IMPLEMENTACIÓN DE TÉCNICAS DE SEGURIDAD INFORMÁTICA PARA GARANTIZAR LOS PRINCIPIOS DE INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN A UN SISTEMA DE RADIOLOCALIZACIÓN HÍBRIDO

MAURICIO MEJÍA MEDINA

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLIN

2019

IMPLEMENTACIÓN DE TÉCNICAS DE SEGURIDAD INFORMÁTICA PARA GARANTIZAR LOS PRINCIPIOS DE INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN A UN SISTEMA DE RADIOLOCALIZACIÓN HÍBRIDO

MAURICIO MEJIA MEDINA

Trabajo de grado para optar al título de Magister en TIC

Asesor

CRISTINA GOMEZ SANTAMARIA

PhD en Ingeniería

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLIN

2019

DECLARACIÓN ORIGINALIDAD

“Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad”. Art. 82 Régimen Discente de Formación Avanzada, Universidad Pontificia Bolivariana.

FIRMA AUTOR (ES) _____

AGRADECIMIENTOS

El apoyo y el estímulo provienen de diferentes fuentes y de varias maneras. En particular, me gustaría agradecer al profesor Leonardo Betancour y al grupo de investigación GIDATI (Grupo de Investigación Desarrollo y Aplicación en Telecomunicaciones e Informática) por brindarme la oportunidad de pertenecer a la Universidad Pontificia Bolivariana e iniciar mis estudios de Maestría. A mi madre quien me ha brindado la mejor orientación posible a lo largo de mi vida, a todos mis mentores que me han brindado su conocimiento y experiencias y que de alguna manera me han permitido ser el profesional que hoy soy.

También quiero expresar mi profundo agradecimiento a mi directora de tesis, la PhD Cristina Gómez Santamaria, por su consejo, paciencia, apoyo constante y una fuente inagotable de ideas, quien me direccionó durante mi paso por la universidad nutriéndome de su conocimiento y experiencias. Su comprensión y consejo han sido factores cruciales para completar con éxito este trabajo. Su amplitud de conocimiento y su entusiasmo por la investigación fueron determinantes. Ella ha sido la responsable de introducirme en el campo de las redes de sensores y sentó las bases sobre las cuales se construyó este trabajo.

CONTENIDO

LISTA DE IMAGENES

RESUMEN

Con la globalización de las comunicaciones y la alta demanda de servicios inalámbricos, gran parte de los sectores de la industria (público y privado) han adoptado este tipo de tecnologías con el fin de optimizar sus procesos e incrementar su productividad, lo que se traduce en desarrollo y oportunidad.

A medida que las redes inalámbricas y más exactamente las de sensores se acercan hacia un despliegue generalizado, los problemas de seguridad se convierten en una preocupación central. Hasta ahora, muchas investigaciones se han centrado en hacer las redes de sensores factibles y útiles dejando una brecha importante en cuanto a la seguridad. Además, con la llegada de Internet de las Cosas, estas tecnologías de red de sensores han comenzado a tener un avanzado desarrollo y auge en el entorno mundial.

La UPB viene ejecutando el Proyecto de investigación “CLASS – Compressed Localization and Spectrum Sensing for cognitive radio and radiosurveillance”, el cual pretende desarrollar un sistema de radiolocalización híbrida basado en el paradigma de sensado comprimido. Este sistema IoT (Internet of Things) Internet de las cosas en español, pretende localizar transmisores, en algunos casos ilegales, con fines de monitoreo, vigilancia, regulación y gestión del espectro electromagnético. Teniendo en cuenta estas importantes tareas, que son en la práctica implementadas por organismos nacionales como la ANE (Agencia Nacional del Espectro) en Colombia, es necesario garantizar los principios básicos de seguridad de la información.

Este trabajo de grado propone la implementación de métodos de seguridad de la información a las vulnerabilidades que sean identificadas en el sistema de radiolocalización híbrida propuesto en el proyecto CLASS, centrándonos en el

centro de fusión y tomando como base un pre-diagnóstico realizado con anterioridad en otro trabajo de grado.

PALABRAS CLAVE: Red de sensores inalámbricos; Radiolocalización; Internet de las Cosas; Algoritmos híbridos; Seguridad en WSN, Apache, ModSecurity, Servidor web, Centro de fusión.

ABSTRACT

With the globalization of communications and the high demand for wireless services, most sectors of industry (public and private) have adopted this type of technology in order to optimize their processes and increase their productivity, which translates into development and opportunity.

As wireless networks become widespread, security issues become a central concern. So far, much research has been focused on making sensor networks feasible and useful, opening an important safety gap. In addition, with the advent of IoT (Internet of Things), these sensor network technologies have begun to have an advanced development and increase in the global environment.

The project “CLASS – Compressed Localization and Spectrum Sensing for cognitive radio and radiosurveillance”, is being executed by UPB. This project intends to develop a hybrid radiolocation system based on compressed sensing. This IoT system is designed to locate illegal transmissions for applications as monitoring, surveillance, regulation and spectrum management. These important tasks are executed by national agencies like ANE in Colombia, hence it is necessary to guarantee the basic principles of information security in this network.

This thesis pretends to implement information security methods to vulnerabilities identified in the hybrid radiolocation system, focusing on the fusion center and thus giving continuity to a pre-diagnosis obtained in a previous master thesis.

KEY WORDS: Wireles sensor network; Radiolocalization, Internet of things; Hybrid algorithms; WSN security, Apache, ModSecurity, Web server, Fusion Center.

1. INTRODUCCIÓN

En los últimos años, los avances tecnológicos en el diseño de procesadores, memoria y comunicaciones de radio han impulsado un interés activo en el área de la red de sensores distribuidos, en la que una cantidad de nodos independientes y autosostenibles colaboran para realizar una gran tarea de detección. Las redes de dichos dispositivos, comúnmente denominadas Wireless Sensor Networks (WSN), se acercan cada vez más a la viabilidad generalizada y han permitido el diseño y la proliferación de nuevos entornos inteligentes basados en una variedad de sensores.

En ese sentido, los avances en sistemas y las tecnologías de comunicación inalámbrica han permitido la construcción de pequeños dispositivos que pueden funcionar de manera autónoma y ser implementados a gran escala, gracias a características como baja potencia y bajo costo, lo que es atractivo para la industria.

Por todo lo anterior, y dando continuidad al proyecto “CLASS – Compressed Localization and Spectrum Sensing for Cognitive Radio and Radiosurveillance”, este trabajo surge de la necesidad de fortalecer el sistema frente a amenazas y/o posibles ataques de ciberseguridad y para esto, inicialmente se realizará una consulta de diferentes fuentes bibliográficas que permitirán fundamentar algunos conceptos necesarios, para posteriormente recorrer el estado del arte que a su vez servirá como insumo para el desarrollo y construcción del plan de aseguramiento en el capítulo de presentación y análisis de resultados, que incluye; El análisis de vulnerabilidades, tratamiento y fortalecimiento del servidor que tendrá el rol de centro de fusión para la plataforma.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 PROBLEMA

La ANE (Agencia Nacional del Espectro) es la entidad encargada de diseñar y formular políticas, planes y programas relacionados con la vigilancia y control del Espectro, en concordancia con las políticas nacionales y sectoriales y las propuestas por los organismos internacionales competentes, cuando sea el caso. Dado lo anterior surge la necesidad de identificar fuentes transmisoras y/o emisoras que usen el espectro radioeléctrico de forma ilegal, con el fin de ejercer el control aplicando las sanciones pertinentes o que haya lugar.

El grupo de Investigación GIDATI de la Universidad Pontificia Bolivariana sede Medellín viene trabajando desde hace aproximadamente 2 años en un proyecto de radiolocalización híbrido haciendo uso de técnicas de sensado comprimido. Este proyecto titulado “CLASS – Compressed Localization and Spectrum Sensing for Cognitive Radio and Radiosurveillance” se está desarrollando en cooperación con la Universidad ICESI de la ciudad de Cali, la Universidad Técnica de Ilmenau y la Universidad de Aaachen de Alemania, y tiene como objetivo la vigilancia del espectro radioeléctrico utilizando técnicas de radiolocalización híbrida bajo el paradigma de sensado comprimido.

El prototipo del sistema de radio localización híbrido propuesto en este proyecto está compuesto por varios nodos sensores y un servidor central (Centro de Fusión) que gestiona el sistema. Actualmente los principios usados en este tipo de arquitecturas inalámbricas, más específicamente en los WSN, presentan vulnerabilidades intrínsecas. Estas vulnerabilidades fueron evaluadas y tratadas en un trabajo anterior y no son objeto de estudio de este trabajo; enfocándonos principalmente en la arquitectura que soporta el servidor central o centro de fusión (Sistema Operativo Linux y Servidor Apache).

El ecosistema es susceptible a ataques de seguridad tales como: Ataques de acceso, que incluyen intentos de obtener acceso no autorizado a los recursos del sistema. Ataques a la privacidad, que representan intentos de interceptar la transferencia de datos en el entorno de transporte. Ataques a la integridad, que incluyen la generación y transferencia de frames para capturar y controlar el sistema, invocar fallas y errores en su funcionamiento o para preparar otros ataques como por ejemplo de denegación de servicio, entre otros. (Finogeev &

Finogeev, 2017) De este modo es necesario el aseguramiento de la infraestructura ya que la información a transmitir es determinante para la toma de decisiones en el sistema.

2.2 JUSTIFICACIÓN

La Agencia Nacional de Espectro (ANE) es la entidad encargada de realizar la planeación, atribución, vigilancia y control del Espectro Radioeléctrico en Colombia (MinTIC, 2016), así como de brindar la asesoría técnica para la gestión eficiente del mismo y fomentar su conocimiento, tiene la necesidad de gestionar eficientemente este recurso. La ANE, requiere de mecanismos tecnológicos de sensado que permitan identificar las fuentes de transmisión dentro del territorio nacional, todo ello soportado en una infraestructura que garantice políticas de seguridad de la información que garanticen principios tales como: integridad, confidencialidad y disponibilidad.

Dado lo anterior surgió el proyecto de grado de Maestría “Seguridad de la Información en una red de sensores para radiolocalización en aplicaciones de vigilancia del espectro electromagnético” donde se buscaba identificar vulnerabilidades del sistema y asegurar los nodos de la red de sensores. De esta forma, el presente trabajo de grado constituye una continuación, buscando complementar el diagnóstico de vulnerabilidades allí realizado, así como implementar las recomendaciones identificadas para asegurar el centro de fusión mediante la implementación de técnicas y/ó metodologías de seguridad de la información que brinden un tratamiento adecuado a las vulnerabilidades críticas del sistema.

3. OBJETIVOS

3.1 Objetivo General

Implementar técnicas de seguridad a un prototipo del sistema de radio localización híbrido (Centro de Fusión) con el fin de garantizar los principios de confidencialidad, integridad y disponibilidad de la información del sistema.

3.2 Objetivos Específicos

a) Identificar las diferentes vulnerabilidades presentes en el Centro de Fusión.

b) Asegurar el Centro de Fusión acorde al análisis de resultados obtenido, mediante las técnicas disponibles a las vulnerabilidades previamente identificadas.

c) Validar la implementación de las técnicas de seguridad en el Centro de Fusión.

4. MARCO REFERENCIAL

4.1 MARCO CONTEXTUAL

Este trabajo de grado se enmarca en el desarrollo del proyecto de investigación "CLASS – Compressed Localization And Spectrum Sensing for cognitive radio and radiosurveillance", una propuesta aprobada en el Marco de Cooperación Colombo-Alemana en Ingeniería Eléctrica y Comunicaciones. Este proyecto inició en Marzo de 2015 y finalizará en Marzo de 2019.

La motivación del proyecto proviene de la reglamentación establecida por la ITU – International Telecommunications Union, que establece que la vigilancia de radio debe realizarse por las entidades gubernamentales de regulación del espectro, con el fin de monitorear posibles usos ilegales del mismo (ITU, 2012) Esto tiene aplicaciones para tecnologías como vigilancia de radio y radios cognitivos.

El proyecto CLASS aborda esta problemática desde el punto de vista del paradigma Sensado Comprimido, revolucionario en la forma de realizar la adquisición de señales. El problema de radiovigilancia es también abordado por el grupo de investigación GIDATI en el programa estratégico de investigación "Desarrollo de Capacidades Tecnológicas en Comprobación Técnica del Espectro", desde un punto de vista clásico en la manera de realizar la adquisición de señales. Aunque estos proyectos son diferentes en la forma de dar solución al problema, ambos utilizan la misma red de sensores, la diferencia son los algoritmos implementados en cada caso. Uno de los retos identificados en ambos proyectos es que la información enviada por los sensores al centro de fusión, la cual es clave para realizar los algoritmos de radiolocalización, puede ser alterada si no se establecen mecanismos de seguridad.

Por este motivo se desarrolló el trabajo de grado de Maestría "Seguridad de la Información en una Red de sensores para radiolocalización en aplicaciones de vigilancia del espectro electromagnético", realizada por el estudiante Vladimir Francesco Pérez. Esta tesis tenía como objetivo general "Proponer un grupo de métodos para minimizar el impacto de las vulnerabilidades de seguridad para los nodos sensores del prototipo del sistema de sensado de espectro en el proyecto "Desarrollo de Capacidades Tecnológicas en Comprobación Técnica del Espectro", con el fin de garantizar al centro de fusión el procesamiento de señales fidedignas

para sus labores de identificación de transmisores". Este trabajo de grado tenía como alcance realizar un informe final exponiendo el plan de seguridad para asegurar el nodo de sensores de la red de sensado del espectro e implementar la solución a algunos de ellos. Dentro de ese trabajo de grado se decidió asegurar los nodos de la red de sensores. De esta forma, el presente trabajo de grado constituye una continuación al anterior, buscando complementar y actualizar el diagnóstico realizado ya que se incorporaron nuevos nodos sensores en la red IoT y se rediseñó e integró el centro de fusión local desarrollado en la UPB, con el centro de fusión global implementado por la Universidad ICESI. Adicionalmente se realizará la implementación de las técnicas de seguridad requeridas según el diagnóstico de vulnerabilidades con énfasis en el aseguramiento del centro de fusión de la red de sensores.

4.2 MARCO CONCEPTUAL

4.2.1 ESCENARIOS DE LOCALIZACIÓN

Un escenario de localización, como el que muestra la Imagen 1, está conformado por un conjunto de al menos tres nodos cuyas coordenadas (X_{Nr1},Y_{Nr1}), (X_{Nr2},Y_{Nr2}) y (X_{Nr3},Y_{Nr3}) establecen el área de localización (sombreada en gris) y uno o más nodos móviles (X_{M1},Y_{M1}) de los cuales se desconoce su ubicación. En uno de los posibles escenarios (Escenario 1) los nodos fijos pueden funcionar como receptores (P_{rx1}, P_{rx2}, P_{rx3}) desde donde es posible medir algunos parámetros de la señal enviada por cada uno de los nodos móviles como son: potencia recibida, expresada como la señales RSSI (Received Signal Strength Indicator) indicadas en la Imagen 1 como (RSSI_1, RSSI_2, RSSI_3), el ángulo de llegada (θ_1, θ_2, θ_3) o el tiempo que tardan las señales (t_1, t_2, t_3) en viajar desde el nodo transmisor hasta los nodos receptores. En otro de los escenarios (Escenario 2), los nodos fijos funcionan como transmisores (T_{X1}, T_{X2} y T_{X3}) y el nodo móvil es el receptor (Pr_x). El cálculo de la posición puede realizarse directamente en este nodo, si se tiene suficiente poder de cómputo. Este escenario solo puede aplicarse en casos donde los algoritmos no requieren medidas de varios sensores (R_X) o en un punto externo E_1 (Escenario 3) que recibe los parámetros medidos con los cuales estima la posición y que puede o no, realimentar las coordenadas estimadas al nodo móvil.

El procesamiento de las señales puede realizarse en cada uno de los nodos fijos, lo cual se conoce como procesamiento distribuido. Este permite la auto-organización

de la red de sensores inalámbricos basado en la combinación de dos estrategias complementarias; la primera denominada jerarquización de la red, refiriéndose a la división de la red en grupos de nodos, cada grupo contando con un nodo representante y la segunda, procesado intra-red, donde todo el tratamiento y todos los algoritmos aplicados a los datos antes de abandonar la red de sensores, es decir, es un procesado realizado por los nodos.

Cuando las señales son enviadas a un solo nodo procesador (Centro de Fusión) para allí realizar los cálculos de la posición desconocida, es lo que se conoce como procesamiento centralizado. (Rugeles & Leon, n.d.)

La localización se desarrolla en tres fases; primero se realiza la estimación de la distancia y/o ángulo, posteriormente se calcula la posición aproximada y por último se hace un refinamiento de la posición. Las técnicas de localización pueden de tres tipos: basadas en distancias, en ángulos o independientes de distancias y/o ángulos (Garcia Polo, n.d.). Cualquiera de ellas, busca recopilar mediante mediciones de parámetros de las señales de radio, suficiente información del entorno que permita establece la ubicación del nodo móvil. Para realizar estas medidas se deben tener en cuenta los requerimientos en cuanto al hardware necesario en cada nodo y las capacidades de procesamiento, según la técnica a utilizar.

Entre las técnicas más empleadas se encuentran: RSSI (Received Signal Streng Indication), ToA (Time of Arrival), TDoA (Time Delay of Arrival), AoA (Angle of Arrival) y RTOF (Round Trip Time Of Fligth), Fingerprinting y APIT (Approximate Point In Triangulation). Dependiendo de si el transmisor “desea” ser localizado o no, los sistemas de radiolocalizacion pueden ser clasificados en colaborativos o no colaborativos. Un Sistema colaborativo es aquel donde el transmisor aporta información importante para la estimación de su posición, allí puede aplicarse cualquiera de las técnicas anteriormente mencionadas. Un Sistema no colaborativo es aquel donde el transmisor no proporciona ninguna información que ayude a la estimación de sus posición, alli aplican las tecnicas TDoA, y DoA principalmente.

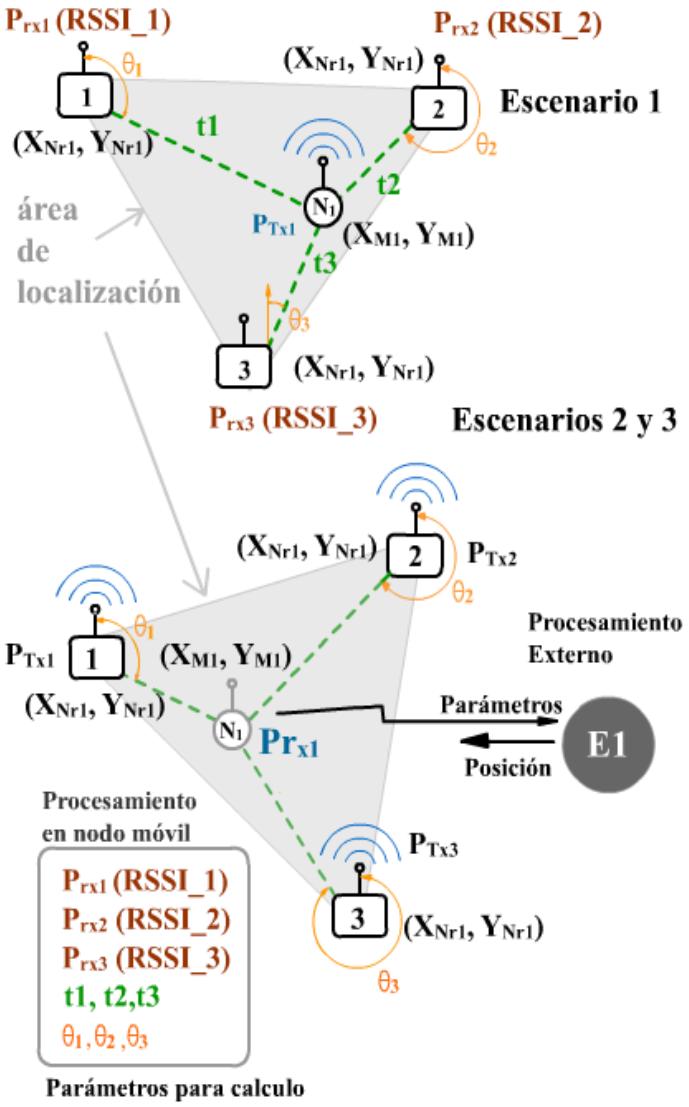


Imagen 1 Escenarios de localización nodo móvil transmisor

Fuente (Rugeles & Leon, n.d.)

En la Imagen 2 se describe el escenario para las tecnologías de radiolocalización descrito en *"Survey of Wireless Indoor Positioning Techniques and Systems"* (Liu, 2007) , donde se relacionan las técnicas de localización, las tecnologías y los niveles de resolución alcanzados en la fecha de estudio de ese entonces.

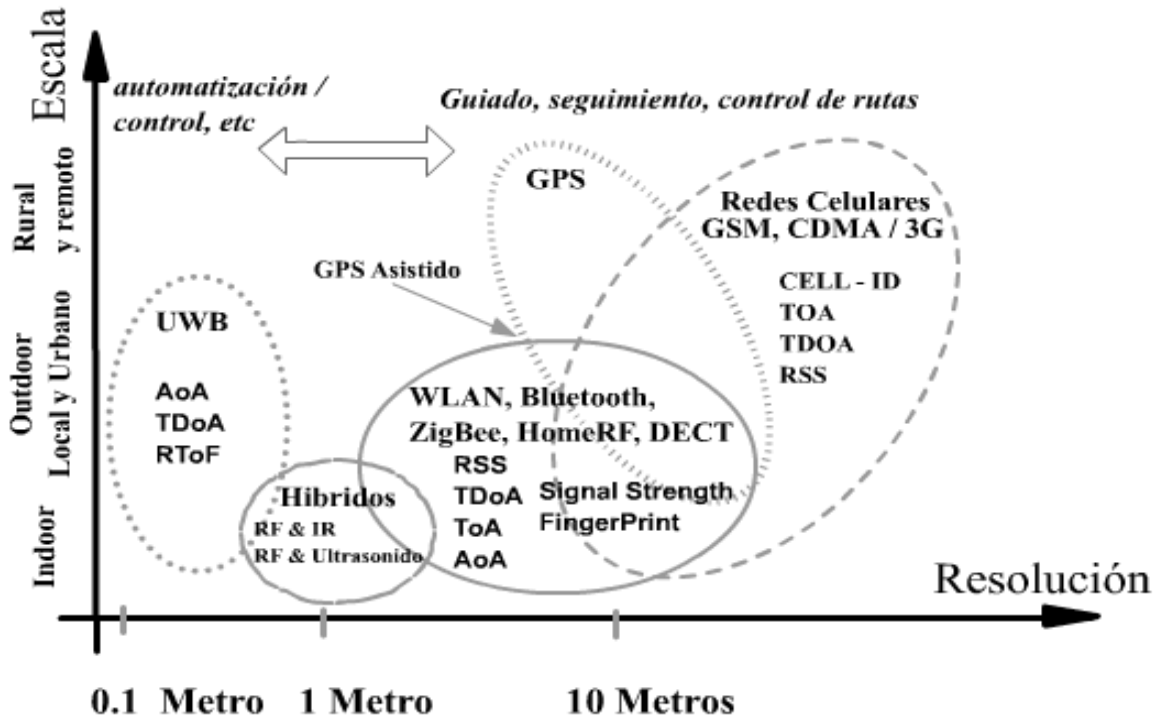


Imagen 2 Tecnologías de localización

Fuente (Liu, 2007)

4.2.2 TECNICAS BASADAS EN DISTANCIAS

4.2.2.1 INDICADOR DE INTENSIDAD DE SEÑAL RECIBIDA (RSSI):

Existen diferentes métodos para medir la potencia de una señal radioeléctrica recibida por un dispositivo, Si se conoce su intensidad de potencia se podría estimar la distancia a la cual está ubicado el emisor. Para calcular la potencia recibida, el estándar IEEE 802.11 propone el uso del indicador RSSI, el cual es un valor almacenado en un byte que puede tomar 256 valores enteros entre 0 y 255. (Rey & Carlos, 2014). RSSI solo puede ser empleada en escenarios colaborativos, dado que es necesario conocer la potencia de trasmisión.

Aunque pareciera simple, esta técnica presenta significativos errores ocasionados por las pérdidas de trayecto dependientes de las características

físicas del entorno (Chen & Yang, 2006). Hoy por hoy las señales RSSI no son el método más confiable para implementar sistemas de radiolocalización, pero se consolida como una de las técnicas con mayor potencial para masificar la tecnología de radiolocalización por su bajo costo de implementación. (Rugeles & Leon, n.d.)

El modelo propuesto por (O. Gualdrón, S. Pinzón, L. De Luque, I. Díaz, 2006) realiza la predicción de RSSI en un escenario dado teniendo en cuenta:

- La disminución de la señal generada por los obstáculos de la edificación.
- La influencia del material de construcción del escenario en la atenuación del RSSI.
- La separación entre el punto de acceso y cada uno de los usuarios móviles.

$$RSSI = P_{AP} - (L_{FS} + L_T + L_{T-x})$$

Ecuación 1 RSSI

Fuente: (O. Gualdrón, S. Pinzón, L. De Luque, I. Díaz, 2006)

Donde:

P_{AP} = Potencia emitida por el Access Point

L_{FS} = Pérdida por espacio libre

L_T = Pérdida por transmisión (obstáculos)

L_{T-x} = Pérdida por transmisión hasta el punto de cálculo

4.2.2.2 TIEMPO DE LLEGADA (ToA)

La técnica ToA se refiere al tiempo medido en el que una señal de radio tarde en llegar al receptor. El tiempo de medición ToA se compone del tiempo de transmisión más el tiempo necesario utilizado por la señal para propagarse por el medio. (Fern, 2010); En este método la distancia $\boldsymbol{r_{TOA}}$ entre dos nodos es directamente proporcional al tiempo que tarda la señal en propagarse desde un punto a otro, como se observa en la ecuación 2, donde c corresponde a la velocidad de la luz, ***t1*** al tiempo en el cual se envía la señal desde el nodo 1 al nodo 2 y ***t2*** es el tiempo en el cual se recibe la señal en el nodo 2, lo que implica alta capacidad de computo, incrementándose de este modo la latencia en el procesamiento de los receptores.

La distancia entre dos terminales es directamente proporcional al tiempo de propagación de la señal entre ellos.

$$\boldsymbol{r_{TOA} = c \times (t1 - t2)}$$

Ecuación 2 ToA

Fuente: (Fern, 2010)

Esta técnica requiere de un sistema de sincronización entre nodos y del envío de la información de los tiempos dentro de los paquetes.

4.2.2.3 DIFERENCIA EN EL TIEMPO DE LLEGADA (TDOA)

TDoA, utiliza la medición de la diferencia de tiempos que tarda en llegar una señal radiada desde un nodo móvil hasta cada uno de los receptores; estas diferencias de tiempo se miden con respecto a uno de los sensores elegido como nodo de referencia, y los tiempos que tardan en llegar las señales enviadas desde los receptores hasta el nodo móvil. En este caso la sincronización entre receptores es de vital importancia para la estimación de la posición con buena precisión. Esta técnica puede usarse en esquemas colaborativos calculando el TDoA a partir del ToA, o en esquemas no colaborativos con base en análisis por correlación.

TDoA se clasifica además en dos tipos, es decir, TDoA de múltiples nodos y TDoA de señales múltiples. El TDoA de varios nodos utiliza mediciones de ToA

de señales transmitidas desde múltiples balizas y esta técnica se basa en medir la diferencia en el tiempo. El TDoA de señales múltiples utiliza dos tipos diferentes de señales con diferente velocidad de propagación para estimar su distancia a otro nodo. Sin embargo, esta técnica necesita equipo adicional: un micrófono y un altavoz, como se puede observar en la Imagen 4. Debido a que las distancias entre un transmisor y diferentes receptores varían, la señal transmitida se retrasa en consecuencia. La Imagen 1, muestra un escenario de localización TDOA con un grupo de cuatro receptores en las ubicaciones r1, r2, r3, r4 y un transmisor en rt. Otra forma de estimar la TDoA se refiere a la medición del retardo de tiempo entre los receptores mediante el cálculo de la correlación cruzada de las señales recibidas. Todos los métodos TDoA mencionados demuestran una alta precisión solo en condiciones de visibilidad directa.

Dependiendo del escenario, colaborativo o no colaborativo, también conocidos como escenarios centralizados o distribuidos (Imagen 3), dichas diferencias de tiempo se pueden calcular de varias maneras.

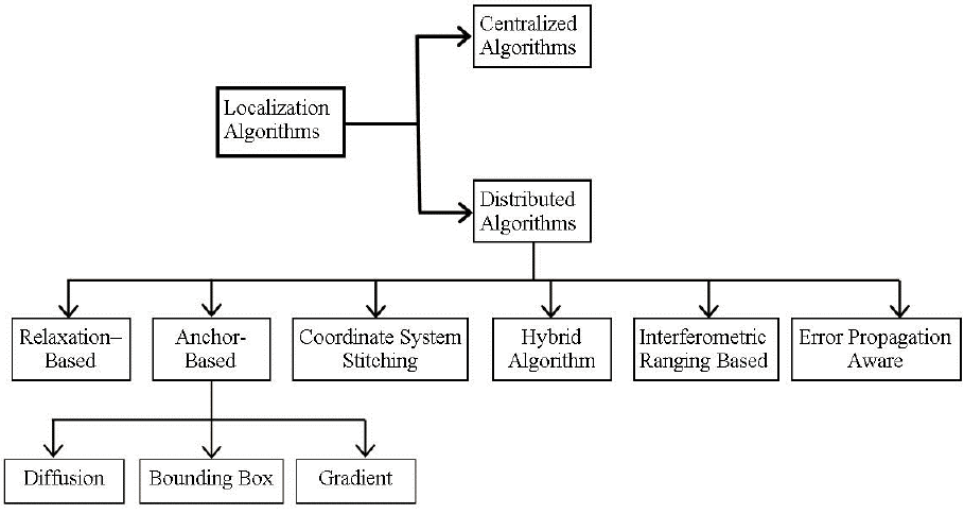


Imagen 3 Clasificación algoritmos de localización

Fuente: (Abdullah & Teknologi, 2014)

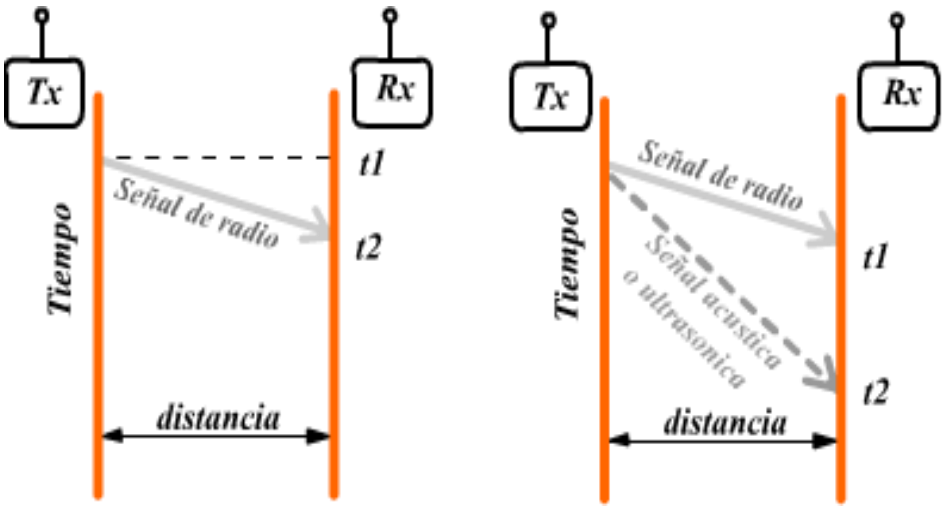


Imagen 4 Medida de distancia con ToA y TDoA

Fuente: (Rugeles & Leon, n.d.)

La distancia se puede obtener mediante la ecuación 3. Además de la señal de radio, se requiere enviar otra señal, que puede ser acústica o ultrasónica.

$$D = (V_r - V_s) \times (t_s - t_r - t_{retardo})$$

Ecuación 3 Distancia con ToA y TDoA

Fuente: (Rugeles & Leon, n.d.)

Donde, V_r es la velocidad de propagación de la señal de radio frecuencia, V_s la velocidad de propagación de la señal acústica o ultrasónica, t_r el tiempo que tarda la señal de radio, t_s = tiempo de la señal acústica o ultrasónica y $t_{retardo}$ = tiempo fijo de espera. Los errores en la medida utilizando TDoA son del orden de los centímetros. La desventaja de esta técnica radica en la necesidad de un hardware adicional y en el poco alcance debido a la baja velocidad de propagación del sonido de este modelo en particular. Se tienen referencias de implementaciones con señales ultrasónicas con errores de 3 cm en áreas de 3 metros.(Rugeles & Leon, n.d.)

4.2.3 TECNICAS BASADAS EN ÁNGULOS

4.2.3.1 Ángulo de Llegada (AOA)

Mediante AoA como menciona (Barbara, 2012), la localización del objetivo deseado puede encontrarse por la intersección de las líneas que se prolongan desde sus ángulos, cada uno de ellos formado por el radio circular desde la entidad emisora hasta el objetivo móvil. Estos métodos necesitan usar al menos dos puntos de referencia conocidos y dos ángulos medidos para deducir la localización en 2 dimensiones del objetivo (García et al., 2016).

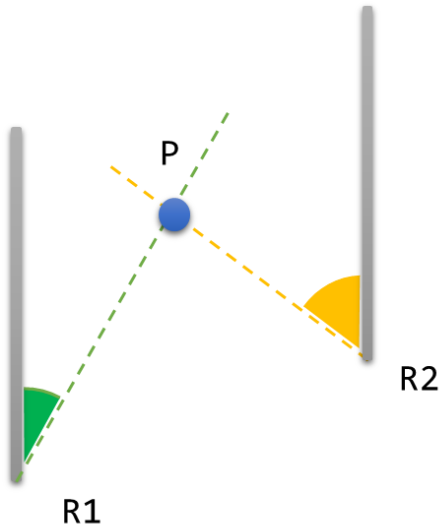


Imagen 5 Ángulo de Llegada

Fuente: Elaboración propia

También conocido como dirección de llegada. Con mínimo dos medidas angulares se puede determinar la posición aproximada de la fuente, como se observa en la imagen 4. Este método necesita de un grupo de antenas directivas o un conjunto de receptores, separados uniformemente (Barbara, 2012). Dependiendo del tipo de arreglo de antenas el desempeño de la técnica puede verse significativamente afectado.

En este método medimos el ángulo entre la línea del transmisor-receptor y la dirección de referencia. Para ello debemos utilizar una antena anisotrópica.

En realidad, las mediciones de AoA utilizan la respuesta de amplitud o fase de la antena y esto representa un problema y es la variación de intensidad de señal, ya que requiere una segunda antena isotrópica no giratoria para normalizar la intensidad de la señal. Por este motivo es necesario usar un mínimo de dos (generalmente al menos cuatro) antenas estacionarias con patrones conocidos de antenas anisotrópicas (Mazurek, 2011).

En términos generales AoA presenta limitaciones de las mediciones en:

- Directividad de la antena: la medida depende en gran medida de la resolución angular de la antena.
- Sombreado: los transmisores y receptores deben estar en línea de visión.
- Reflexiones de trayectoria múltiple.

4.2.4 ARQUITECTURA DEL SISTEMA DE RADIOLOCALIZACIÓN HIBRIDO

El sistema propuesto está diseñado en una topología de red en estrella a través de conexiones punto a punto donde de manera centralizada la información es procesada en el Centro de Fusión (FC) como se muestra en la Imagen 6.

El FC para este proyecto estará implementado bajo una arquitectura Linux de 64 bits, adicionalmente el core de aplicaciones para su funcionamiento será implementado en un servidor web (Apache).

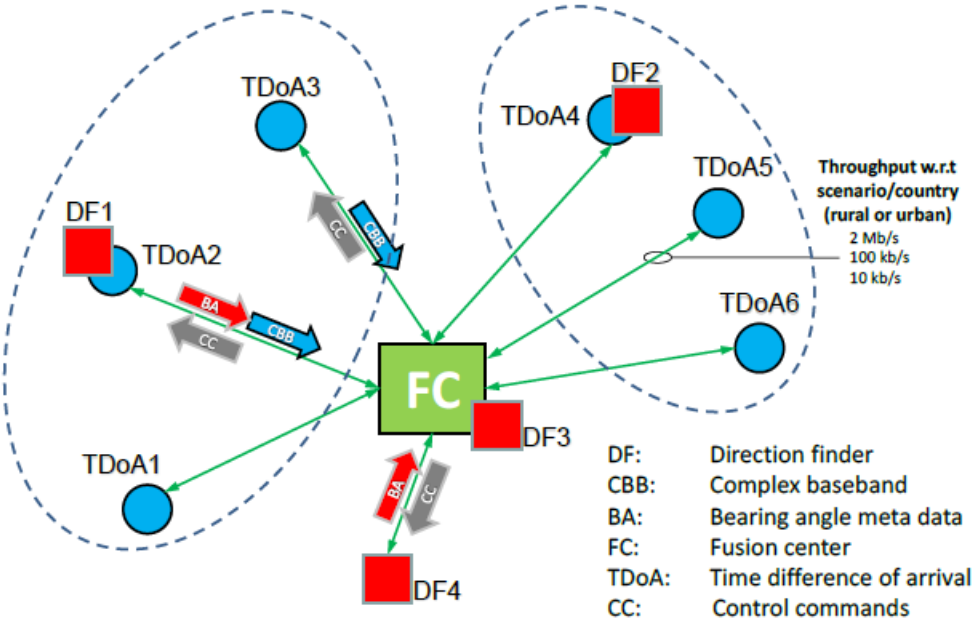


Imagen 6 Arquitectura del Sistema de Radiolocalización Hibrido

Fuente: (Proposal & Engineering, 2015)

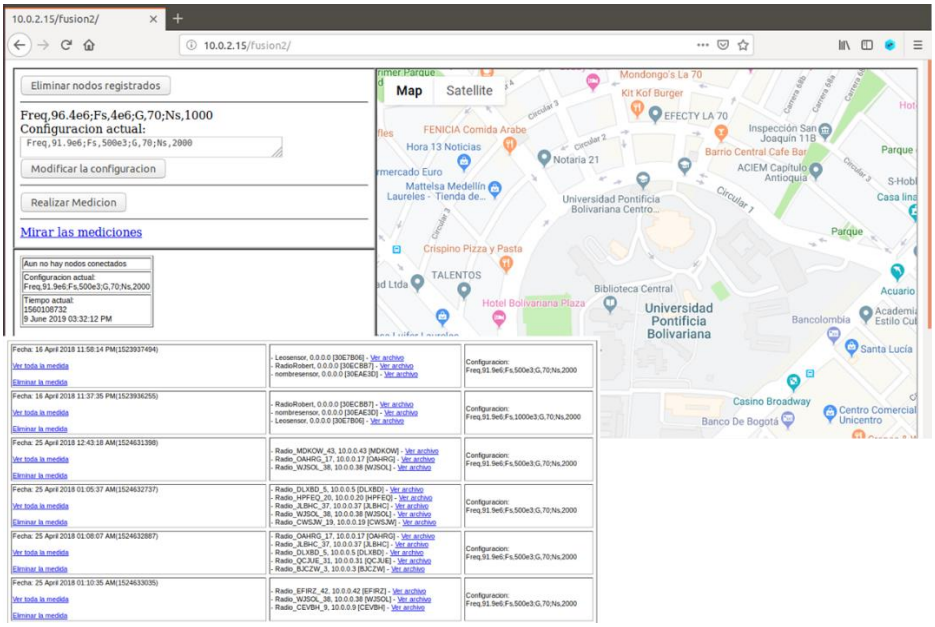


Imagen 7 Centro de Fusion (Servidor Apache)

Fuente: Elaboración propia

4.2.5 SEGURIDAD EN REDES DE SENSORES INALAMBRICOS

Como ha ocurrido con muchas tecnologías existentes, el desarrollo de las redes de sensores nace de la necesidad en aplicaciones militares.

Para entender las ventajas y desventajas en redes inalámbricas de sensores de hoy en día, es útil examinar brevemente su historia. Al igual que muchas tecnologías avanzadas, el origen de las WSN se puede ver en aplicaciones militares e industriales pesadas, muy alejadas de las aplicaciones de WSN industriales ligeras e industriales que prevalecen en la actualidad. La primera red inalámbrica que se parecía mucho a una WSN moderna es el Sistema de Vigilancia de Sonido (SOSUS), desarrollado por el Ejército de los Estados Unidos en la década de 1950 para detectar y rastrear submarinos soviéticos.

Esta red utilizó sensores acústicos sumergidos (hidrófonos) distribuidos en los océanos Atlántico y Pacífico. Esta tecnología de detección todavía está en servicio hoy en día, aunque cumple funciones más pacíficas de monitoreo de la actividad submarina de vida silvestre y volcánica.

Haciendo eco de las inversiones realizadas en los años 60 y 70 para desarrollar el hardware para la Internet de hoy, la Agencia de Proyectos de Investigación Avanzada de la Defensa de los Estados Unidos (DARPA) inició el programa de Red de sensores distribuidos (DSN) en 1980 para explorar formalmente los desafíos en la implementación de sensores distribuidos / inalámbricos. redes Con el nacimiento de DSN y su progresión hacia la academia a través de universidades asociadas como la Universidad Carnegie Mellon y los Laboratorios Lincoln del Instituto de Tecnología de Massachusetts, la tecnología WSN pronto encontró un hogar en la academia y en la investigación científica civil (Zou, Zhu, Wang, & Hanzo, 2016).

Aunque los primeros investigadores en redes de sensores tenían en mente redes compuestas por un gran número de pequeños sensores, la tecnología para aquel entonces todavía no estaba suficientemente desarrollada ya que aún no se satisfacían algunos requisitos de gran importancia en este tipo de redes tales como la autonomía y el tamaño.

Como menciona (García Arano, 2010, p. 4) en su tesis:

> “El desarrollo de las redes de sensores requiere tecnologías de tres áreas de investigación diferentes: detección, comunicación, y computación (incluyendo hardware, software y algoritmia).

Los nodos sensores se encuentran normalmente esparcidos en un campo sensor (Ver Imagen 8). Cada uno de estos nodos sensores esparcidos por la red tiene capacidad tanto para recolectar datos, como para enrutarlos hacia el nodo recolector (sink node) mediante una arquitectura ad hoc de múltiples saltos. El nodo recolector puede comunicarse con el nodo administrador (gestor de tareas) vía Internet, vía satélite o de forma directa."

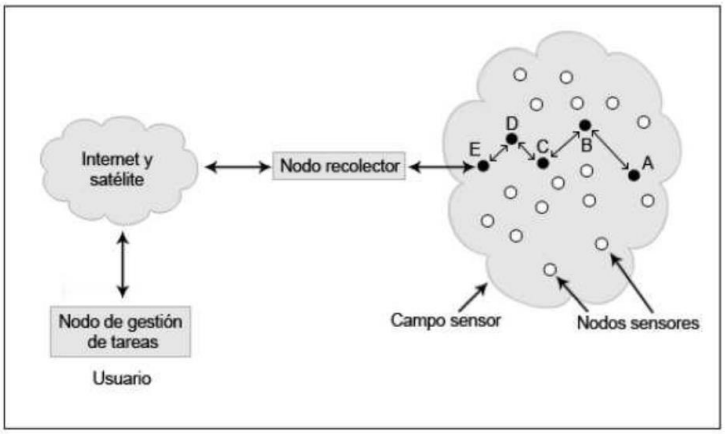


Imagen 8 Nodos de sensores

Fuente: (García Arano, 2010)

El diseño de una red de sensores está altamente influenciado por diferentes factores restrictivos; una red de sensores inalámbricos es una red especial que tiene muchas limitaciones en comparación con una red de computadoras tradicional. Debido a estas restricciones, es difícil emplear directamente los enfoques de seguridad existentes en el área de redes de sensores inalámbricos. Por lo tanto, para desarrollar mecanismos de seguridad útiles mientras se toman prestadas las ideas de las técnicas de seguridad actuales, es necesario conocer y comprender estas limitaciones.

4.2.6 PROBLEMAS DE SEGURIDAD EN REDES DE SENSORES

4.2.6.1 Recursos muy limitados

Todos los enfoques de seguridad requieren una cierta cantidad de recursos para su implementación, incluida la memoria de datos y espacio de almacenamiento, la energía para alimentar el sensor. Sin embargo, actualmente estos recursos son muy limitados en un sensor inalámbrico.

- **Limitación de potencia:** La energía es la mayor restricción para las capacidades de los sensores inalámbricos. Una vez que los nodos sensores se despliegan en una red de WSN, no pueden ser reemplazados fácilmente (alto costo de operación) o recargados (alto costo de sensores). Por lo tanto, la carga de la batería llevada con ellos al campo debe conservarse para prolongar la vida útil del nodo sensor individual y de toda la red de sensores. (Akyildiz, Su, Sankarasubramaniam, & Cayirci, 2002). Al implementar una función o protocolo criptográfico dentro de un nodo sensor, se debe considerar el impacto energético del código de seguridad agregado. Al agregar seguridad a un nodo sensor, estamos interesados en el impacto que la seguridad tiene en la vida útil de un sensor (es decir, la duración de la batería). La energía adicional consumida por los nodos sensores debido a la seguridad está relacionada con el procesamiento requerido para las funciones de seguridad (por ejemplo, cifrado, descifrado, firma de datos, verificación de firmas), la energía requerida para transmitir los datos relacionados con la seguridad o la sobrecarga (por ejemplo, los vectores de inicialización necesarios). para el cifrado / descifrado), y la energía requerida para almacenar los parámetros de seguridad de manera segura (por ejemplo, almacenamiento de claves criptográficas).

- **Memoria y espacio de almacenamiento limitado:** Un sensor es un dispositivo pequeño con solo una pequeña cantidad de memoria y espacio de almacenamiento para el código. Para construir un mecanismo de seguridad efectivo, es necesario limitar el tamaño del código del algoritmo de seguridad.

4.2.6.2 Comunicación no confiable

Indiscutiblemente, la comunicación no confiable es otra amenaza para la seguridad de los sensores. La seguridad de la red se basa en gran medida en un protocolo definido, que a su vez depende de la comunicación.

- **Transferencia no confiable:** Normalmente, el enrutamiento basado en paquetes de red de sensores no tiene conexión y, por lo tanto, es intrínsecamente no confiable. Los paquetes pueden dañarse debido a errores de canal o caerse por nodos altamente congestionados. (Walters, Liang, Shi, & Chaudhary, 2006). El resultado es la pérdida o falta de paquetes. Además, el canal de comunicación inalámbrica no confiable también resulta por paquetes dañados. Una mayor tasa de error del canal también obliga al desarrollador de software a dedicar recursos al manejo de errores. Más importante aún, si el protocolo carece del control de errores adecuado, es posible perder paquetes de seguridad críticos. Esto puede incluir, por ejemplo, una clave criptográfica.

- **Latencia:** El enrutamiento de múltiples saltos, la congestión de la red y el procesamiento del nodo pueden llevar a una mayor latencia en la red, lo que dificulta la sincronización entre los nodos de los sensores. Los problemas de sincronización pueden ser críticos para la seguridad del sensor, donde el mecanismo de seguridad se basa en informes de eventos críticos y en la distribución de claves criptográficas.

- **Conflictos:** Incluso si el canal es confiable, la comunicación puede ser poco confiable. Esto se debe a la naturaleza de transmisión de la red de sensores inalámbricos. Si los paquetes se encuentran o chocan en medio de la transferencia, se producirán conflictos y la transferencia en sí fallará.

4.2.6.3 Operación desatendida

Dependiendo de la función de la red de sensores en particular, los nodos de sensores se pueden dejar desatendidos por largos períodos de tiempo. Hay tres advertencias principales para los nodos de sensores desatendidos:

- **Gestión central desatendida:** Una red de sensores debe ser una red distribuida sin un punto de administración central. Esto aumentará la vitalidad de la red de sensores. Sin embargo, si se diseña incorrectamente, hará que la organización de la red sea difícil, ineficiente y frágil.

- **Exposición a ataques físicos:** El sensor puede ser desplegado en un entorno abierto a adversarios, el mal tiempo, etc. La probabilidad de que

un sensor sufra un ataque físico en un entorno de este tipo es, por lo tanto, mucho más alta que las PC típicas, que se encuentran en un lugar seguro y se enfrentan principalmente a ataques desde una red.

- **Gestión de forma remota:** La administración remota de una red de sensores hace que sea prácticamente imposible detectar la manipulación física (es decir, a través de sellos a prueba de manipulación indebida) y los problemas de mantenimiento físico (por ejemplo, el reemplazo de la batería). Quizás el ejemplo más extremo de esto sea un nodo sensor utilizado para misiones de reconocimiento remoto detrás de las líneas enemigas. (He, Yang, Zhang, Liu, & Liu, 2018). En tal caso, el nodo puede no tener ningún contacto físico con fuerzas amigas una vez desplegado.

- **Hardware de un sensor**: Un nodo sensor está constituido por cuatro componentes básicos, como muestra la Imagen 9 Estructura de un sensor: una unidad sensora, una unidad de proceso, una unidad transceptora, y una unidad de energía, aunque pueden tener también componentes adicionales dependiendo de su aplicación como un sistema de localización, un generador de energía o un movilizador.

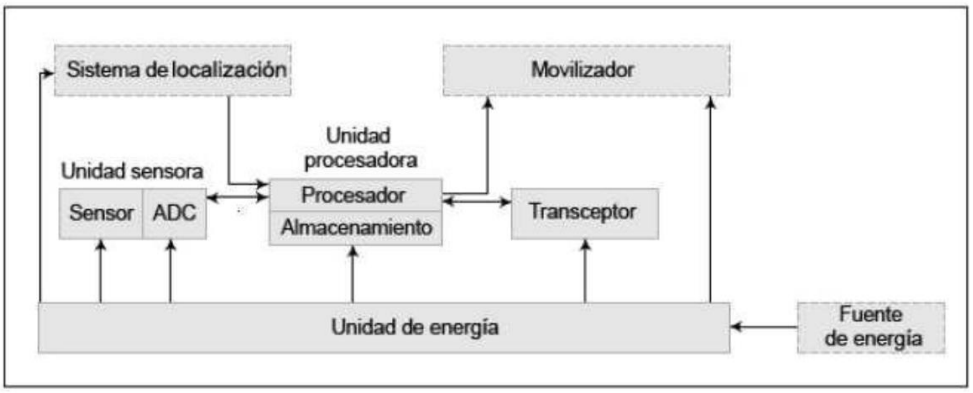


Imagen 9 Estructura de un sensor

Fuente: (García Arano, 2010)

4.2.7 PROBLEMAS DE SEGURIDAD EN CENTRO DE FUSION

4.2.7.1 LINUX HARDENING

El primer paso para fortalecer un servidor GNU / Linux es determinar la función del servidor y los servicios que deben instalarse en él. Por ejemplo, para este caso el servidor en cuestión (Centro de Fusion) se usa como un servidor web, debe instalar los servicios de Linux, Apache, MySQL y Perl / PHP / Python (LAMP). Nada adicional debe instalarse por dos razones:

a) Instalar software adicional o ejecutar servicios adicionales crea vulnerabilidades innecesarias. Por ejemplo, si ejecuta el Protocolo ligero de acceso a directorios (LDAP) en un servidor para servicios de directorio, tanto el sistema operativo como LDAP deben estar actualizados con revisiones y parches de seguridad. Si LAMP (o cualquier otro software) estuviera instalado en este servidor, también requeriría actualizaciones y atención, incluso si no se utilizara. Su sola existencia en el servidor le da al atacante otra vía de acceso al sistema.

b) Instalar software adicional en un servidor significa que alguien tendrá la tentación de usar ese servidor para algo que no sea su uso previsto. El uso del servidor para tareas distintas de su tarea principal desvía recursos de su trabajo principal y lo expone a amenazas potenciales.

4.2.7.2 APACHE WEB SERVER

Apache Foundation lanzó la versión 2 de Apache en 2002, después del éxito de la versión 1 del servidor web Apache. La versión 2 fue casi una reescritura total centrada principalmente, en una mayor modularización y desarrollo del núcleo de Apache. Apache Versión 2 tiene varias mejoras, que incluyen subprocesos de Unix, soporte de IP versión 6 y lo más importante de todo, un mejor soporte para plataformas que no son de Unix, como Microsoft Windows. Estas mejoras ayudaron a que el servidor web Apache se convirtiera en el primer servidor web utilizado para alojar más de 100 millones de sitios web y aplicaciones web en Internet, por lo que es el servidor web más utilizado.(Boulton, 2014).

4.2.7.3 APACHE MODSECURITY MODULE

ModSecurity es un potente filtro de aplicaciones web (WAF), que permite mejorar considerablemente la seguridad del servidor web para detectar y prevenir ataques antes de que lleguen a las aplicaciones web.(Igor Ljubuncic, 2011)

ModSecurity puede realizar una variedad de tareas, incluida la detección de violaciones de los protocolos HTTP, la detección contra ataques web comunes, la detección de bots y rastreadores, la detección de caballos de Troya, el filtrado basado en conjuntos de reglas existentes, políticas o expresiones regulares entre otros. La aplicación se basa en reglas genéricas para detectar y prevenir vulnerabilidades y no se basa en listas negras o firmas.

En realidad, ModSecurity nos provee un alto nivel de confianza. Además, de no afectar el rendimiento del tráfico y lo mejor de todo, ModSecurity es muy fácil de agregar a un servidor Apache existente y en ejecución. Podríamos decir que ModSecurity es una herramienta de detección de intrusiones HTTP (Hypertext Transfer Protocol).

4.2.7.4 BREVE HISTORIA DE MODSECURITY

La primera versión se lanzó en noviembre de 2002, pero se necesitaron algunos meses más antes de que la herramienta fuera útil. Desde muchas partes personas comenzaron a aprender sobre ModSecurity, y la popularidad comenzó a aumentar.

Inicialmente, para muchos la mayor parte del esfuerzo se gastó luchando con Apache para hacer posible la solicitud de inspección de cuerpo. Apache 1.3.x no tenía ninguna API (Interfaz de Programación de Aplicaciones) de intercepción o filtrado, pero podía engañarse para que se enviara la solicitud. Apache 2.x mejoró las cosas al proporcionar API que permiten la introducción de contenido, pero no había documentación en su momento.

En el verano de 2006, ModSecurity se enfrentó con otros firewalls de aplicaciones web, en una evaluación realizada por Forrester Research, y resultó muy favorable. Más tarde ese año, mi compañía fue adquirida por Breach Security. Un equipo de uno eventualmente se convirtió en un equipo de muchos: Brian Rectanus vino a trabajar en ModSecurity, Ofer Shezaf

asumió las reglas y Ryan C. Barnett, la administración y educación de la comunidad. ModSecurity 2.0, una reescritura completa, se lanzó a fines de 2006. Al mismo tiempo, llegó ModSecurity Community Console, que combinaba la funcionalidad de un sensor de registro remoto y una GUI (Interfaz Gráfica de Usuario) de monitoreo e informes(Trustwave, 2016).

En el 2007, Nick Kew presentó su libro The Apache Modules Book (Prentice Hall), que de una forma experimental y practica permite llevar a cabo el desarrollo de ModSecurity.

4.2.7.5 ¿QUÉ PUEDE HACER MODSECURITY?

ModSecurity es un kit de herramientas para el monitoreo, registro y control de acceso de aplicaciones web en tiempo real. Actúa como un habilitador: no hay reglas estrictas que le digan qué hacer; en su lugar, depende de usted elegir su propio camino a través de las funciones disponibles. Es por eso que el título de esta sección pregunta qué puede hacer ModSecurity, no qué hace (Igor Ljubuncic, 2011).

La libertad de elegir qué hacer es una parte esencial de la identidad de ModSecurity y va muy bien con su naturaleza de código abierto. Con acceso completo al código fuente, su libertad de elección se extiende a la capacidad de personalizar y extender la herramienta para que se ajuste a sus necesidades.

Volviendo al tema de lo que puede hacer ModSecurity, la siguiente es una lista de los escenarios de uso más importantes:

a) **Monitoreo de seguridad y control de acceso en tiempo real**

   En su núcleo, ModSecurity le da acceso al flujo de tráfico HTTP, en tiempo real, junto con la capacidad de inspeccionarlo. Esto es suficiente para el monitoreo de seguridad en tiempo real. Existe una dimensión adicional de lo que es posible a través del mecanismo de almacenamiento persistente de ModSecurity, que le permite realizar un seguimiento de los elementos del sistema a lo largo del tiempo y realizar la correlación de eventos. Puede bloquear de forma confiable, si así lo desea, porque ModSecurity usa el búfer completo de respuesta y solicitud.

b) Parches virtuales

La aplicación de parches virtuales es un concepto de mitigación de vulnerabilidades en una capa separada, donde puede solucionar problemas en las aplicaciones sin tener que tocarlas. La aplicación de parches virtuales es aplicable a las aplicaciones que usan cualquier protocolo de comunicación, pero es particularmente útil con HTTP, ya que el tráfico generalmente puede ser bien entendido por un dispositivo intermediario. ModSecurity se destaca en la aplicación de parches virtuales debido a sus capacidades de bloqueo confiables y al lenguaje de reglas flexible que puede adaptarse a cualquier necesidad. Es, de lejos, la actividad que requiere la menor inversión es la actividad más fácil de realizar y la que la mayoría de las organizaciones pueden beneficiarse de inmediato.

c) Registro de tráfico HTTP completo

Los servidores web tradicionalmente hacen muy poco cuando se trata de registrar por motivos de seguridad. Registran muy poco de forma predeterminada, e incluso con muchos ajustes, no puede obtener todo lo que necesita. Todavía tengo que encontrar un servidor web que pueda registrar datos completos de transacciones. ModSecurity le brinda la capacidad de registrar cualquier cosa que necesite, incluidos los datos de transacciones sin procesar, lo que es esencial para el análisis forense. Además, puede elegir qué transacciones se registran, qué partes de una transacción se registran y qué partes se desinfectan.

d) Evaluación de seguridad pasiva continua.

La evaluación de la seguridad se considera en gran parte como un evento activo programado, en el que un equipo independiente se solicita para intentar realizar un ataque simulado. La evaluación de seguridad pasiva continua es una variación del monitoreo en tiempo real, donde, en lugar de centrarse en el comportamiento de las partes externas, se enfoca en el comportamiento del sistema en sí. Es un sistema de alerta temprana que puede detectar rastros de muchas anomalías y debilidades de seguridad antes de que sean explotadas.

e) Endurecimiento de aplicaciones web

Uno de mis usos favoritos de ModSecurity es la reducción de la superficie de ataque, en la cual se restringe las características HTTP que está dispuesto a aceptar (por ejemplo, métodos de solicitud, encabezados de solicitud, tipos de contenido, etc.). ModSecurity puede ayudar a hacer cumplir muchas restricciones similares, ya sea directamente o mediante la colaboración con otros módulos de Apache. Todos caen bajo endurecimiento de aplicaciones web. Por ejemplo, es posible solucionar muchos problemas de administración de sesión, así como vulnerabilidades de falsificación de solicitudes entre sitios.

4.2.8 SEGURIDAD INFORMÁTICA

Con el paso del tiempo la seguridad informática ha ido adquiriendo mayor relevancia debido al crecimiento tecnológico y las amenazas de los sistemas de información a los que son expuestos.

En la dinámica actual grandes cantidades de información viajan a través de las redes de comunicación con información relevante para las empresas y gobiernos, lo que se traduce en la necesidad de garantizar que la información sea genuina y segura, para ello nos apoyamos en varios de los principios de seguridad de la información.

4.2.8.1 INTEGRIDAD

Con la implementación de la confidencialidad, un adversario puede ser incapaz de robar información. Sin embargo, esto no significa que los datos estén seguros. El adversario puede cambiar los datos para desorganizar la red del sensor. Por ejemplo, un nodo malicioso puede agregar algunos fragmentos o manipular los datos dentro de un paquete. (Ver Imagen 10). Este nuevo paquete puede ser enviado al receptor original. La pérdida o daño de los datos puede ocurrir incluso sin la presencia de un nodo malicioso debido al entorno de comunicación hostil. Por lo tanto, la integridad de los datos garantiza que los datos recibidos no se hayan alterado en el tránsito.

La integridad exige que los elementos de un sistema informático puedan ser modificados sólo por aquellas personas o sistemas autorizados.(García Arano, 2010). La modificación incluye escritura, cambio, cambio de estado, borrado y creación.

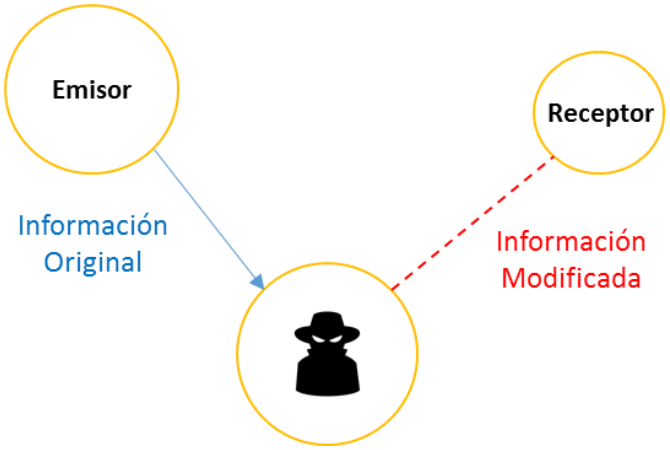


Imagen 10 Esquema de integridad

Fuente: Elaboración propia

4.2.8.2 CONFIDENCIALIDAD

La confidencialidad exige que la información de un sistema sea accesible para lectura solamente a aquellas personas o sistemas autorizados. (García Arano, 2010). Dicha confidencialidad de los datos es el tema más importante en la seguridad de la red. Por lo general, cada red con un enfoque de seguridad abordará este problema primero. (Walters et al., 2006). En redes de sensores, la confidencialidad se refiere a las siguientes restricciones y/o enfoques:

- Una red de sensores no debe filtrar las lecturas del sensor a sus vecinos. Especialmente en una aplicación militar, los datos almacenados en el nodo sensor pueden ser altamente sensibles.
- En muchas aplicaciones, los nodos comunican datos altamente confidenciales, por ejemplo, distribución de claves, por lo que es extremadamente importante construir un canal seguro en una red de sensores inalámbricos.
- La información pública del sensor, como las identidades del sensor y las claves públicas, también se debe cifrar en cierta medida para proteger contra los ataques de análisis de tráfico.
- El enfoque estándar para mantener secretos los datos confidenciales es cifrar los datos con una clave secreta que solo poseen los receptores previstos, logrando así la confidencialidad.

La amenaza a la confidencialidad se encuentra en la intercepción de la comunicación por un agente no autorizado, ilustrado en la imagen 11.

La probabilidad de esto ocurra dependerá del medio físico de la comunicación, o de los elementos intermedios ubicados entre los dos extremos de la comunicación.(Kavitha & Sridharan, 2010).

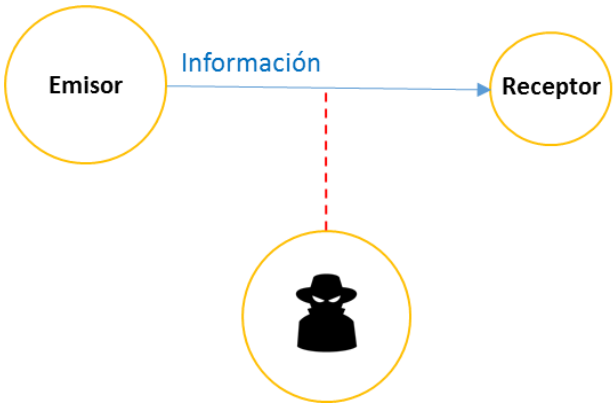


Imagen 11 Esquema de confidencialidad

Fuente: Elaboración propia

4.2.8.3 DISPONIBILIDAD

La disponibilidad se refiere a la continuidad del servicio de los elementos de un sistema informático y que este sea accesible en el momento que un usuario y/o sistema autorizado lo requiera.

La amenaza a este principio se encuentra en la interrupción de las comunicaciones, ya sea interviniendo sobre el medio, sobre los interlocutores o sobre los elementos intermedios involucrados en la comunicación, como ilustra la imagen 12.

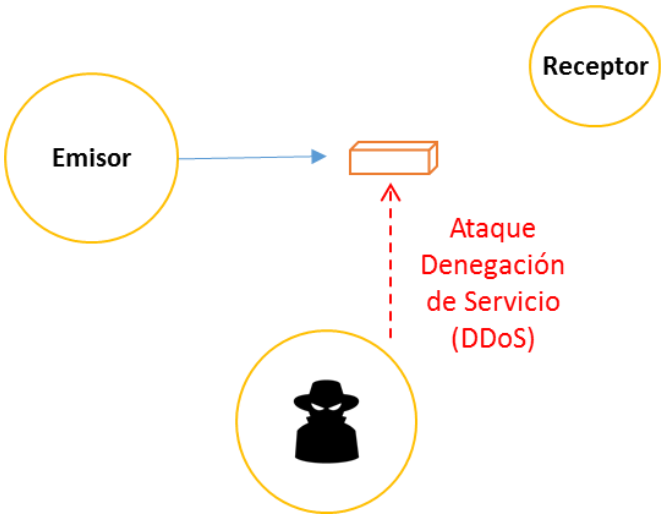


Imagen 12 Esquema de disponibilidad

Fuente: Elaboración propia

4.3 MARCO LEGAL

El marco normativo para este documento está fundamentado en la Ley Colombiana.

LEY/NORMA	TITULO	RESUMEN
DECRETO 195 DE 2005	Por el cual se adopta límites de exposición de las personas a campos electromagnéticos, se adecuan procedimientos para la instalación de estaciones radioeléctricas y se dictan otras disposiciones.(Comunicaciones, 2005)	*Ámbito de aplicación.* Las obligaciones establecidas en el presente decreto, se aplicarán a quienes presten servicios y/o actividades de telecomunicaciones en la gama de frecuencias de 9 KHz a 300 GHz, en el territorio de la República de Colombia, sin perjuicio a lo establecido en el artículo 76 de la Constitución Política. *Definiciones y acrónimos.* Reglamentado por la Resolución del Min. Comunicaciones 1645 de 2005. Para efectos del presente decreto y teniendo bases en las definiciones adoptadas internacionalmente por la Unión Internacional en Telecomunicaciones, UIT.(ITU, 2000) *Límites máximos de exposición.* Quienes presten servicios y/o actividades de telecomunicaciones deben asegurar que en las distintas zonas de exposición a campos electromagnéticos,

		el nivel de emisión de sus estaciones no exceda el límite máximo de exposición correspondiente a su frecuencia de operación, según los valores establecidos en la Tabla 1, correspondientes al cuadro I.2/K.52 de la Recomendación UIT-T K.52 "Orientación sobre el cumplimiento de los límites de exposición de las personas a los campos electromagnéticos".
LEY 1273 DE 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.	Dicha ley tipifica delitos relacionados con el manejo de datos personales obligando a las empresas y personas a cuidar el tratamiento de dicha información a través de los diferentes canales tecnológicos en los que pueda ser vulnerada.(Un & Preservan, 2009)
LEY 1341 DE 2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-,	Determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el

	se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.	régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.(La, Nacional, Se, & Otras, 2009)

Tabla 1 Marco Legal

Fuente: Elaboración propia

4.4 ESTADO DEL ARTE

Con el auge de los servicios móviles y las comunicaciones inalámbricas, el sector científico y productivo ha logrado grandes avances tecnológicos que hacen viables importantes modelos e implementaciones soportadas en las comunicaciones, la electrónica y la informática. Este es el caso de las aplicaciones y/o sistemas que surgen para el sensado de dispositivos para la estimación de su radiolocalización.

La seguridad informática, es el área que se enfoca de la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo sistemas de información). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a los que está expuesta. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de personas no autorizadas. Este tipo de información se conoce como información privilegiada o confidencial.

El traslado de la actividad socioeconómica a Internet ha generado un aumento de las amenazas y, por tanto, de la importancia de la ciberseguridad. Para el caso de las redes inalámbricas y en particular los nodos de sensores inalámbricos pese a su gran evolución están limitados en sus habilidades de energía y computación.

Hay tres elementos principales que en la seguridad de la información deben garantizarse: la confidencialidad, la integridad y la disponibilidad. Las técnicas tradicionales para estos tres principios no pueden utilizarse fuera de la plataforma debido a que las redes de sensores inalámbricas tienen características estrictas y distintivas. En primer lugar, los nodos de sensores suelen estar desplegados en ambientes a los que los atacantes pueden acceder fácilmente. Los nodos sensores no suelen ser inviolables, debido a limitaciones de hardware y costos. Por lo tanto, los atacantes pueden alcanzarlos, extraer las llaves almacenadas e insertar código malicioso. Como menciona (Contreras Javier & Mayol Reinaldo, 2016) proporcionar condiciones de confiabilidad durante el procesamiento y transmisión de datos sobre las WSN (Wireless Sensor Network) presenta aún un importante reto debido a sus características de limitados recursos de computación, ancho de banda y energía, largos periodos de operación ininterrumpidos, despliegue en zonas

de difícil acceso, heterogeneidad, entre otras.

El despliegue de redes de sensores inalámbricos (WSN) es una solución realista para muchos mercados, como la fabricación y el monitoreo del entorno, el de infraestructura militar y crítica y, más recientemente, en sectores de eficiencia energética y salud (Bravo, Palomar, Gardel, & Lázaro, 2017), debido a sus grandes capacidades para adquirir y transmitir datos y procesarlos para diferentes propósitos. Los diseños y arquitecturas actuales utilizan canales de radio para compartir información entre nodos y una puerta de enlace / concentrador, e implementan sensores integrados con batería autónoma o microprocesadores de baja potencia. Las plataformas estándar, como Telos B, y los sistemas operativos, como TinyOS o Contiki, son utilizados por la mayoría de los interesados.

La seguridad, la topología de red y el protocolo de comunicación son cuestiones críticas en la implementación actual de las aplicaciones WSN. Diferentes estrategias deben desarrollarse de acuerdo con los requisitos de la aplicación, tales como la distancia, número de transmisiones durante un período de tiempo, las necesidades de autenticación, y la velocidad de la banda de frecuencia, por mencionar unos pocos.

La colocación del sensor es una tarea importante en aplicaciones basadas en redes de sensores, ya que la cantidad de sensores y su ubicación afectan la precisión y el costo de todo el sistema (Azzedine Boukerche, 2009). Entre los métodos disponibles para estimar la posición de un objetivo, los sistemas de localización basados en rangos usan nodos de anclaje y mediciones que se pueden convertir en distancias o diferencias de distancia; ej., hora de llegada (ToA), diferencia de tiempo de llegada (TDoA), intensidad de señal recibida (RSS), etc. Una vez que se ha obtenido la información sobre las distancias entre el objetivo y los nodos de anclaje, se puede usar trilateración o multilateración para estimar la posición del objetivo (considerando que el objetivo es un emisor y los anclajes son sensores). Por lo tanto, es muy importante que la colocación de sensores; en una situación realista, es necesario colocar sensores para cubrir toda el área, o no, a fin de obtener la mejor precisión en ciertas áreas. Colocar sensores debería minimizar el límite de error de posición, que es una medida ampliamente utilizada.

Como menciona (Bravo et al., 2017) sobre la investigación realizada del estado del arte de la ubicación del sensor para la localización, dice *"Los autores han llegado a la necesidad de recurrir a métodos heurísticos al implementar sensores en un escenario complejo, considerando funciones complejas para el modelo de error de medición o centrándose en una región de interés (ROI) en lugar de un solo objetivo".* En un trabajo continuo, se aplica una optimización evolutiva multiobjetivo para obtener la ubicación óptima del sensor. Inspirado por trabajos en la literatura, el conocido algoritmo genético de clasificación no dominado (NSGA-II) se ha adaptado para resolver el problema de ubicación del sensor para la localización del objetivo. Dicha investigación es una continuación de trabajos anteriores de los mismos autores, donde utilizaron un algoritmo genético multiobjetivo estándar para colocar sensores después de considerar múltiples criterios: colocar un número fijo de sensores para la localización con mediciones de diferencia de rango; considerando una cantidad variable de sensores, así como también condiciones de ausencia de línea de vista (NLOS); etc. Aplicar el algoritmo considerando una cantidad variable de sensores, sin modificaciones, causa problemas graves. Por lo tanto, los autores han tenido que modificar el NSGA-II original agregando especiación y subpoblaciones en evolución de acuerdo con el tamaño de diferentes conjuntos de sensores. Los resultados obtenidos muestran una mejora considerable con respecto a la norma NSGA-II. A demás como menciona (Bravo et al., 2017), dado que los objetivos en conflicto se han optimizado, los autores obtuvieron un conjunto de soluciones óptimas de Pareto. Esto supone la mayor ventaja de la optimización multiobjetivo, ya que cada solución óptima se ha obtenido cuantificando los valores de esos objetivos. Esta información puede ser utilizada por el administrador de recursos de acuerdo con las necesidades y disponibilidad actuales. Hasta ahora, no hay otros investigadores que aborden el problema de ubicación del sensor para la localización de una manera similar. La mayoría de los trabajos de optimización multiobjetivo a los que se hace referencia en las encuestas se centran en la implementación de sensores para optimizar la cobertura y la administración de energía, y los que se ocupan del seguimiento de objetivos solo abordan el problema de programación del sensor.

La seguridad y la autenticación en WSN se enfrentan a un entorno más desafiante en comparación con las redes tradicionales. Los WSN tienen una naturaleza ad-hoc en la que los nodos pueden entrar o salir dinámicamente de la red, lo que conduce a una topología de red variable (Benenson, Cholewinski, & Freiling, 2007). En consecuencia, no existe una ruta predefinida para la

replicación de datos. Con la ambigüedad de los nodos involucrados, un problema crítico puede ocurrir cuando un intruso malicioso ataca el sistema. Además, la limitación de potencia puede hacer que el nodo se comporte egoístamente para conservar su energía, lo que aumenta el riesgo de que la red no funcione correctamente. Por lo tanto, los aspectos antes mencionados de las WSN hacen que los esquemas de seguridad en WSN sean más desafiantes y vulnerables. Por esta razón, la seguridad en WSN ha ganado un interés creciente. La teoría de juegos es una rama moderna de optimización inteligente que aborda problemas donde las funciones de costos de diferentes entidades son mutuamente dependientes. La teoría de juegos se ha aplicado ampliamente para modelar el comportamiento en una variedad de aplicaciones. Recientemente, con la aparición de sistemas distribuidos y sin infraestructura, la teoría de juegos ha encontrado su camino en los sistemas de comunicación descentralizados.

4.4.1 REQUISITOS DE SEGURIDAD Y MITIGACIÓN DE SUBPROCESOS

Se han propuesto varias técnicas para cumplir con la mitigación de amenazas de seguridad de WSN. La situación de seguridad, que implica una interacción entre el (los) defensor (es) y el atacante (s), se puede asignar directamente a un juego entre jugadores en el que cada jugador se esfuerza por promover su beneficio. Más particularmente, tener la acción del (de los) atacante (s) o del (los) defensor (es), dependiendo de la contra acción de la otra parte, coloca la teoría de juego como un ajuste perfecto para este modelo de seguridad. Según la introducción e interpretación de (Abdalzaher et al., 2016) sobre las diferentes técnicas de juego presentadas en la literatura para abordar la seguridad de WSN. Se presenta una vista general de las propiedades WSN deseadas en términos de cumplimiento de seguridad. Este trabajo analiza enfoques basados en la teoría de juegos para la mitigación de diferentes amenazas a la seguridad WSN de acuerdo con la literatura de última generación sobre el tema, clasificando esos enfoques en dos categorías principales, a saber, juegos cooperativos y juegos no cooperativos, y cada resume las estrategias de defensa involucradas basadas en la teoría de juegos. A continuación, (Abdalzaher et al., 2016) propone una taxonomía de las estrategias de defensa teóricas de los juegos teniendo en cuenta la capa atacada, las características de ataque, las consecuencias de los ataques, el enfoque conveniente del juego de defensa y el tipo de juego. Posteriormente, se introduce un modelo de confianza general basado en los enfoques y

escenarios de la teoría de juegos discutidos para tener en cuenta la variabilidad y las características de los tipos de ataque. En consecuencia, los autores proponen el uso de este modelo para cualquier entorno de red (juego cooperativo / no cooperativo con ataque interno / externo). Además, presentan algunas tendencias futuras aplicables para los investigadores interesados, que muestran la capacidad de enfrentar ataques inteligentes.

4.4.2 SIMULACIÓN DE ATAQUES PARA SEGURIDAD

Una de las claves para la implementación continua de WSN es la posibilidad de utilizar una plataforma incrustada de bajo costo con un amplio soporte entre la comunidad de desarrolladores. Estas plataformas incluyen sensores para recopilar información de diferentes escenarios, y esta información generalmente se envía a un nodo central u otros nodos mediante comunicación inalámbrica (Athanasios, 2011). Sin embargo, la seguridad en este tipo de plataforma es uno de los valores a analizar y mejorar.

4.4.3 CONFIDENCIALIDAD

La protección de los datos y la privacidad, son retos difíciles de cumplir en las redes de sensores, pero que son necesarios para garantizar un grado razonable de confidencialidad. Los nodos de red son fáciles de capturar y comprometer, por lo tanto, las fracciones de activos pueden robarse del sistema sin protección adecuada contra los nodos atacantes. La red de confianza también puede fallar al asegurar la privacidad si la autenticación y el control de acceso no se aplican de manera consistente: las consultas en la red desde diferentes ubicaciones o con diferentes credenciales podrían proporcionar diferentes niveles de acceso sin una administración adecuada. Las WSN son por lo tanto vulnerables a los ataques de Sybil[1], ataques de distanciamiento (nodos enmascarados en algunas localizaciones), y fugas de la localización (Castillejo, Martínez-Ortega, López, & Alcón, 2015).

La confidencialidad requiere mecanismos específicos entre estos, las soluciones de seguridad tradicionales incluyen cifrado y protocolos que garantizan el enmascaramiento de los datos y el procesamiento consistente

[1] En un ataque Sybil, un atacante puede contaminar un sistema distribuido creando un gran número de identidades que aparenten ser independientes y usarlas para obtener una influencia desproporcionada, alterar rutas o modificar contenido almacenado de forma redundante. De esta forma ciertos nodos legítimos pueden sufrir una usurpación de identidad al estar solo conectados a los del atacante. La vulnerabilidad del sistema depende de la facilidad para crear nuevas identidades y la (falta de) importancia de la cadena de confianza, que puede hacer que todas las identidades sean tratadas por igual.

respectivamente. El cifrado suele implementarse en infraestructura clave para asegurar las comunicaciones.

Las claves deben desplegarse en los nodos de red para garantizar la confidencialidad de los datos. Un ataque físico a los nodos podría revelar algunas claves, de modo que la confidencialidad no puede garantizarse localmente al nodo atacado con riesgo potencial de romper epidemiológicamente las protecciones a través de la red. El cifrado es también un proceso costoso computacionalmente como por ejemplo la criptografía asimétrica. En la actualidad diversos equipos de investigación trabajan para controlar y reducir su impacto en los costos; las curvas elípticas parecen ser una excelente opción ya que proporcionan un alto grado de confidencialidad y mitigan el impacto de procesamiento de las WSN.

4.4.4 INTEGRIDAD

La integridad es un problema muy conocido en las redes de comunicaciones alámbricas e inalámbricas. En este sentido las WSN pueden depender de una cantidad significativa de modelos y técnicas con una cantidad de desafíos interesantes debido a sus limitados recursos. A pesar del desarrollo tecnológico con el hardware más reciente, las limitaciones físicas claramente evitan la comparación de las capacidades de WSN con otros dispositivos portátiles más complejos o incluso con los teléfonos móviles de gama baja, ya que los nodos WSN tienden a ser aún más pequeños.

Como menciona (Platon & Sei, 2008), la criptografía es una de las principales técnicas para garantizar la integridad y sigue siendo un reto en lo que respecta a la gestión de la energía y los enfoques descentralizados.

La localización de fuentes de datos plantea problemas agudos de integridad en WSN. Generalmente los forenses y administradores de redes se ven obligados a rastrear los datos de vuelta a sus fuentes en algunas circunstancias (cuando sea posible, debido a la destrucción en la agregación de red). La ubicación de las fuentes requiere que los datos no se alteren cuando migren al nodo principal, de modo que la integridad es una condición necesaria.

4.4.5 DISPONIBILIDAD

La disponibilidad también se convierte en un factor crítico en el sistema de radiolocalización hibrido principalmente en los WSN.

Las razones son dobles y considerablemente restrictivas. En primer lugar, el suministro de energía es limitado comprometiendo en definitiva la disponibilidad de la red. Los grandes sistemas pueden depender de la intervención humana y las soluciones de energía renovable están en muchos lugares en desarrollo, en ese sentido las medidas holísticas que involucran intervenciones de hardware y humanos son requeridas en algunas condiciones.

El compromiso del nodo sigue siendo un problema, ya que la destrucción o pérdida del control de los nodos reduce unilateralmente la disponibilidad del sistema.

En segundo lugar, el modelo de comunicación de radiodifusión de WSN es sensible a diferentes ataques; por ejemplo, los de denegación de servicio, incluyendo de alta energía y ataques de interferencia. Los ataques tradicionales como la caída de mensajes se gestionan con enfoques estándar, como el enrutamiento múltiple del mismo mensaje, pero las limitaciones de recursos disminuyen claramente su viabilidad (Chan & Perrig, 2003).

Los desafíos en WSN siguen siendo numerosos, especialmente en relación con los existentes en materia de seguridad en sistemas distribuidos y móviles. La importancia del enfoque holístico es destacable debido a la exposición directa del sistema a amenazas externas, ambientales y maliciosas.

Una de las dificultades en este tema es encontrar un equilibrio entre la contribución de software, que consume energía, pero que a su vez es potencialmente robusto frente a intrusiones, y el hardware o intervenciones humanas que pueden optimizar la eficiencia energética, incluso llegar a renovarla. La ingeniería de seguridad debe hacer frente a este equilibrio.

Además de las principales propiedades de seguridad, encontramos también temas como la calidad del servicio y la autenticidad. La calidad de servicio amplía la disponibilidad y es un reto también. La autenticidad de los datos se refiere a problemas de mensajes duplicados e inapropiados (intencionales o accidentales) y que convergen en problemas de integridad y disponibilidad.

La autenticación tiene por objeto garantizar la identidad de los actores principales y, por tanto, es una condición previa para la confidencialidad.

4.4.6 SOLUCIONES DE SEGURIDAD EXISTENTES

En esta sección, revisamos algunos trabajos representativos para abordar los desafíos de seguridad mencionados anteriormente. Complementamos esta revisión con la presentación de diferentes técnicas y/o métodos que abordan varios temas de seguridad en un único enfoque. La sección termina con un mapeo de esta revisión sobre el proceso estándar de desarrollo de software similar a una cascada para mostrar el estado actual de la investigación en ingeniería de seguridad.

4.4.6.1 La Criptografía:

Constituye el principal concepto teórico junto con infraestructuras clave; enfoques subyacentes que garantizan la integridad y la confidencialidad. La criptografía de curvas elípticas (ECC) ha sido reconocida como una técnica bastante viable para WSN. (Contreras Javier & Mayol Reinaldo, 2016). ECC está ganando impulso con una importante empresa emitiendo una declaración oficial de adopción de tecnología en 2005, La Agencia de Seguridad Nacional de Estados Unidos añadiendo el enfoque a su Suite oficial B para firmas digitales.

ECC es una alternativa prometedora a los algoritmos basados en RSA, ya que el tamaño típico de las claves ECC es mucho más corto para el mismo nivel de seguridad.

El proyecto SPINS muestra que el costo de seguridad en esencia de la criptografía (entre otros cálculos) se debe más a la sobrecarga de comunicación por paquete que a la demanda computacional. A pesar de este resultado, un trabajo significativo apunta a mejorar la ejecución de algoritmos ECC con soporte de hardware o elaborar nuevos algoritmos para la multiplicación eficiente, ya que es una operación muy común y costosa en la criptografía de clave pública. Otros enfoques también explotan hardware específico para mejorar la confidencialidad, por ejemplo, con chips anti-falsificación que evitan que los ataques revelen claves criptográficas, al costo de aumentar el precio de las unidades de hardware.

4.4.6.2 Infraestructuras Clave:

Las infraestructuras clave llaman la atención de la comunidad investigadora en la actualidad por temas de confidencialidad e integridad. La gestión de claves es crítica en la raíz de las defensas de seguridad del sistema. Las claves en WSN tienen un ciclo de vida que enfatiza las fases de despliegue, protección y revocación. La instalación de infraestructuras clave a menudo se basa en esquemas de pre-distribución. Ghosh demuestra que tales enfoques son válidos si la topología de la red verifica las propiedades estructurales como la ausencia de nodos de cuello de botella en algunas condiciones. La protección de las claves se logra ya sea por hardware específico, como se ha introducido anteriormente, o por protocolos de seguridad que gestionan el ciclo de vida de las claves. Por ejemplo, se recomienda la revocación regular de claves para actualizar la infraestructura y proteger contra las claves robadas.

4.4.6.3 Integridad y procesamiento de red:

Las preocupaciones por la integridad de la información también son objeto de investigación adicional en relación con la seguridad en la técnica de agregación de red. La agregación en red tiene como objetivo procesar los datos de los sensores mientras migran hacia el nodo central, típicamente para calcular promedios o sumas. Es una técnica importante para utilizar la energía del nodo de manera más eficiente en WSN. Varios enfoques de agregación existentes carecen de garantías de seguridad, de tal manera que las investigaciones posteriores y los desastres proponen esquemas seguros.

4.4.6.4 Otros:

Los problemas de localización, el aseguramiento de protocolos junto con la recuperación, se suman a los aspectos actuales en el tratamiento de seguridad sobre WSN proporcionando diferentes mecanismos y/o alternativas que mitigan un posible ataque. Como ejemplo, encontramos que la localización de fuentes de datos confiables es una disyuntiva de verificación en el origen de datos de que sea de una fuente de confianza al igual que la protección de la privacidad. Los protocolos de seguridad proporcionan mecanismos de defensa contra ataques externos por ejemplo DoS a alguno de los nodos.

4.4.7 PREOCUPACIONES DE SEGURIDAD DEL SERVIDOR WEB (CENTRO DE FUSION)

Compartir información y realizar negocios a través de internet se ha convertido en un requisito fundamental para la mayoría de las organizaciones de hoy. Sin embargo, un servidor web que permite a una organización compartir información con el mundo exterior podría potencialmente ser explotado para causar modificación o destrucción no autorizada de información y otros recursos del sistema.

A través de varios ataques, como los ataques de desbordamiento de búfer, un usuario malintencionado podría controlar nuevamente un proceso de un servidor web. Puesto que los servidores web a menudo se ejecutan con privilegios mejorados, el usuario que obtiene el control del proceso del servidor web posee privilegios que pueden ser utilizados para causar daños en el sistema mejorado.

Incluso si un usuario malintencionado no puede controlar el proceso del servidor web, los scripts potencialmente permiten a los usuarios dirigir al servidor web para que realice una acción maliciosa. Un script de Common Gateway Interface[2] (CGI) acepta la entrada del usuario y la envía al servidor para su procesamiento. Por ejemplo, los formularios electrónicos de compra y los libros de visitas del sitio web se implementan normalmente a través de scripts CGI. Desafortunadamente, es posible que un usuario malintencionado

[2] Desarrollado por Apache Software Foundation (http://www.apache.org)

ingrese código ejecutable como entrada en un formulario o libro de visitas. Si el servidor ejecuta ese código, el servidor podría causar daños al sistema.

Otro tipo de script es un Server Side Include (SSI). Un SSI es un archivo que el servidor web puede analizar para proporcionar información dinámica para una página web, como la fecha y la hora actuales. Se pueden incluir comandos de shell ejecutables o una interfaz para scripts CGI en un SSI. Por ejemplo, un SSI podría incluir una declaración como <!--#exec cgi= "runme.cgi"-->. El servidor web ejecutaría runme.cgi cuando analiza el SSI. Si runme.cgi contiene código malicioso, el servidor web podría causar daños al ejecutar el código.(Gosselin & Schommer, n.d.).

4.4.7.1 Enfoques para reducir el riesgo:

Hay varios enfoques que se pueden tomarse para reducir el riesgo asociado con un servidor web.

Uno de los métodos más sencillos para reducir el riesgo es ejecutar el servidor como "nobody".

Esto puede ocurrir cuando se inicia el servidor o cuando el servidor realiza un proceso para manejar una conexión en el puerto 80.

Sin embargo, una vez que el servidor comienza a ejecutarse como "nobody", el administrador del sistema tiene que asegurarse de que el servidor aún tenga acceso a los archivos a los que necesita acceder al configurar los permisos de manera adecuada. Esto puede resultar en otorgar un acceso más amplio a ciertos archivos que el deseado.

Este enfoque tampoco impide el acceso a directorios y archivos legibles / grabados / ejecutables en todo el mundo, de los cuales hay muchos en un sistema típico. Si cualquiera de estos ejecutables se configura correctamente, puede ser posible obtener privilegios de raíz indirectamente.

Como es conocido, los sistemas informáticos como los servidores web, suelen ser vulnerables a los ataques. Para evitar que los ataques tengan éxito, se pueden mitigar las vulnerabilidades conocidas al reducir la funcionalidad de la aplicación o al implementar correcciones o parches dentro del código fuente de la aplicación. La reducción de la funcionalidad a menudo no es aceptable

para los usuarios, y la implementación de correcciones requiere en la mayoría de los casos cooperación del proveedor y, por lo general, es una reacción a los daños que ya se han producido.

Una alternativa es reducir el nivel de riesgo al limitar la aplicación. La definición de una aplicación significa controlar el acceso de la aplicación y los daños maliciosos a los recursos del sistema (por ejemplo, procesos y archivos).

Restringir el acceso de un servidor web a los recursos del sistema limita el daño potencial causado a los recursos a través de la explotación de las vulnerabilidades del servidor web. Sin embargo, permitir que el servidor web acceda a los recursos requeridos permite proporcionar la funcionalidad esperada.

Esta combinación de negar el acceso innecesario y permitir el acceso requerido da como resultado la funcionalidad del servidor web al tiempo que limita los daños.

Para demostrar esto, configuramos el servidor web Apache en Linux con seguridad mejorada, un sistema operativo que impone una política de control de acceso obligatorio. Al adaptar la política de Linux con seguridad mejorada, pudimos controlar la interacción entre el servidor web Apache y otros procesos y archivos en el sistema. La política dicta que Apache solo tiene permitido mostrar páginas web y realizar funciones limitadas que admiten la visualización de páginas web.

4.4.8 APACHE SECURITY - ASEGURANDO EL CENTRO DE FUSION (SERVIDOR WEB APACHE)

Las siguientes sugerencias contribuirán en gran medida a mejorar la seguridad de la instalación de un servidor web Apache. A pesar de aplicar la regla "menos es mejor" para fortalecer un servidor web al deshabilitar una serie de módulos, no será suficiente. Aún se recomienda aplicar todos los parches de seguridad en caso de que un módulo deshabilitado esté habilitado en el futuro (Bowen & Coar, 2008).

4.4.8.1 Limitar la funcionalidad del servidor:

Primero se debe saber para qué función o funciones se utilizará el servidor web. ¿Servirá solo páginas HTML, o también ejecutará una serie de scripts? Habilitar el soporte para PHP, ASP.NET y otras tecnologías web similares solo aumentará la superficie de ataque que un usuario malintencionado podría penetrar. Esto puede suceder debido a vulnerabilidades en un módulo de servidor web específico. Por lo tanto, solo se deben admitir las tecnologías web que se van a utilizar.

4.4.8.2 Limitar el acceso al sistema operativo y sus archivos:

El sistema operativo en el que se ejecutará el servidor web Apache también debe reforzarse. Lea más sobre la seguridad del servidor web (https://www.acunetix.com/websitesecurity/webserver-security/) y sobre cómo proteger un sistema operativo de servidor web. Es importante que el proceso del servidor web Apache se ejecute bajo una ID de usuario única, que no debe ser utilizada por ningún otro proceso del sistema. Los procesos de Apache también deben tener acceso limitado a los archivos del sistema operativo (chrooting). Chrooting es el proceso de crear una nueva estructura de directorio raíz a la que se mueven todos los archivos del daemon de Apache. Como resultado del proceso de chrooting, el daemon del servidor web Apache solo tendrá acceso a la nueva estructura de directorios. No hay programas de shell, por ejemplo. / bin / sh, / bin / csh / debe estar presente en el entorno chroot de Apache. De esta manera, el servidor web se beneficia de la inmunidad de un gran número de explotaciones existentes.

4.4.8.3 Deshabilitar módulos de servidor web innecesarios:

Apache se entrega con una serie de módulos pre-habilitados para que sean más fáciles de usar. Esto es un pequeño descanso de su pasado Unix de solo proporcionar lo esencial. En este caso, la regla de "menos es mejor" se debe aplicar con más diligencia y la elección de qué módulo habilitar es probablemente el paso más importante. Un administrador evitaría posibles robos simplemente deshabilitando módulos innecesarios cuando se encuentren nuevas vulnerabilidades en ellos. Verifique sobre cada módulo pre-habilitado para confirmar si es necesario, y si no, deshabilítelo.

4.4.8.4 Ajustar la configuración de Apache:

La configuración predeterminada de Apache contiene una gran cantidad de directivas que no se utilizan en un escenario típico. Uno puede apagar o deshabilitar con seguridad las directivas enumeradas a continuación si no se utilizan:

- Indices de directorio
- "Alias" y "ScriptAlias" por defecto innecesarios

- Manejadores (solo deje los manejadores que usará. Remueva todos los demás) Opciones de directorio como 'FollowSymLinks' (si no se usan enlaces simbólicos en los directorios web).

- Los mensajes de error del servidor web también deben configurarse para asegurarse de que se divulgue la menor cantidad de información sobre la instalación y configuración del servidor web Apache. Si es posible, el banner del servidor web también debe estar confuso (seguridad por oscuridad).

4.4.8.5 Deshabilitar los lados del servidor incluye:

Los SSI traen consigo una serie de posibles riesgos de seguridad. Lo más importante de todo es que los documentos web habilitados para SSI aumentarán considerablemente la carga en el servidor. En sitios web de alto tráfico o en un entorno de alojamiento web compartido, dicha carga puede ser muy significativa. Además, los lados del servidor incluyen plantean la misma cantidad de riesgos asociados con los scripts CGI (Interfaz de puerta de enlace común) en general. Los archivos habilitados para SSI pueden ejecutar cualquier script o programa CGI con los permisos del usuario en el que se ejecuta el servidor web Apache, lo que representa un gran riesgo para la seguridad. Una serie de tecnologías web que evitan el uso de SSI y transfieren el procesamiento requerido al lado del cliente / navegador están disponibles hoy. Un webmaster debe aprovechar tales tecnologías web.

4.4.8.6 Archivos del monitor de registro:

El acceso adecuado a la aplicación web y el registro del funcionamiento del servidor web deben estar habilitados. Dichos registros no se deben colocar en

el directorio raíz del servidor web. Al igual que con cualquier otro servicio de Internet, es importante revisar regularmente todos los archivos de registro de Apache. El análisis de eventos pasados de los archivos de registro del servidor web le dará al administrador una buena idea de las tendencias de ataque que se están siguiendo. Esto también ayudará al administrador a identificar dónde debe ajustarse el servidor web.

4.4.8.7 Instalar todas las actualizaciones del servidor web Apache:

De vez en cuando, Apache Foundation lanza una serie de parches. Siempre es una buena práctica para su seguridad de Apache mantener actualizada la instalación del servidor web, a pesar de que el parche sea uno de seguridad o una actualización de software. suscríbase a una lista de correo como 'Anuncios de Apache Server' para recibir notificaciones de cuándo hay actualizaciones y parches disponibles. Estas listas de correo son alojadas por la Fundación Apache.

4.4.8.8 Manténgase informado y con frecuencia revise la configuración del servidor web:

Hay varios libros, artículos de pautas de seguridad en línea y documentos técnicos sobre seguridad de Apache, para ayudar a los administradores a asegurar una instalación de servidor web de Apache e implementar las sugerencias de seguridad de Apache anteriores, que sin embargo son universales. Se sugiere leer dichos artículos y seguir las pautas. Después de aplicar dichos cambios, también es importante probar la funcionalidad del servidor web y de la aplicación web, para confirmar que dichos cambios no impiden la funcionalidad de la aplicación web. El uso de herramientas de seguridad de terceros, puede ayudar a confirmar que los procedimientos aplicados mejoraron la seguridad de su servidor web.(Boulton, 2014).

5. METODOLOGÍA

La investigación abarcará la implementación de mínimo 3 tratamientos a vulnerabilidades del centro de fusión . Para esto se tomará como punto de partida el análisis de riesgo realizado el trabajo de maestría "**SEGURIDAD DE LA INFORMACIÓN EN UNA RED DE SENSORES PARA RADIOLOCALIZACIÓN EN APLICACIONES DE VIGILANCIA DEL ESPECTRO ELECTROMAGNÉTICO"** que hace parte de una primera fase del proyecto. Dicho análisis será cruzado con un estado del arte basado en las mejores prácticas para este tipo de implementaciones de seguridad, más exactamente relacionado al aseguramiento (hardening) de servidores web Apache bajo plataforma Linux.

Posteriormente, se llevará a cabo un análisis de vulnerabilidades a través de software especializado que permita identificarlas y clasificarlas para su posterior tratamiento, seleccionando así las más críticas como alcance de este trabajo.

Finalmente se explorará y tratará las configuraciones de seguridad para las vulnerabilidades más importantes encontradas durante el análisis, y de este modo fortalecer la postura de seguridad de una instalación predeterminada del sistema operativo Linux. Este documento no es de ninguna manera una guía de seguridad completa para el sistema operativo Linux; sin embargo, describe el fortalecimiento básico de un sistema Linux, por lo que puede no ser un blanco fácil para los ataques. Muchos administradores de sistemas no se dan cuenta del hecho de que, una instalación predeterminada de Linux es vulnerable a una variedad de ataques. Por lo tanto, este documento presenta la seguridad básica y las mejores prácticas de la industria para proteger el Servidor Linux, así como algunos de los servicios de aplicaciones, más exactamente el servidor web apache.

6. PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

6.1 IDENTIFICACIÓN DE LAS VULNERABILIDADES DEL CENTRO DE FUSIÓN

En esta sección se presentan los resultados orientados al cumplimiento del objetivo específico 1.

Para la identificación de vulnerabilidades del Centro de Fusión hemos utilizado una herramienta estándar de la industria para profesionales de la seguridad (Nessus). Esta herramienta ayuda a identificar y corregir vulnerabilidades con rapidez y facilidad, incluidos fallas de software, parches faltantes, malware y configuraciones erróneas, en una variedad de sistemas operativos, dispositivos y aplicaciones.

Tras configurar el prototipo del sistema en un ambiente simulado a las condiciones y características del sistema en producción, se inicia el análisis de vulnerabilidades arrojando los resultados de la Imagen 13.

6.1.1 ANALISIS DE VULNERABILIDADES

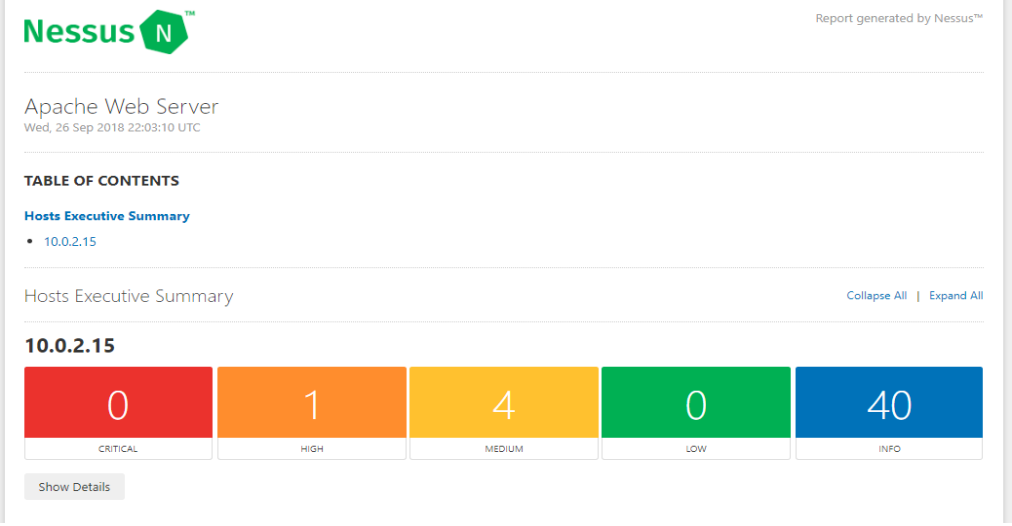


Imagen 13 Reporte de vulnerabilidades detectadas

Fuente: Nessus

Como se observa en la Imagen 13, se obtuvo un total de 0 vulnerabilidades críticas, una vulnerabilidad alta, cuatro medianas y 40 de tipo información.

Para esta simulación analizamos las más representativas (clasificación alta y media) cumpliendo con el objetivo especifico uno.

Severity	CVSS	Plugin	Name
HIGH	N/A	112058	Ubuntu 18.04 LTS : base-files vulnerability (USN-3748-1)
MEDIUM	6.8	108758	Apache 2.4.x < 2.4.33 Multiple Vulnerabilities
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.0	10677	Apache mod_status /server-status Information Disclosure
MEDIUM	5.0	111788	Apache 2.4.x < 2.4.34 Multiple Vulnerabilities

Imagen 14 Vulnerabilidades representativas del informe

Fuente: Nessus

Seguido de la identificación de las vulnerabilidades más importantes (Imagen 14), tomando el alcance fijado en los objetivos de este trabajo, se inicia el proceso de análisis.

6.1.2 VULNERABILIDAD UBUNTU 18.04 LTS: BASE-FILES (USN-3748-1)

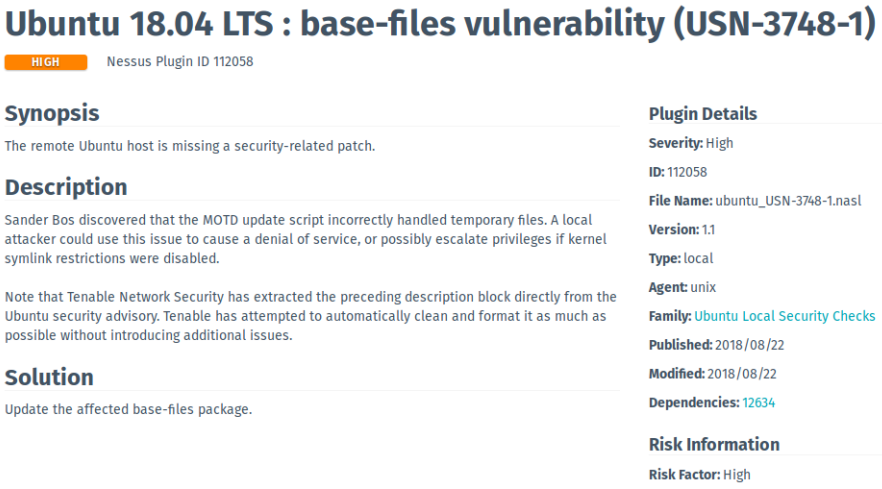
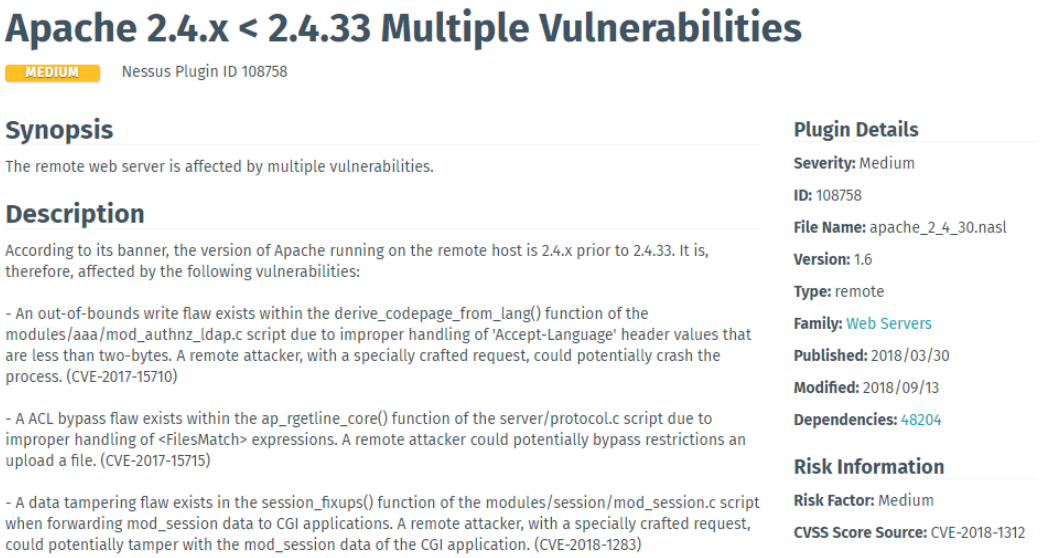


Imagen 15 Reporte Vulnerabilidad USN-3748-1

Fuente: Tenable.com

La vulnerabilidad de la Imagen 15 se refiere a la falta de un parche de actualización crítico del sistema. Dicha vulnerabilidad descubierta por Sander Bos reveló que el script de actualización de MOTD[3] (Message Of The Day) manejaba incorrectamente archivos temporales. Un atacante local podría usar este problema para provocar una denegación de servicio, o posiblemente escalar privilegios si se deshabilitaran las restricciones del enlace simbólico del kernel.(Tenable, 2018)

6.1.3 VULNERABILIDADES APACHE 2.4.X < 2.4.33



Apache 2.4.x < 2.4.33 Multiple Vulnerabilities

MEDIUM Nessus Plugin ID 108758

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.33. It is, therefore, affected by the following vulnerabilities:

- An out-of-bounds write flaw exists within the derive_codepage_from_lang() function of the modules/aaa/mod_authnz_ldap.c script due to improper handling of 'Accept-Language' header values that are less than two-bytes. A remote attacker, with a specially crafted request, could potentially crash the process. (CVE-2017-15710)

- A ACL bypass flaw exists within the ap_rgetline_core() function of the server/protocol.c script due to improper handling of <FilesMatch> expressions. A remote attacker could potentially bypass restrictions an upload a file. (CVE-2017-15715)

- A data tampering flaw exists in the session_fixups() function of the modules/session/mod_session.c script when forwarding mod_session data to CGI applications. A remote attacker, with a specially crafted request, could potentially tamper with the mod_session data of the CGI application. (CVE-2018-1283)

Plugin Details

Severity: Medium

ID: 108758

File Name: apache_2_4_30.nasl

Version: 1.6

Type: remote

Family: Web Servers

Published: 2018/03/30

Modified: 2018/09/13

Dependencies: 48204

Risk Information

Risk Factor: Medium

CVSS Score Source: CVE-2018-1312

Imagen 16 Reporte Vulnerabilidad Apache 2.4.x < 2.4.33

Fuente: Tenable.com

Esta vulnerabilidad (Imagen 16) se refiere a la versión de Apache que se ejecuta en el host remoto es 2.4.x antes de 2.4.33. Es, por lo tanto, afectado por las siguientes vulnerabilidades:

a. Existe una falla de escritura fuera de los límites dentro de la función derive_codepage_from_lang () de los scripts modules / aaa / mod_authnz_ldap.c debido a un manejo incorrecto de los valores de encabezado 'Aceptar-Idioma' que tienen menos de

[3] Esto permite que aparezcan mensajes personalizados cuando los visitantes ingresan a un sitio web o una sección del sitio web, sin la necesidad de modificar ninguna página web o código de aplicación web. La página web a la que se accede en el servidor web redirigirá al visitante al mensaje personalizado momentáneamente.

dos bytes. Un atacante remoto, con una solicitud especialmente diseñada, podría bloquear el proceso. (CVE-2017-15710)

b. Existe una falla de omisión de ACL dentro de la función ap_rgetline_core () del script server / protocol.c debido a un manejo inadecuado de las expresiones <FilesMatch>. Un atacante remoto podría pasar por alto las restricciones y cargar un archivo. (CVE-2017-15715)

c. Existe un defecto de manipulación de datos en la función session_fixups () del script modules / session / mod_session.c cuando se reenvían datos mod_session a aplicaciones CGI. Un atacante remoto, con una solicitud especialmente diseñada, podría manipular los datos de mod_session de la aplicación CGI. (CVE-2018-1283)

d. Existe una falla de lectura fuera de límite cuando se alcanza un límite de tamaño mientras se manejan los encabezados HTTP. Un atacante remoto, con una solicitud especialmente diseñada, podría bloquear el proceso. (CVE-2018-1301)

e. Existe una falla de uso después de liberarse cuando se maneja el cierre de la secuencia HTTP / 2. Un atacante remoto podría escribir en la memoria ya liberada y bloquear el proceso. (CVE-2018-1302)

f. Existe una falla de lectura fuera de los límites en la función read_table () de la secuencia de comandos modules / cache / mod_cache_socache.c cuando se manejan encabezados vacíos. Un atacante remoto, con una solicitud especialmente diseñada, podría bloquear el proceso. (CVE-2018-1303)

g. Existe una falla dentro de la secuencia de comandos modules / aaa / mod_auth_digest.c debido a la generación indebida de nonce cuando se envían desafíos de autenticación HTTP Digest. Un atacante remoto podría potencialmente llevar a cabo ataques de reproducción contra el servidor. (CVE-2018-1312)

6.1.4 VULNERABILIDAD SSL CERTIFICATE CANNOT BE TRUSTED

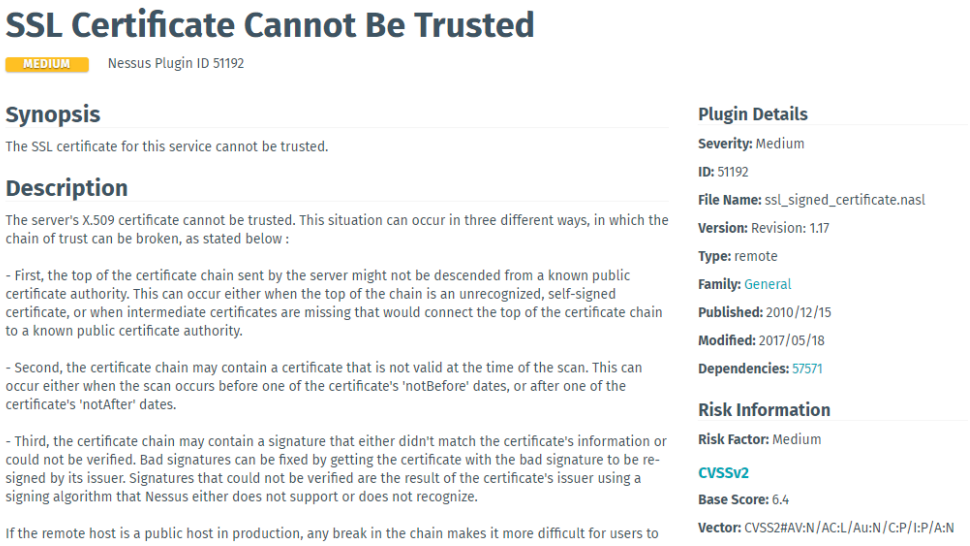
Esta vulnerabilidad (Imagen 17) se debe a que el certificado X.509 del servidor no es confiable. Esta situación puede ocurrir de tres maneras diferentes, en las que se puede romper la cadena de confianza, como se indica a continuación:

a. Primero, la parte superior de la cadena de certificados enviada por el servidor podría no descender de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido o cuando faltan certificados intermedios que conectan la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.

b. Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento de la exploración. Esto puede ocurrir cuando la exploración se produce antes de una de las fechas de "no antes" del certificado, o después de una de las fechas de "no después de" del certificado.

c. En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o no se pudo verificar. Las firmas erróneas se pueden arreglar al obtener el certificado con la firma errónea para que el emisor lo vuelva a firmar. Las firmas que no se pudieron verificar son el resultado del emisor del certificado que utiliza un algoritmo de firma que Nessus no admite o no reconoce.

d. Si el host remoto es un host público en producción, cualquier ruptura en la cadena hace que sea más difícil para los usuarios verificar la autenticidad y la identidad del servidor web. Esto podría hacer que sea más fácil llevar a cabo ataques de hombre en el medio contra el host remoto.



SSL Certificate Cannot Be Trusted

MEDIUM Nessus Plugin ID 51192

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to

Plugin Details

Severity: Medium

ID: 51192

File Name: ssl_signed_certificate.nasl

Version: Revision: 1.17

Type: remote

Family: General

Published: 2010/12/15

Modified: 2017/05/18

Dependencies: 57571

Risk Information

Risk Factor: Medium

CVSSv2

Base Score: 6.4

Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

Imagen 17 Reporte Vulnerabilidad SSL Certificate Cannot Be Trusted

Fuente: Tenable.com

6.1.5 VULNERABILIDAD APACHE MOD_STATUS /SERVER-STATUS INFORMATION DISCLOSURE

Un atacante remoto no autenticado puede obtener una descripción general de la actividad y el rendimiento del servidor web Apache remoto, solicitando la URL "/ server-status". (Ver Imagen 18 y 19) Esta descripción general incluye información como los hosts actuales y las solicitudes que se procesan, el número de procesos inactivos, las solicitudes de servicio y la utilización de la CPU.

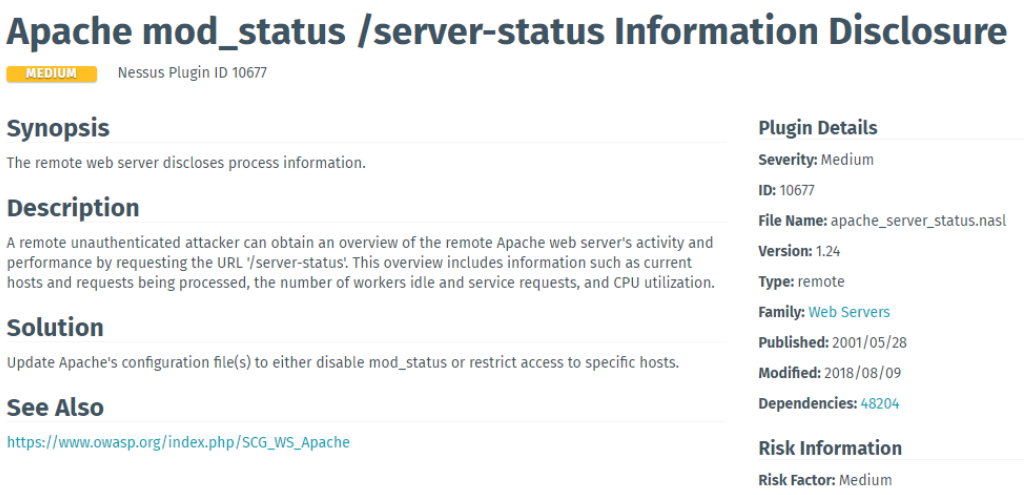


Imagen 18 Apache mod_status report

Fuente: Tenable.com

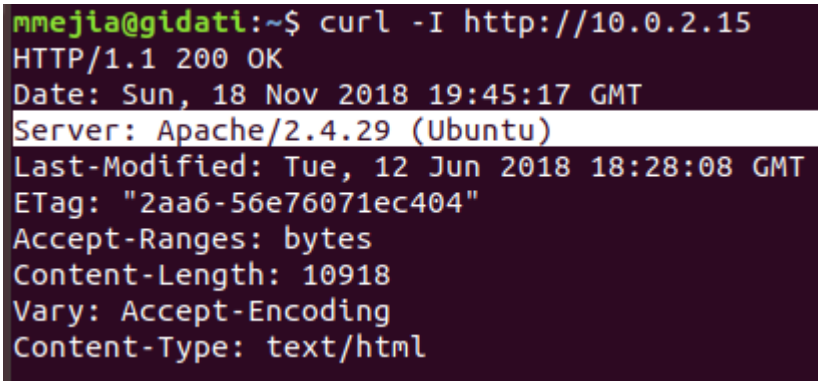


Imagen 19 Comprobación Apache Server Status

Fuente: Elaboración propia

6.1.6 APACHE 2.4.X < 2.4.34 MULTIPLE VULNERABILITIES

Esta vulnerabilidad (Ver Imagen 20) se refiere a la versión de Apache que se ejecuta en el host remoto es 2.4.x antes de 2.4.34. Es, por lo tanto, afectado por las siguientes vulnerabilidades:

a. Robert Swiecki descubrió que el módulo HTTP / 2 del servidor HTTP Apache destruyó incorrectamente ciertas transmisiones. Un atacante remoto podría posiblemente usar este problema para causar que el servidor se bloquee, lo que lleva a una denegación de servicio. (CVE-2018-1302)

b. Craig Young descubrió que el módulo HTTP / 2 del servidor HTTP Apache manejaba incorrectamente ciertas solicitudes. Un atacante remoto posiblemente podría usar este problema para hacer que el servidor consuma recursos, lo que lleva a una denegación de servicio. (CVE-2018-1333)

c. Gal Goldshtein descubrió que el módulo HTTP / 2 del servidor HTTP Apache manejaba incorrectamente grandes marcos de CONFIGURACIÓN. Un atacante remoto posiblemente podría usar este problema para hacer que el servidor consuma recursos, lo que lleva a una denegación de servicio. (CVE-2018-11763) (Ubuntu Security Notes, 2018)

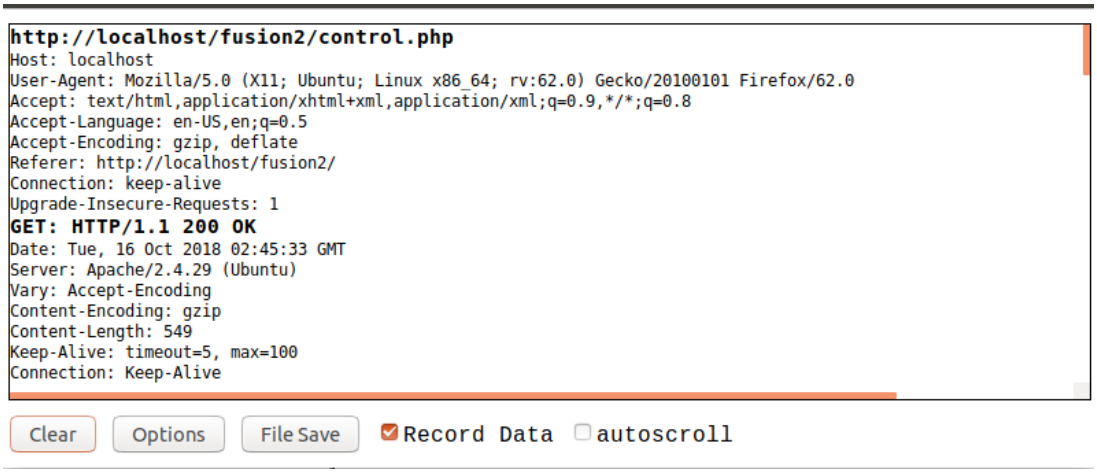


Imagen 20 Versión Apache Web Server y SO

Fuente: Elaboración Propia

6.2 RESOLUCION DE VULNERABILIDADES DETECTADAS

En esta sección se presenta el aseguramiento del centro de fusión con base en las vulnerabilidades significativas detectadas. Con esto se da cumplimiento al objetivo específico 2.

6.2.1 Vulnerabilidad Ubuntu 18.04 LTS: base-files (USN-3748-1), Apache 2.4.x < 2.4.34 Multiple Vulnerabilities y Vulnerabilidades Apache 2.4.x < 2.4.33

Para dar solución a estas vulnerabilidades se requiere llevar a cabo una actualización del sistema. Ejecutamos con elevación de privilegios de super usuario el comando sudo apt-get update (Imagen 21) para listar las ultimas actualizaciones de seguridad disponibles. Seguido de esto procedemos a instalar las actualizaciones con sudo apt-get upgrade (Ver Imagen 22).

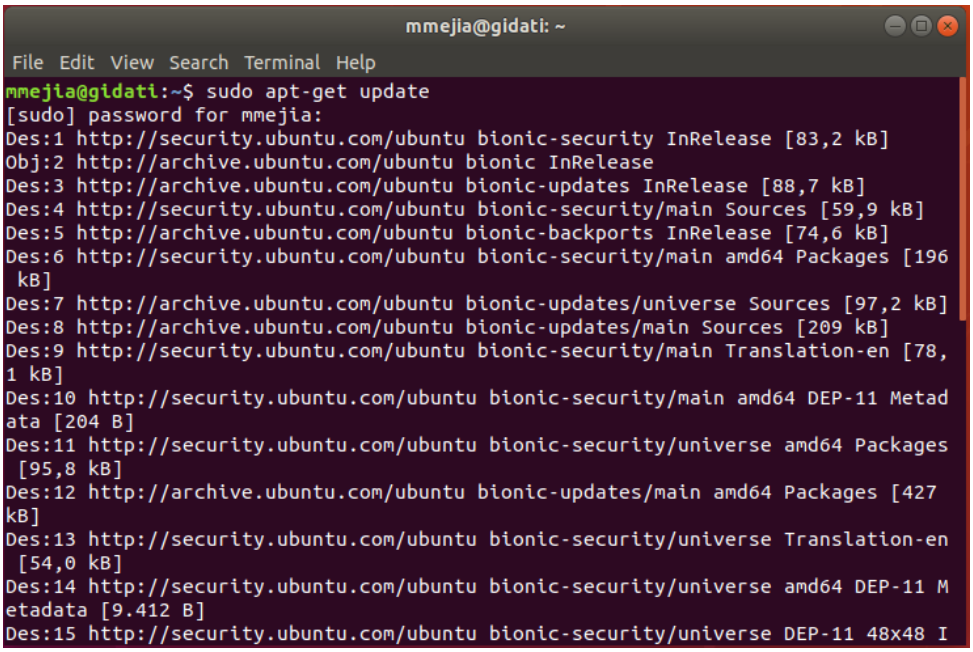


Imagen 21 Update del sistema

Fuente: Elaboración propia

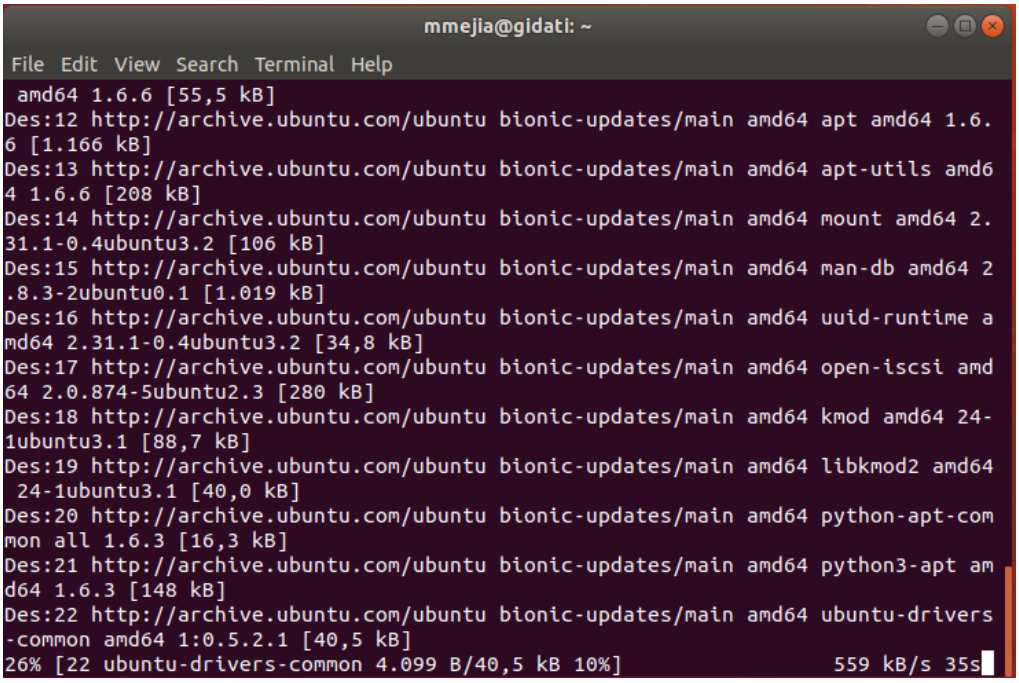


Imagen 22 Upgrade del sistema

Fuente: Elaboración propia

6.2.2 HARDENING APACHE WEB SERVER (CENTRO DE FUSIÓN)

El servidor web es una parte crucial de las aplicaciones basadas en web. Apache Web Server se coloca a menudo en el borde de la red o DMZ (Zona Desmilitarizada), por lo que se convierte en uno de los servicios más vulnerables a los ataques.

La configuración por defecto de Apache proporciona información confidencial que puede poner en riesgo el sistema siendo presa fácil de los cybercriminales.

La mayoría de los ataques de aplicaciones web se realizan a través de XSS [4](Cross-site scripting), Info Leakage, Session Management y PHP Injection,

[4] XSS es un tipo de vulnerabilidad informática o agujero de seguridad típico de las aplicaciones Web, que puede permitir a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar (ej: VBScript), se puede evitar usando medidas como CSP (Política del mismo origen).

que se deben a un código de programación débil y a la falta de desinfección de la infraestructura de la aplicación web.

A continuación, algunas de las mejores prácticas de la industria para el aseguramiento de servidores web Apache.

6.2.2.1 VULNERABILIDAD APACHE MOD_STATUS /SERVER-STATUS INFORMATION DISCLOSURE

Para dar solución a esta vulnerabilidad se desactivan desde al archivo status.conf los parámetros SetHandler server-status en la imagen 23 con el fin de evitar que un host externo rastree información acerca del servidor web que estamos ejecutando.

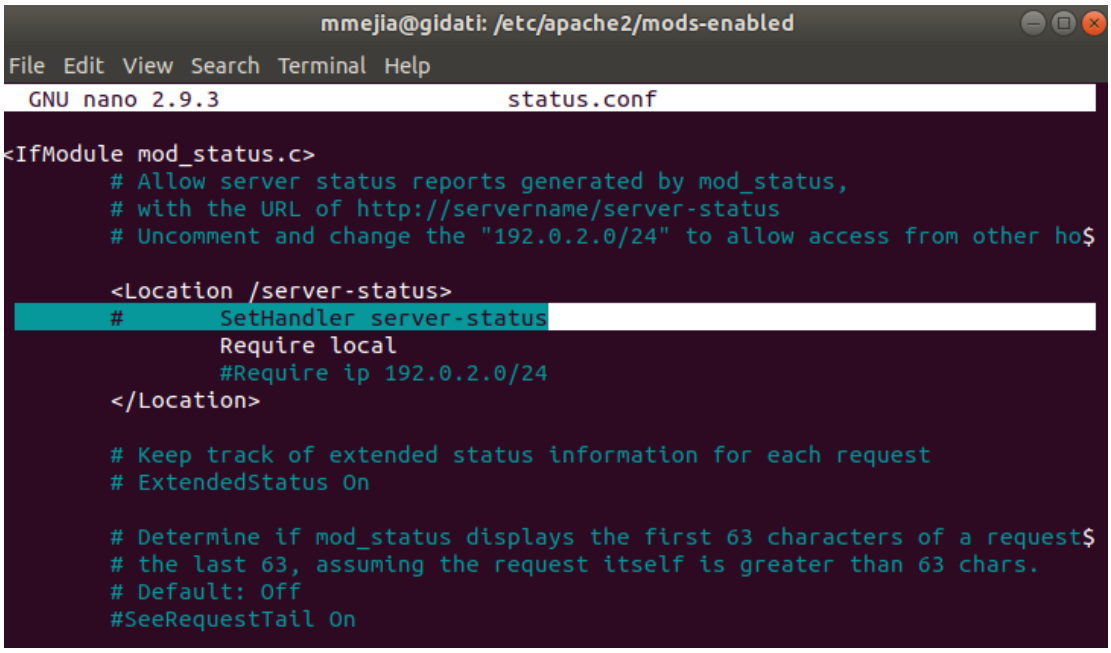


Imagen 23 Deshabilitando mod_status /server-status information disclosure

Fuente: Elaboración propia

6.2.2.2 DESHABILITAR EL LISTADO DEL NAVEGADOR DE DIRECTORIO

Se desactiva la lista de directorios en un navegador de modo que el visitante no vea todos los archivos y carpetas que tiene bajo la raíz o un subdirectorio.

- Veremos cómo se ve en la configuración predeterminada (Imagen 23)
- Vamos al directorio $ Web_Server/htdocs en este caso /var/www
- Creamos una carpeta y algunos archivos dentro de esta.

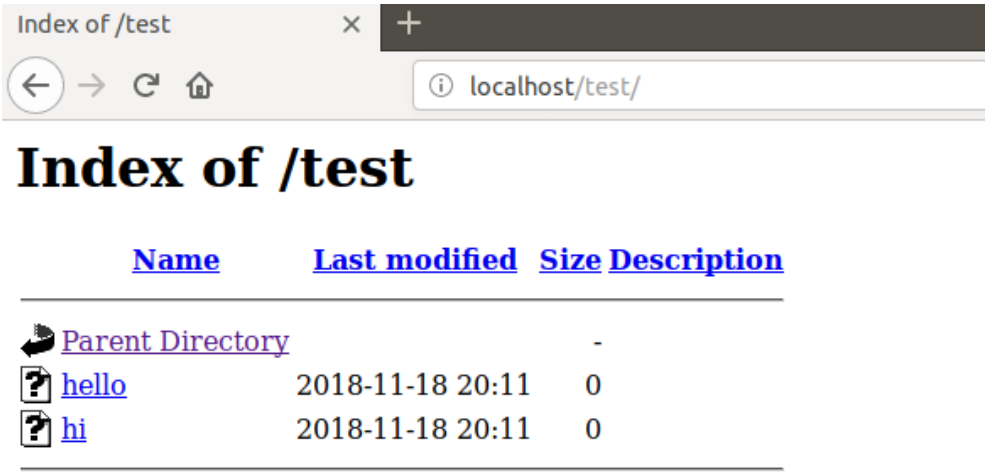


Imagen 24 Listado de archivos y directorios

Fuente: Elaboración propia

Como se puede observar en la Imagen 23, se revelan todos los archivos / carpetas que tiene el servidor y esto es algo que debemos evitar. Para ello cambiamos los parámetros resaltados dentro del archivo apache2.conf (Ver Imagen 24)

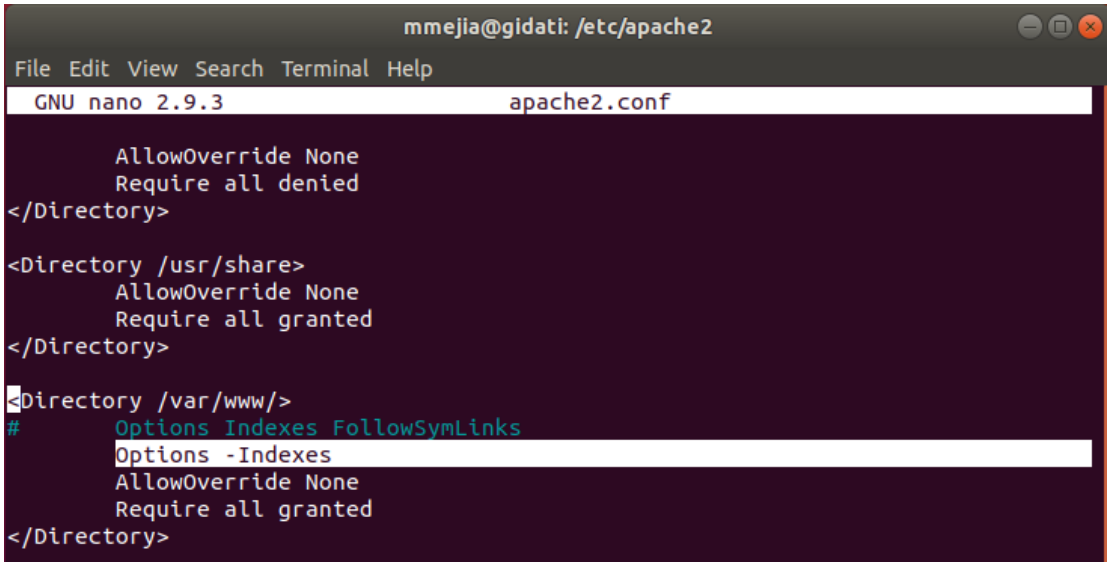


Imagen 25 Parámetro de configuración

Fuente: Elaboración propia

Luego de hacer el cambio en la configuración observamos que los archivos no están disponibles como muestra la Imagen 25.

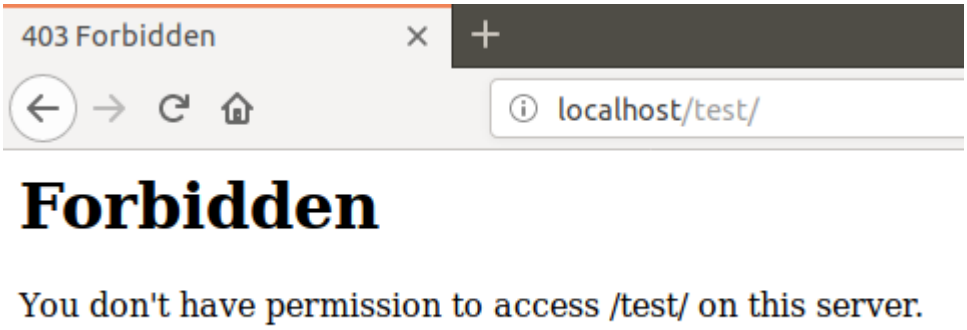


Imagen 26 Negación de navegación de directorio

Fuente: Elaboración propia

6.2.2.3 ETag

Un ETag es un identificador opaco asignado por un servidor web a una versión específica de un recurso que se encuentra en una URL. Si el contenido del recurso en esa URL cambia, se le asigna un nuevo y diferente ETag. Usado

de esta manera los ETags son similares a las huellas digitales, y se puede comparar de forma rápida para determinar si dos versiones de un recurso son la misma. (Ayenson, Mika & James Wambach, Dietrich & Soltani, Ashkan & Good, Nathaniel & Hoofnagle, 2011)

Un ETag, permite a los atacantes remotos obtener información confidencial como el número de inodo, el límite MIME[5] de varias partes y el proceso secundario a través del encabezado Etag.

Para evitar esta vulnerabilidad, procederemos a configurarlo como se muestra a continuación (Imagen 26). Esto es mandatorio generalmente para garantizar el objetivo de conformidad a PCI (Payment Card Industry), que es prevenir el fraude relacionado con tarjetas de crédito.

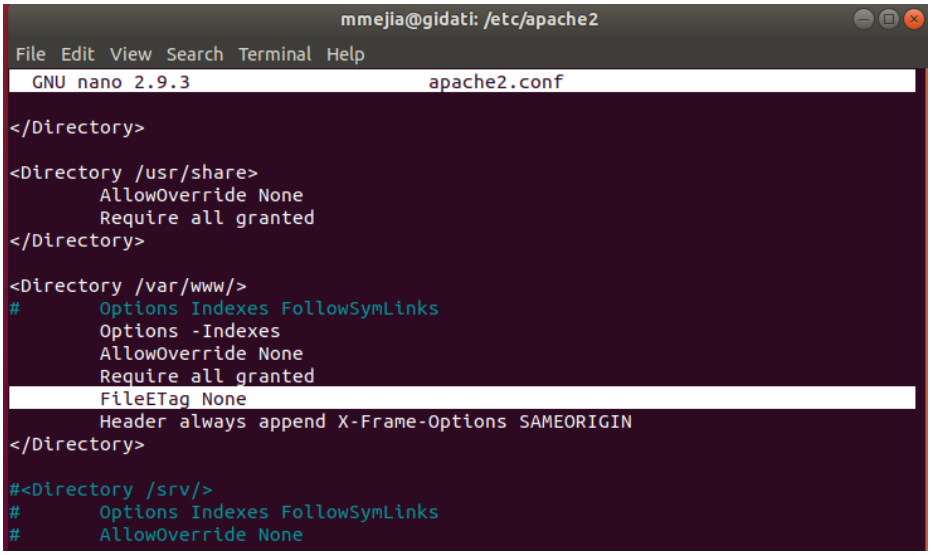


Imagen 27 Configuración ETag

Fuente: Elaboración propia

[5] MIME significa Extensiones de correo de Internet de usos múltiples.

6.2.2.4 MODSECURITY APACHE

Como vimos anteriormente ModSecurity, también conocido como Modsec, es una robusta aplicación WAF de código abierto para el servidor web Apache y ofrece funciones de seguridad a HTTP (Protocolo de transferencia de hipertexto). Dado que es de uso gratuito, se ha adoptado ampliamente para monitorear, registrar y filtrar solicitudes en servidores web Apache.

Se puede observar que la utilidad ha sido un éxito en la lucha contra las vulnerabilidades comunes a lo largo y ancho del mundo, utilizando el conjunto de reglas principales de OWASP ModSecurity[6].

El motor ModSecurity necesita reglas para funcionar. Las reglas deciden cómo se maneja la comunicación en el servidor web. Dependiendo de la configuración, ModSecurity puede pasar, soltar, redirigir, ejecutar un script o incluso mostrar un código de estado durante una sesión.

A continuación, los pasos seguidos para configurar y asegurar el servidor web Apache con ModSecurity en Ubuntu 18.04 Server.

a) Existe un archivo de configuración predeterminado /etc/modsecurity/modsecurity.conf-recommended que copiamos como indica la Imagen 28 en /etc/modsecurity/modsecurity.conf para habilitar y configurar ModSecurity .

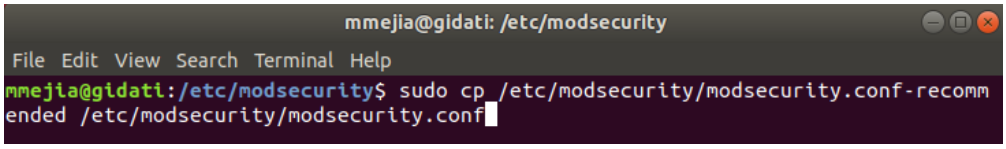


Imagen 28 Copiando archivo de configuración recomendada

Seguido ingresamos al archivo de configuración modsecurity.conf y activamos el motor de reglas como se muestra en la Imagen 29.

[6] El conjunto de reglas básicas de ModSecurity (CRS) de OWASP es un conjunto de reglas de detección de ataques genéricas para usar con ModSecurity - https://modsecurity.org/crs/

Imagen 29 Activando motor de reglas

Fuente: Elaboración Propia

b) ModSecurity tiene un conjunto de reglas predeterminadas ubicadas en el directorio /usr/share/modsecurity-crs. Sin embargo, siempre se recomienda descargar las reglas establecidas desde GitHub:

Antes, cambiamos el nombre del directorio de reglas predeterminado como vemos en la Imagen 30.

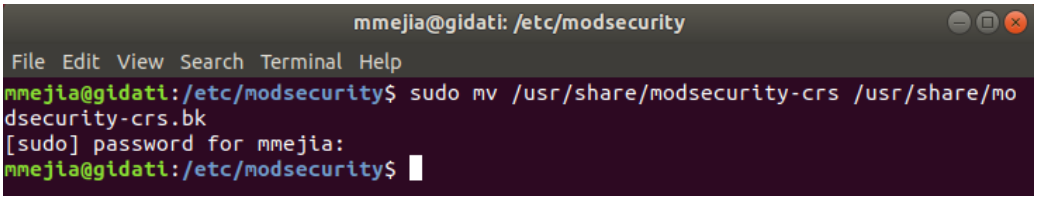


Imagen 30 Cambiando nombre del directorio de reglas predeterminado

Fuente: Elaboración Propia

c) Luego, procedemos a descargar el nuevo conjunto de reglas de GitHub como se muestra en la Imagen 31.

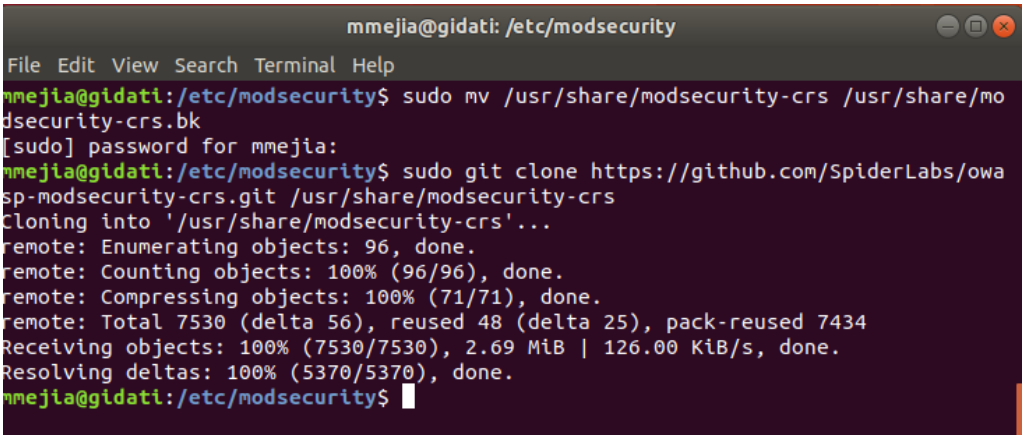


Imagen 31 Descarga conjunto de reglas

Fuente: Elaboración Propia

Copiamos el archivo de configuración de muestra de las reglas descargadas como se muestra en la Imagen 32 con el siguiente comando:

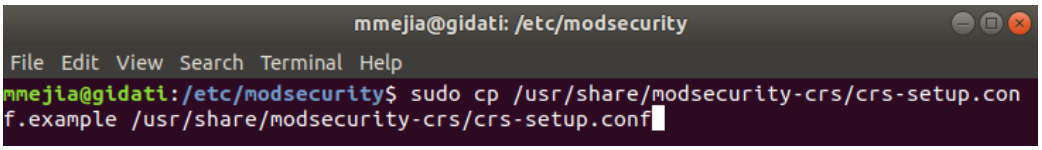


Imagen 32 Copiando configuración de muestra

Fuente: Elaboración Propia

Para que estas reglas funcionen en Apache, debemos editar el archivo /etc/apache2/mods-enabled/security2.conf utilizando un editor como nano y agregando las líneas resaltadas en la imagen 33.

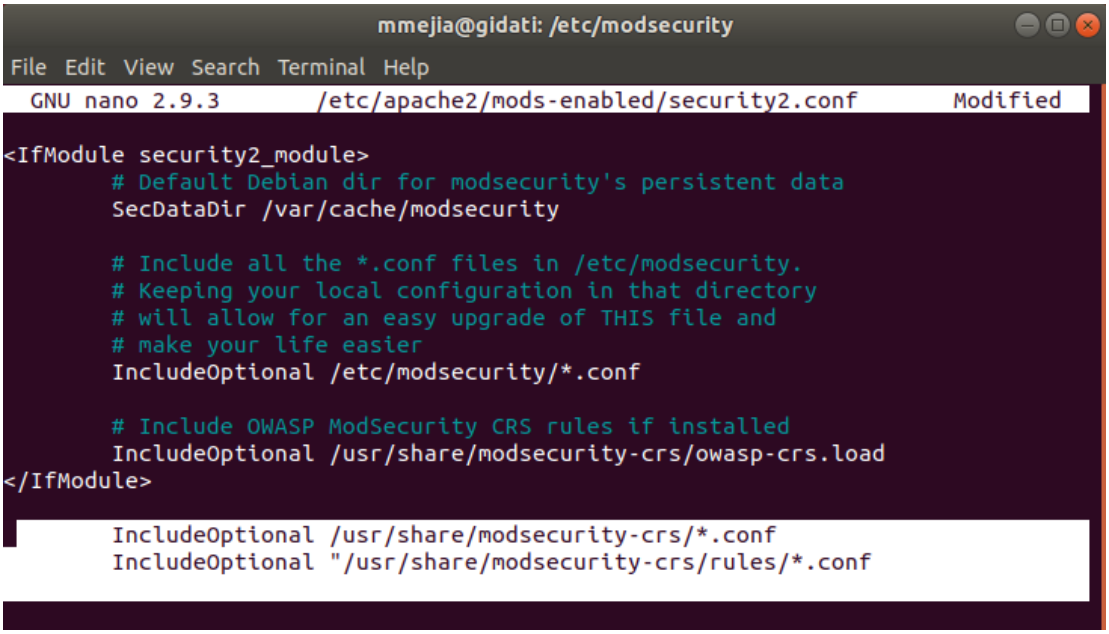


Imagen 33 Activación de configuración para apache

Fuente: Elaboración Propia

Ahora procedemos a ejecutar scripts maliciosos en un navegador y validamos como se activan las reglas de ModSecurity. Introduciendo la URL e instrucción en el navegador como se observa en la Imagen 34.

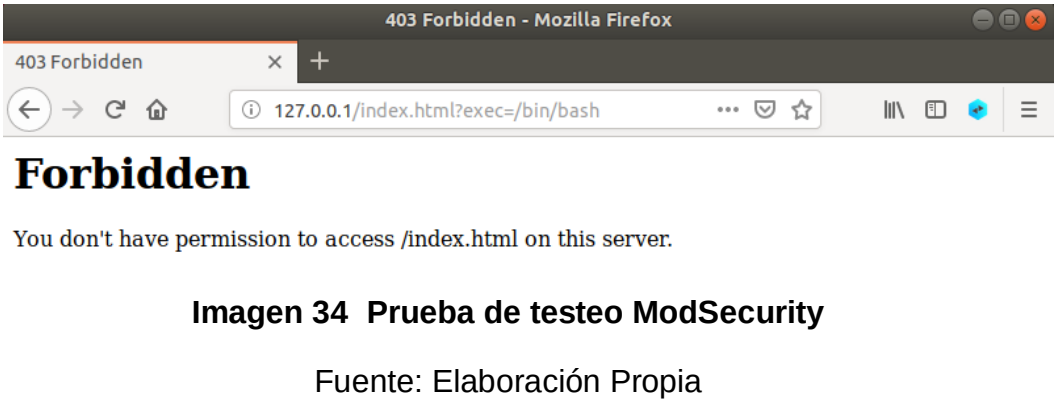


Imagen 34 Prueba de testeo ModSecurity

Fuente: Elaboración Propia

6.3 VALIDACIÓN DE LAS TÉCNICAS DE ASEGURAMIENTO IMPLEMENTADAS

En esta sección se presenta el resultado final con la herramienta de pruebas de vulnerabilidades Nessus después del aseguramiento realizado. Con esto se completa el objetivo específico tres.

Imagen 35 Resultado tratamiento vulnerabilidades

Fuente: Nessus

7. CONCLUSIONES

Los métodos, herramientas, técnicas de seguridad informática son útiles para mitigar un evento de seguridad, teniendo presente que ningún sistema es infalible completamente.

Durante el desarrollo de este trabajo de grado una vez más se logra demostrar que haciendo uso de buenas prácticas de seguridad o hardening basadas en la industria IT, es posible mitigar el riesgo intrínseco de los sistemas informáticos y que para este caso en particular se refiere al Centro de Fusión que en conjunto hablamos de (Sistema Operativo, Servidor Web y Aplicación Web).

Sustentado en la investigación realizada a lo largo de este trabajo y sus correspondientes resultados, podemos afirmar lo siguiente:

1. Para identificar las vulnerabilidades del centro de fusión, fue importante el uso de Nessus como herramienta de análisis y detección.

2. Mantener el sistema operativo actualizado mitiga en gran medida los riesgos de seguridad.

3. Con la seguridad mejorada de Linux a través de hardening, es posible configurar diferentes escenarios de seguridad según las necesidades del sistema.

4. Herramientas como ModSecurity son una excelente alternativa WAF de código libre que mejora significativamente la seguridad a las aplicaciones web no solo en servidores Apache si no también en otras plataformas como IIS (Internet Information Service), Nginx).

5. Es importante que la protección de la red de sensores inalámbricos y del sistema en general, sea compatible con todas las propiedades de seguridad o según sea el caso: confidencialidad, integridad, autenticidad y disponibilidad.

8. TRABAJOS FUTUROS

Los continuos avances en la utilización de las propiedades inherentes de las redes de sensores, ha dado paso a escalar novedosos y más eficientes mecanismos de seguridad e implementación. Sin embargo, se observa que estos adelantos se encuentran en desarrollo por lo que es un tema de estudio constante y abierto a nuevas y prometedoras investigaciones.
Este es el caso por ejemplo de ML (Machine Learning) que es extremadamente útil en las siguientes áreas relacionadas con la ingeniería de software y la ciberseguridad:

6. Problemas de minería de datos donde las grandes bases de datos pueden contener valiosas regularidades implícitas que pueden descubrirse automáticamente.

7. Dificultad para entender los dominios en los que los humanos no tienen el conocimiento para desarrollar algoritmos efectivos.

8. Dominios en los que se requiere que el programa se adapte a condiciones dinámicas.

9. En el caso de los sistemas tradicionales de detección de intrusiones, las alertas generadas son analizadas por un analista humano que las evalúa y realiza una acción adecuada. Sin embargo, esta es una tarea extremadamente ardua ya que la cantidad de alertas generadas puede ser bastante grande y el entorno puede cambiar continuamente. Esto hace que Machine Learning sea adecuado para la detección de intrusiones.

9. REFERENCIAS

Abdalzaher, M. S., Seddik, K., Elsabrouty, M., Muta, O., Furukawa, H., & Abdel-Rahman, A. (2016). Game theory meets wireless sensor networks security requirements and threats mitigation: A survey. *Sensors (Switzerland)*, *16*(7), 22–27. https://doi.org/10.3390/s16071003

Abdullah, H., & Teknologi, U. (2014). Issues and Challenges in Localization of Wireless Sensor Networks ISSUES AND CHALLENGES IN LOCALIZATION OF WIRELESS, (MAY).

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine*, *40*(8), 102–105. https://doi.org/10.1109/MCOM.2002.1024422

Athanasios, G. (2011). Security Threats in Wireless Sensor Networks : Implementation of Attacks & Defense Mechanisms.

Ayenson, Mika & James Wambach, Dietrich & Soltani, Ashkan & Good, Nathaniel & Hoofnagle, C. (2011). Flash cookies and privacy II: now with HTML5 and ETag respawning. *SSRN Electronic Journal. 10.2139/Ssrn.1898390*.

Azzedine Boukerche, P. (2009). *Algorithms And Protocols For Wireless Sensor Networks*. *Networks* (Vol. 6). https://doi.org/10.1002/9780470396360

Barbara, F. (2012). Estudio de algoritmos de localización en interiores, para tecnologías móviles de última generación.

Benenson, Z., Cholewinski, P. M., & Freiling, F. C. (2007). Vulnerabilities and attacks in wireless sensor networks. *Wireless Sensor Network Security*, 22–43. Retrieved from http://www1.informatik.uni-erlangen.de/filepool/publications/zina/attacker-models-bookchapterIOS_Press.pdf%5Cnhttp://books.google.com/books?hl=en&lr=&id=pA2XUtdwewAC&oi=fnd&pg=PA22&dq=Vulnerabilities+and+attacks+in+wireless+sensor+networks&ots=EWSDVSXYOF&

Boulton, J. (2014). Apache web server. *100 Ideas That Changed the Web*, (London, UK), [Online]. London: Laurence King. Available from: h.

Bowen, R., & Coar, K. (2008). Apache Cookbook, 310. https://doi.org/10.1017/CBO9781107415324.004

Bravo, I., Palomar, E., Gardel, A., & Lázaro, J. L. (2017). Trusted and secure wireless sensor network designs and deployments. *Sensors (Switzerland)*, *17*(8), 1–6. https://doi.org/10.3390/s17081787

Castillejo, P., Martínez-Ortega, J. F., López, L., & Alcón, J. A. S. (2015).

SensoTrust: Trustworthy Domains in Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*, *2015*. https://doi.org/10.1155/2015/484820

Chan, H., & Perrig, A. (2003). Security and privacy in sensor networks. *Computer*, *36*(10), 103–105. https://doi.org/10.1109/MC.2003.1236475

Chen, Y., & Yang, C. (2006). A RSSI-based algorithm for indoor localization using ZigBee in wireless sensor network. *International Journal of Digital Content Technology and Its ApplicationsJournal of Digital Content Technology and Its Applications*, *5*(7), 407–416. Retrieved from http://www.aicit.org/jdcta/paper_detail.html?q=606

Comunicaciones, M. de. (2005). Decreto Nro 195 de 2005. Campos electromagneticos.

Contreras Javier & Mayol Reinaldo. (2016). (VARIATION OF PARAMETERS OF ELLIPTIC CURVE CRYPTOGRAPHY USED IN, 41–53.

Fern, J. N. (2010). Simulación de Redes de Sensores Wireless, 105.

García, A. F., Gómez, C., Sánchez, T., Redondo, A. D., Betancur, L., & Hincapié, R. C. (2016). Algoritmos de Radiolocalización basados en ToA, TDoA y AoA. *Ingeniería y Región*, *14*(2), 9. https://doi.org/10.25054/22161325.689

García Arano, C. (2010). Impacto de la seguridad en redes inalámbricas de sensores IEEE 802.15.4, 15–49. Retrieved from http://eprints.ucm.es/11312/1/Memoria_Fin_de_Master_-_Carlos_Garc﷿a_Arano.pdf

Garcia Polo, E. M. (Universidad de C. (n.d.). Técnicas de Localización en Redes Inalámbricas de Sensores, *46*.

Gosselin, M. J., & Schommer, J. (n.d.). Confining the Apache Web Server with Security-Enhanced Linux, 1–12.

He, J., Yang, Z., Zhang, J., Liu, W., & Liu, C. (2018). On the security of a provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. *International Journal of Distributed Sensor Networks*, *14*(1). https://doi.org/10.1177/1550147718756311

Igor Ljubuncic. (2011). Apache Web Server - Complete Guide. *Dedoimedo.Com*.

ITU. (2000). K.52 (02/2000), *52*.

Kavitha, T., & Sridharan, D. (2010). Security Vulnerabilities In Wireless Sensor

Networks : A Survey. *Journal of Information Assurance and Security*, *5*(2010), 31–44.

La, C., Nacional, A., Se, D. E. E. Y., & Otras, D. (2009). Nh.1341 ~ 2009 ••. *Ley No.1341 30 Julio*, 1–34.

Liu, H. (2007). Survey of Wireless Indoor Positioning Techniques and Systems, *37*(6), 1067–1080. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4343996&tag=1

Mazurek, L. (2011). Localization in Wireless Sensor Networks Localization problem in WSN.

O. Gualdrón, S. Pinzón, L. De Luque, I. Díaz, S. V. (2006). UNA HERRAMIENTA PARA LA PREDICCIÓN DE LA DE INTENSIDAD DE LA SEÑAL RECIBIDA (RSSI) PARA WIRELESS LAN 802.11B. *Mycological Research*, *1*(11), 1323–1330.

Platon, E., & Sei, Y. (2008). Security software engineering in wireless sensor networks. *Progress in Informatics*, (5), 49–64. https://doi.org/10.2201/NiiPi.2008.5.6

Proposal, P., & Engineering, E. (2015). Compressed Localization And Spectrum Sensing for Cognitive Radio and Distributed Radio Surveillance (CLASS) Collaborative Research Initiative in Electrical Engineering, 1–36.

Rey, U., & Carlos, J. (2014). Algoritmos de aprendizaje estadístico aplicados a la radiolocalización en interiores Algoritmos de aprendizaje estad ´ a la radiolocalizaci ´, (October).

Rugeles, J. D. J., & Leon, D. (n.d.). Técnicas de localización de nodos inalámbricos mediante redes de sensores.

Tenable. (2018). Ubuntu 18.04 LTS : base-files vulnerability (USN-3748-1).

Trustwave. (2016). ModSecurity: Documentation. Retrieved from http://www.modsecurity.org/documentation.html

Ubuntu Security Notes. (2018). USN-3783-1: Apache HTTP Server Vulnerabilities.

Un, S. E. C., & Preservan, Y. S. E. (2009). Ley No 1273. *MinTIC*, (48). Retrieved from http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Walters, J. P., Liang, Z., Shi, W. (Department of C. S. W. S. U., & Chaudhary,

V. (Department of C. S. W. S. U. (2006). Chapter 17 Wireless Sensor Network Security : A Survey ∗. *Security in Distributed, Grid, and Pervasive Computing*, 1–50.

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE*, *104*(9), 1727–1765. https://doi.org/10.1109/JPROC.2016.2558521

10. ANEXO 1

MAQUINA VIRTUAL UBUNTU SERVER 18.04