Cont.)

- Configuración de los archivos de políticas.

  El archivo SITCON. Contiene la lista de direcciones a las que se permite acceder desde la aplicación prototipo. Para definir las direcciones se debe utilizar obligatoriamente la siguiente sintaxis:

(allow URL "direccion1" "direccion2" "direccionN")

Implementación de políticas de seguridad con REFEREE(Cont.)

- Configuración de los archivos de políticas(Cont.).

  El archivo SITRES. Contiene la lista de direcciones desde las que no se permite bajar código y/o acceder desde la aplicación prototipo. Para definir las direcciones se debe utilizar obligatoriamente la siguiente sintaxis:

(block URL "direccion1" "direccion2" "direccionN")

Guia de la presentación

- ✓ Objetivos.
- ✓ Contexto general.
- ✓ REFEREE.
- ✓ Políticas de seguridad.
- ✓ Implementacion de políticas de seguridad con REFEREE.
- Demostración aplicación desarrollada.
- Proyecciones.

DEMOSTRACION

Guia de la presentación

- ✓ Objetivos.
- ✓ Contexto general.
- ✓ REFEREE.
- ✓ Políticas de seguridad.
- ✓ Implementacion de políticas de seguridad con REFEREE.
- ✓ Demostración aplicación desarrollada.
- Proyecciones.

Proyecciones

A manera de futuros desarrollos con REFEREE consideramos que seria interesante y provechoso instalarlo en un servidor WEB y evaluar los resultados desde el punto de vista técnico (funcionalidad, tiempo de respuesta, facilidad de uso, consumo de recursos, etc) y desde el punto de vista de los usuarios.

Fin de la presentación.

Agradecimientos