TITULO: Un Mecanismo de Defensa para la Seguridad de Redes con los Módulos de Seguridad de Linux  
AUTOR: Jichiang Tsai, Chung-Hsin Feng y Chuyuan Tsai  
FUENTE: Departamento de Ingeniería Eléctrica, Universidad Nacional Chung Hsing, Taichung.

SINTESIS:

Ante el creciente uso de Internet y el aumento de dispositivos conectados, los gateways son un punto crítico de seguridad. Este mecanismo, refuerza la seguridad interceptando y validando las llamadas de API antes de ejecutarlas en el kernel. Cada llamada es verificada en función de políticas de seguridad previamente configuradas, permitiendo o denegando la acción.

Cuando se invoca una API de sockets, el sistema revisa varios atributos clave:

* **Número de puerto:** Solo se permiten puertos autorizados.
* **Tipo de socket (UDP o TCP):** Se restringe el uso de UDP a menos que sea estrictamente necesario.
* **Nombre del proceso:** Se verifica que el proceso que solicita acceso sea legítimo.
* **UID (User ID):** Solo usuarios autorizados, especialmente con privilegios pueden realizar ciertas acciones.

Es crucial que el sistema valide los atributos fundamentales de cada llamada de red para garantizar que solo las operaciones legítimas puedan ejecutarse. Una vez establecido este filtro inicial, el mecanismo también cuenta con medidas específicas para prevenir distintos tipos de ataques.

* **Backdoor y Worm:** Se evita que procesos no autorizados abran puertos o establezcan conexiones no permitidas.
* **Escaneo de puertos:** Se detectan intentos de escaneo analizando la frecuencia de los paquetes RST, bloqueando IPs sospechosas.
* **SYN Flood**: Se utiliza la tecnología de cookies SYN para evitar la saturación de las colas de conexión del servidor.

En definitiva, este mecanismo refuerza la seguridad en redes basadas en Linux, proporcionando una protección robusta y flexible contra amenazas comunes, sin afectar la funcionalidad de las conexiones legítimas y asegurando una gestión eficaz de los recursos en la red.