Red Nacional de Semáforos Inteligentes: Dando luz verde a la ciberseguridad

Erick Brenes, Alvaro Mora, Oscar Alpízar, and Randall Barnett

Escuela de Ingeniería,
Universidad Latinoamericana de Ciencia y Tecnología,
ULACIT, Urbanización Tournón, 10235-1000
San José, Costa Rica
ebrenesm522,amoral306,oalpizarp588,rbarnettv200@ulacit.ed.cr
http://www.ulacit.ac.cr

Resumen La naturaleza crítica del control del flujo vehicular propicia que los semáforos inteligentes sean la solución adecuada para la mayoría de ciudades que han tenido la necesidad de llevar el orden a la carretera. Dicha infraestructura estatal está conformada por una serie de elementos pero en su mayoría por dispositivos electrónicos inteligentes haciendo dicha infraestructura muy susceptible a ataques informáticos.
Por medio de distintas técnicas para obtener información como la ingeniería social, visitas de campo y acceso a documentación de los fabricantes, el artículo plantea el estado de arte de la Red Nacional de Semáforos Inteligentes desarrollada por el MOPT, así como también la revisión de la seguridad dando como resultado la identificación de una serie de vulnerabilidades de diseño e implementación, las cuales podrían convertirse en una falla sistémica que podrían ocasionar desde la caída de un semáforo, o intersección, hasta la salida de operación del centro de monitoreo. Se plantean mejoras a varios niveles, pero principalmente en materia de alta disponibilidad, tolerancia a fallos y en la adopción de un marco para gestionar la seguridad informática por parte del ente rector.

Keywords: semaforización inteligente, flujo vehicular, infraestructura estatal, ataques informáticos, ingeniería social.

1. Introducción

Debido al aumento del flujo vehicular en el mundo, en conjunto con el auge de nuevas tecnologías, ha evolucionado la forma de cómo las entidades responsables de la seguridad vial gestionan sus recursos para innovar con productos que favorezcan la fluidez y seguridad de los recorridos realizados por los usuarios en la actualidad. Buscando la manera de interconectar los diferentes sistemas de señalización, es donde la tecnología ha sido aliada durante el proceso de rediseño de muchos de los sistemas anteriormente conocidos y que recibieron no solo una nueva utilidad sino que también acarrean nuevos mecanismos de control para el confort en carretera.

La utilización de tecnologías ya existentes se ha convertido en un proceso de reinserción hacia los sistemas de señalización, dado que no eran anteriormente diseñados para estos mecanismos, pero que gracias a su efectividad y confiabilidad ha generado que muchos de los medios de señalización actuales tengan la facilidad de emigrar hacia nuevas plataformas, dando la pericia a las organizaciones responsables de crear sistemas en red, acarreando controles más exhaustivos y centralizados de la información actualizada en carretera.

Gracias a estas nuevas técnicas, se pueden crear semáforos capaces de automatizar el intercambio de señalización dependiendo de la cantidad de flujo vehicular y a su vez que otros dispositivos cercanos pertenecientes a la misma red, ejecutando el mismo mecanismo, puedan recolectar información y brindarla a un sistema centralizado, donde se realizan las labores necesarias para el control de tráfico de una ciudad. Con esto, muchos de los sistemas de señalización actuales dejarían de ser un simple mecanismo autosuficiente y se convertirían en un medio compartido de información y de control inteligente en la infraestructura vial de un país.

Utilizar tecnologías de red en estos dispositivos, tanto inalámbricas como alámbricas ha favorecido el crecimiento de este nuevo método de control en carretera, dado que permite la conexión entre los equipos de manera segura y eficiente, garantizando no solo su correcta comunicación con la sede central, también utilizando todos los factores de seguridad que estas técnicas ofrecen ya sea por medio de protocolos o de cableado son muchas las virtudes que se aprovechan para la creación de sistemas de control de tráfico inteligente.

Uno de los principales factores que ha priorizado la implementación de esta tecnología en los sistemas de control de tráfico actual, radica en la necesidad de introducir productos que apoyen las políticas mundiales de protección al medio ambiente, ya sea mediante el uso de energías limpias, utilizando paneles solares para la operación de los equipos o bien colaborando en la reducción de congestiones vehiculares favoreciendo la disminución de los índices contaminación y mejorando la huella carbono neutral, favoreciendo a los gobiernos que implementen estas iniciativas. Utilizar este tipo de sistemas, le garantiza al país un mejor aprovechamiento de sus recursos en inversión de infraestructura vehicular, convirtiéndose en una nación abierta al uso de nuevas tecnologías para el bienestar social, acarreando adicionalmente un atractivo de inversión extranjera, dada las condiciones favorables con las que se contarían. El país ha dado inicio con la implementación de estas nuevas técnicas, como método de mitigación al gran número de problemas existentes, que hacen de las carreteras nacionales una agonía de paso en paso.

Constantemente la congestión en las autopistas o en las principales carreteras de las ciudades aunado a la mala educación vial de la población, provocan malestar en los conductores y a su vez preocupación en las entidades de salud, dada la cantidad de accidentes que se presentan por irrespeto o desconocimiento al sistema de señalización. Es por esta razón que implementar paulatinamente la utilización de semáforos inteligentes puede colaborar en la disminución del

flujo vehicular en las horas de mayor congestionamiento y un aseguramiento del cumplimiento y aplicación de las leyes de tránsito.

Adicionalmente, este tipo de tecnologías cuenta con la capacidad de aumentar sus beneficios para el control de tránsito, adaptando nuevos mecanismos que pueden ser fácilmente adicionados, mejorando la intercomunicación entre los equipos de red, abriendo una puerta efectiva de comunicación entre los sistemas de control y los usuarios. Este tipo de tecnología pretende brindar al país un paso efectivo e innovador en la lucha por evitar un aumento en la congestión vehicular, permitiendo de manera controlada en puntos estratégicos agilizar, supervisar e informar la situación en tiempo real del estado del tránsito en carretera.

Durante el desarrollo de este artículo, se recurrirá a fuentes primarias como lo es el MOPT [1], como ente encargado de la seguridad vial del país, con entrevistas directamente con las personas encargadas del área del sistema de control, y por toda la información brindada en las visitas de campo realizadas durante el periodo de realización de la investigación, adicionalmente se recurrirá a revisar contenido bibliográfico como tesis, publicaciones en revistas, artículos, por medio de la plataforma EBSCO, la misma facilitada por la ULACIT [2], para el desarrollo de dicho documento, también se utilizarán libros relacionados con los temas de estudio, así como casos de uso y metodologías utilizadas por países en el extranjero por medio de publicaciones en foros especializados de personas que se han dado a la tarea de realizar estudios similares a este.

2. Antecedentes

Se dice que todos los caminos conducen a Roma, esto debido a que fueron los primeros en diseñar una red internacional de caminos, llamadas “Calzadas Romanas” que se encargaban de unir la ciudad con todas las demás poblaciones del Imperio, es por esta razón que para cubrir las necesidades de dirección entre ciudades se creó un sistema de señalización por medio de hitos, que se utilizaban para transmitir información a los viajeros, en términos generales partiendo desde este punto podemos marcar este acontecimiento como pieza fundamental de la evolución de los sistemas de señalización en el mundo.

Con la invención del automóvil, estos sistemas comenzaron a sufrir diferentes variantes, con el objetivo de contar con un sistema que permitiera informar, controlar y ubicar a los usuarios durante sus recorridos, siendo divididas en familias en las que se puede encontrar las señales:

1. Preventivas.
2. Reguladoras.
3. Informativas.
4. Semáforos.

Siendo estos últimos catalogados como señales de control de tráfico, normalmente situados en intersecciones o puntos específicos con el objetivo de regular el

[1] Del acrónimo Ministerio de Obras Públicas y Transportes
[2] Del acrónimo Universidad Latinoamericana de Ciencia y Tecnología

tráfico vehicular y por ende el peatonal. Considerándose en este tema al inventor afroamericano Garrett Morgan, como el encargado de desarrollar los automatismos del semáforo en el año 1922 y William Potts, como el creador de la señal de tres colores que se utiliza en la actualidad (Semáforo, 2015).

Propiamente en Costa Rica, para el año de 1860, dado el aumento de las edificaciones públicas, caminos y demás tareas realizadas con fondos nacionales se consideró pertinente la creación de una institución que se encargara de supervisar la construcción de dichas obras, manteniendo ciertos estándares requeridos en la época, su solidez y estabilidad;lo cual garantizaba el progreso de la población y el embellecimiento del país. Es así como se crea la Dirección General de Obras Públicas, como el ente responsable de ejecutar estos mandatos y velar por el buen desarrollo de las comunidades.

Con el paso de los años y con esto el cambio constante de administraciones gubernamentales, esta entidad sufre cambios no solo en asignaciones de nuevas labores, sino también directamente con su nombre, siendo rebautizada nuevamente luego de algunos renombramientos ya realizados con anterioridad en el año de 1971 como Ministerio de Obras Públicas y Transportes (MOPT, 2015), tal como se le conoce en la actualidad. Siendo la institución responsable de regular y controlar el transporte, así como de diseñar, ejecutar y mantener obras de infraestructura vial en Costa Rica, velando por la seguridad y eficiencia de estas, contribuyendo al crecimiento social y económico del país, además de colaborar con trabajos amigables con el ambiente.

3. Congestionamiento vehicular

Como lo establece Ortúzar-Willumsen, (1994) el congestionamiento surge en condiciones en que la demanda se acerca a la capacidad de la infraestructura y el tiempo de tránsito aumenta a un valor muy superior al que rige en condiciones de baja demanda (refC). Lo anterior, para un país como Costa Rica, donde el 55 % de la población nacional y el 92 % de las exportaciones se concentran en el GAM (refD), representa un grave problema en vista del impacto frontal que recibe la infraestructura vial producto de la alta densidad en un área pequeña en la cual convergen ambos, centros económicos y espacios habitacionales y que se acrecienta aun más producto del incremento de la flota vehicular y del rezago en inversiones públicas orientadas a mejorar la red nacional vial del país

4. Sistemas de Tráfico Inteligente

La naturaleza crítica del control del flujo vehicular propicia que los sistemas de tráfico inteligente (ITS) sean la solución adecuada para la mayoría de ciudades que han tenido la necesidad de llevar el orden a la carretera. Dichos sistemas conformados en su mayoría por dispositivos electrónicos inteligentes (IEDs [3])

[3] Del Acrónimo en inglés Intelligent Electronic Devices

han ganado terreno como la implementación preferida por las autoridades a las que compete la gestión del control de tráfico.

La premisa sobre la cual se fundamentan los sistemas de tráfico inteligente es el "internet de las cosas" (IoT [4]), el cual busca un deseo de intercambio de información en tiempo real entre múltiples entidades valiéndose de las redes telemáticas (Xi Li - Hong Ji - Yi Li). IoT se ha propuesto conectar todos los elementos posibles juntos, y luego darse cuenta también en tiempo real la interacción que se realiza en sociedad es decir entre las personas y entre las personas y las entidades. Con entidades se definen en dispositivos que interactúan con el ser humano o que lo hacen al nivel de entidad. Se podrían enumerar muchas entidades IoT, pero algunas son cámaras, televisores, teléfonos celulares, Smart TV, dispositivo GPS, dispositivos de parqueo inteligentes, y por supuestos semáforos, cámaras de video, sistemas de control de acceso tráfico, señalización horizontal en autopistas, sistemas de cobro en carretera, radares de patrullas de camino, entre muchos otros.

Como se puede intuir, IoT supone gran cantidad de información, la cual debe ser recogida, analizada, procesada mediante una serie de tecnologías que permitan una identificación y gestión inteligente de la misma, de tal forma que se procese lo que realmente supone información oportuna para el ser humano y para las entidades de IoT. En línea con lo anterior es que los sistemas de tráfico inteligente (ITS) disponen de protocolos como el NTCIP [A] de la NEMA [5] garantiza la interoperabilidad e intercambio de información de transporten entre fabricantes, permitiendo así la recolección y procesamiento de datos para la toma de decisiones en el control de flujo vehicular proveniente de dispositivos como señales de tráfico, sensores, circuitos cerrados de televisión, estaciones de conteo y pesaje de vehículos, rampas de salida o entrada de autopista, sistemas de priorización de trasporte (público y de emergencia)

Para que un ITS sea verdaderamente robusto, debe incorporar la gestión de fallos (Fault Management); la cual cual garantiza la detección, localización y recuperación de fallos. Ahora bien, en implementaciones de ITS, normalmente extensas geográficamente y heterogénas en tecnologías, resulta muy difícil adoptar un solo algoritmo para administración de fallos. Xi Li - Hong Ji - Yi Li [B] plantean que un enfoque práctico es una estructura general que estandarice el procedimiento de control. El cual mediante un enfoque por capas sea flexible y capaz de la detección de fallos, que pueda localizarlas y que pueda rescatarse A sí mismo en caso de fracaso, teniendo en cuenta el entorno de comunicación complicado de IoT sobre el cual operan los componentes de una infraestructura de tráfico en carretera. En este enfoque de capas, los fallos se adaptan a la arquitectura de la red del ITS y se recuperan a sí mismos mediante puntos de observación a lo largo de la infraestructura, estos puntos de observación se denominan "Mapas Cognitivos Difusos" (Fuzzy Cognitives Maps, FCM); los cuales ofrece diversos criterios predictivos para garantizar que el intercambio de información en tiempo real nunca se detenga.

[4] Del Acrónimo en Inglés Internet of Things
[5] Del Acrónimo en inglés National Electrical Equipment Manufacters Association

Tradicionalmente; la administración de fallas (fault management) en la redes telemáticas se ha encaminado en la adopción de algoritmos definidos en el protocolo SNMP (simple network management protocol) por medio del cual se detecta, localiza, analiza y mide el problema; sin embargo, dicho mecanismo no satisface la mayoría de los sistemas inalámbricos, o el propio IoT, por ende no resulta confiable para implementar en bajo una infraestructura de ITS

5. Sistemas de control de tráfico en varias ciudades

En la provincia de Alberta, Canadá la ciudad de Calgary cuenta con un ITS1 interconectado con el centro mediante conectividad inalámbrica de banda ancha. El diseño de la arquitectura de conectividad fue motivada por requerimientos de logística propios de la geografía del lugar, así como por el análisis de costo beneficio [1] planteado por la autoridad. Todo esto ha permitido que la ciudad de Calgary cuente con una plataforma segura y robusta para integrar de forma inalámbrica sistemas como semáforos, controles variables de mensajes para tráfico vehicular, así como para el propio monitoreo de infraestructura por medio de sistemas de CCTV [6].

En el estado de Washington, Estados Unidos, la Administración Nacional de Seguridad en Carreteras (NHTSA [7]) ha iniciado esfuerzos para habilitar la tecnología de comunicación (V2V) [2], la cual permite que los vehículos en carrera recolecten y diseminen datos entre sí y entre los ITS's como por ejemplo ubicación, velocidad de circulación. En esta ciudad, partiendo del estado del flujo de vehículos, la comunicación vehículo a vehículo permite realizar procesos de analítica para controlar el cambio de luces en los semáforos inteligentes o incluso la activación de sistemas de señalización variables de velocidad en carretera (Variable Speed Limit Sing [8]).

En la ciudad de New York, el Departamento de Transporte logró realizar la modernización del sistema de control de tráfico con la premisa de una implementación vanguardista, que cumpliera con la demanda del tránsito vehicular en una de las ciudades más convulsas del mundo, donde además el peatón es parte integral del ecosistema de esta ciudad [2]. La empresa Peek fabricó el controlador de tráfico ATC CBD [3] específico para el requerimiento de la ciudad, el cual es un chasis basado en Linux y alienado al protocolo NTCIP (National Transportation Communication for Intelligent System Transportation [9]). Por otra parte, la empresa Transcore (líder consultor del proyecto) tuvo a cargo el diseño y ejecución con la premisa de impulsar la detección y monitoreo de tráfico de una manera no intrusiva al paisaje urbano, y con la integración al back bone inalámbrico NYCWiN (New York City Wireless Network [10]) el cual pro-

[6] Del Acrónimo en Circuito Cerrado de Televisión
[7] Del Acrónimo en inglés National Highway Traffic Safety
[8] Del Acrónimo en inglés Señales Variables de Límites de Velocidad
[9] Del Acrónimo en inglés Protocolo de Comunicación para Sistemas de Transporte Inteligentes
[10] Del Acrónimo en inglés Red Inalámbrica de la Ciudad de New York

vee comunicación para servicios esenciales de policía, tránsito, salud, bomberos, en tiempo real de forma segura y redundante para las cinco jurisdicciones que forman el ayuntamiento.

Por otra parte, la ciudad de San José, Costa Rica cuenta con una implementación compuesta por noventa intersecciones automatizadas mediante el uso de varios componentes dentro de los cuales se encuentran semáforos, cámaras, dispositivos de control, enlaces de telecomunicaciones y personal de gestión del sistema; esta infraestructura es conocida como la Red Nacional de Semáforos Inteligentes (RNSI) [4]. Para tal efecto, el municipio josefino dispone de un enlace central (BB [11]) de fibra óptica encargado de conectar a la red los dispositivos inalámbricos integrados a los semáforos inteligentes, haciendo que una gran parte de dichas intersecciones esté siendo enlazadas de forma inalámbrica al centro de control, ubicado en la Dirección General de Ingeniería de Tránsito (DGIT) del Ministerio de Obras Públicas y Transporte (MOPT). El consorcio SEMEX, de origen mexicano especializado en semaforización, marcaje horizontal, estructuras, luminarias y mantenimiento de obras, es la empresa consultora que en gran medida ha estado a cargado de la implementación y mantenimiento del proyecto en esta ciudad.

6. Descripción del Sistema de Tráfico

6.1. Controladores de tráfico inteligente

Corresponden a equipos electrónicos que tienen como función la administración de una intersección de tránsito mediante la lectura de las entradas de los sensores y control del estado de las luces de los semáforos. (Ghena, Beyer, Hillaker, Pevarnek, y Halderman, 2014)

Las intersecciones pueden operar en diferentes modos, por ejemplo el modo más sencillo es llamado No Actuado[12] en el cual trabaja con tiempos fijos para cada secuencia de luces y no depende de ningún sensor. Por el contrario, un modo de operación complejo es llamado Normalmente Actuado[13] en el cual la secuencia de luces de un semáforo puede incrementar o disminuir dependiendo de las mediciones de los sensores. (SEMEX, 2003)

En cuanto al equipo controlador, este puede operar en modo aislado, coordinado o centralizado. Cuando opera de manera aislada, los tiempos de las luces son independiente de otras intersecciones. En modo coordinado, opera en conjunto con otras intersecciones y por último en modo centralizado, se encuentra integrado en una red centralizada de control de tránsito con capacidad de integrase a sistemas de respuesta al transito. (Corporation, 2012)

[11] Del Acrónimo en inglés Backbone
[12] Tiempo Fijo
[13] Tiempo de la secuencia de luces varia

6.2. Sensores de Apoyo

Los sensores de apoyo son dispositivos destinados principalmente para la detección e identificación de los diferentes vehículos que circulan en una intersección. En Costa Rica, se ha denominado Puesto de Medición[14] a estaciones compuestas por sensores como detectores electromagnéticos ubicados bajo la capa asfáltica o sensores digitales como la video detección.

Estos puestos de medición están situados en intersecciones estratégicas de la red vial y en una zona específica, conforman un Sistema de detección, el cual realiza los estudios estadísticos para obtener las variables como volúmenes vehiculares, porcentajes de ocusación y velocidades medias.

6.3. Sistemas de telecomunicaciones

De acuerdo con entrevista realizada al Ing. Jose Roldán del DGIT, el sistema nacional de control de tráfico dispone de una red de telecomunicaciones heterogénea, la cual entrelaza las diferentes intersecciones centralizadas con el Centro de Control de Tránsito para su control y monitoreo.

Dependiendo de la zona en la que se ubica la intersección, se define en cada una de ellas una red de interconexión, más conveniente en función de la infraestructura existente. Para la zona central se cuenta con una red de fibra óptica y pares telefónicos que comunican los controladores con el centro de control utilizando el tendido subterraneo de la capital, por otra parte para la zona centro oeste, se dispone de una red inalámbrica.

Las zonas radiales por su parte cuentan con grupos de controladores que se interconectan de manera inalámbrica. Cada grupo de controladores dispone de un controlador designado como principal y que es el encargado de realizar la comunicación con el Centro de Control utilizando enlaces mediante internet arrendados al ICE.

6.4. Software de Gestión de Tránsito

Adicionalmente a los equipos controladores y diferentes sensores instalados, el CCT cuenta con un sistema para la gestión del tránsito, el cual tiene entre sus principales características el mantener comunicación con los controladores, obtención de datos de los puntos de detección y una estrategia de control entre otros.

La comunicación con los controladores le permite al sistema conocer el estado de los controladores así como modificar su programación. La obtención de datos de los puntos de detección permite obtener el estado o alarmas tanto de los controladores como de los puntos de detección. La estrategia de control permite que el software automáticamente pueda modificar los controladores y colocarlos en un modo especifico de operación.

[14] Estación de relevamiento y cuantificación de las variables de tránsito vehicular

6.5. Software de Supervisión Visual de Tránsito

Es un sistema compuesto por cámaras de video, que se encuentran distribuidas en intersecciones estratégicas y que son operadas desde el Centro de Control. Este sistema permite observar el comportamiento del tráfico en puntos principales de la red de vial.

Además de poder observar e identificar eventos importantes como congestión, accidentes, emergencias, incendios, etc,el sistema SSVT posee la posibilidad mediante software especializado en realizar conteo del volumen de tránsito, nivel de congestión, densidad y velocidad de circulación así como detección de incidentes.

6.6. Centro de Monitoreo

Estado de la Red Actualmente el Sistema Nacional de Tráfico Inteligente del país abarca únicamente la cabecera de las provincias de la Gran Área Metropolitana (San José, Heredia, Alajuela, Cartago), como medida de mitigación al gran flujo vehicular presente en estas zonas. Con la implementación de los semáforos inteligentes se busca disminuir la congestión en las principales rutas de estas ciudades y controlar de manera eficiente el tránsito, facilitando la labor de los oficiales de tránsito y a la vez reduciendo los tiempos de recorrido en carretera por parte de los usuarios y colaborando con la reducción de la contaminación causada por los automotores en el ambiente.

El sistema de control de los semáforos inteligentes se encuentra ubicado en San José, propiamente en el edificio del Centro de Control de Tránsito, donde actualmente se administra la red de semáforos inteligentes del país. La red presenta dos variantes de su medio de comunicación con la estación central, por un lado en la provincia de San José se realiza por medios alámbricos, específicamente un nodo principal en fibra óptica donde se conectan los demás semáforos de las calles por medio de cobre, este servicio es proveído por CNFL [15].

El diseño de esta red abarca todo el casco principal de la ciudad de San José, Pavas, Guadalupe, Uruca, San Pedro. La infraestructura de red en esta provincia se encuentra de manera subterránea por conductos propiedad de la CNFL. Este diseño cuenta con la particularidad de que en muchos de los municipios de la capital los cables eléctricos o bien de comunicación no se encuentran expuestos como se tenían anteriormente, por lo que el MOPT tuvo que ajustar su diseño con esta medida para cumplir con las normas establecidas.

Por otro lado en las provincias de Alajuela, Cartago y Heredia la comunicación con el Centro de Control se realiza de manera inalámbrica, siendo este servicio por medio de la red del ICE, a diferencia de la capital, el número de dispositivos en estas localidades es menor, adicionalmente la comunicación debe realizarse de manera inalámbrica ya que las instituciones que brindan servicios públicos en estas comunidades no son necesariamente instituciones del gobierno, por lo que al tratar de utilizar la infraestructura no gubernamental generaría un gasto mayor para el proyecto al tener que pagar alquiler para poder utilizar los medios de estas empresas.

[15] Del acrónimo Compañía Nacional de Fuerza y Luz

Los puntos de ubicación para estas provincias son los que presentan mayor congestión vehicular, por lo que se puede mencionar que la implementación de este proyecto aún no ha llegado con ímpeto a estos sectores y el alcance en carretera se enfoca en lugares con mayor flujo vehicular, donde el tráfico tiende a ser caótico en horas "pico" por lo cual existe la necesidad de controlar estos sectores, agilizar y gestionar tiende a catalogarse como necesaria dentro de estas zonas, a pesar que inicialmente la implementación de semáforos inteligentes del país se encuentra concentrado en la capital, los beneficios y crecimiento automotriz ha generado la necesidad de aumentar la actual red de semáforos, por lo que se desea implementar una segunda fase concentrándose en el área de circunvalación, con el objetivo de controlar todo el tráfico entrante y saliente del casco central dentro de la capital, y a su vez gestionar de manera ordenada y precisa la información necesaria que se desea exponer en carretera para que los usuarios se mantengan informados del tiempo promedio del trayecto y puedan optar por rutas alternas antes de verse atrapados por el tráfico en carretera.

Estado del Cuarto de Comunicaciones Dentro de la metodología empleada para la recolección de datos, se realizó una serie de visitas al Centro de Control de Tráfico del MOPT, como reconocimiento de territorio, donde se pudo comprobar las decadencias en infraestructura que presenta este recinto. Cuando se habla de infraestructura de red es importante que la seguridad sea tanto lógica como física, y los resultados obtenidos en la visita permiten afirmar que este perímetro no cuentan con las seguridades básicas que se requieren para un cuarto de comunicación, además no se contemplaron normas internacionales que permitieran seguir parámetros de diseño para el cuarto de comunicación.Dentro de los factores importantes que se infringen dentro del Centro de Control se pueden citar los siguientes:

- El cuarto de encuentra dentro de una habitación compartida con el taller de mantenimiento sin divisiones adecuadas para la separación de departamentos.
- No existen mecanismo de control de acceso al cuarto de comunicaciones.
- El cuarto de comunicaciones no cuenta con el diseño adecuado para albergar.
- No se observaron cámaras perimetrales para controlar el movimiento de individuos dentro del recinto.

7. Estado de la ciberseguridad

Antes de establecer el estado de la ciberseguridad en la Red de Semáforos Inteligentes del MOPT, es importante señalar que se construye tomando como referencia la metodología de PTF: PenTesting Framework de www.vulnerabilityassessment.co.uk, la cual permite la enumeración de vulnerabilidades riesgos que si llegaran a materializarse, podrían ocasionar una falla sistémica generalizada en la plataforma tecnológica que soporta la Red de Semáforos Inteligentes.

Por medio de la metodología de PenTesting Framework, se pudo realizar una planeación y preparación de pruebas de intrusión no disruptivas a los sistemas observados y es en esta fase donde se efectuaron las tareas de identificación y explotación de dichas vulnerabilidades.

En dicha metodología se establecen tres grande etapas para conducir una revisión sistémica de la ciberseguridad; las cuales al final permiten enumerar los principales riesgos de la Red de Semáforos Inteligentes del MOPT, las etapas son descritas a continuación:

1. Planeación y Preparación: Se enumeran los siguientes aspectos: fechas y tiempos límite, acuerdos legales (contratos de confidencialidad entre las partes, etc), definición de alcances, presentación del equipo de trabajo, plan de trabajo (cronograma). El plan de actividades se entrega al formalizarse la oferta como parte de la reunión de Kick Off.

2. Pruebas de Penetración: En esta fase se efectúan las tareas de identificación y explotación de dichas vulnerabilidades, es donde se ejecuta como tal las labores de análisis hacia los recursos tecnológicos de la infraestructura mas expuesta de la Red de Semáforos Inteligentes del MOPT. Esta fase a su vez tiene tres niveles:

- Reconocimiento y Obtención de Información por medio de búsqueda pasiva y activa de información técnica o no técnica que permita determinar puntos de ingreso a través de diversos mecanismos sean automatizados o manuales con el fin de capturar la mayor cantidad de datos relevantes de la infraestructura.
- Identificación de Vulnerabilidades por medio de scripts, herramientas licenciadas y abiertas que enumeran técnicamente los posibles eslabones débiles en la cadena de pruebas a efectuar con el fin de lograr determinar una vulnerabilidad que descubra una amenaza real que permita comprometer los activo tecnológico con los que cuenta el MOPT en la infraestructura.
- Ataques y Penetración controlada no disruptiva, es decir sin afectar la operación del servicio, la cual se ejecuta tomando como referencia los eslabones de seguridad encontrados con el fin de que permita obtener una respuesta controlada que pueda dar por un hecho que se perpetró un acceso no autorizado o la obtención de información clasificada como confidencial o dolosa a los intereses del MOPT y por ende del Estado costarricense.

3. Generación de Reportes: En esta fase se documentan todas las evidencias que se pudieron obtener de la fase anterior y es en esta parte del estudio donde se construyen las recomendaciones técnicas para cerrar las brechas de seguridad detectadas para que el MOPT o el contratista puedan implementarlas.

Las principales oportunidades de mejora encontradas son las siguientes:

7.1. Problemas que afectan la confidencialidad

La información técnica circulante en Internet en sitios de Gobierno como lo son CompraRed o la edición electrónica del diario La Gaceta, exponen datos valiosos como marcas, modelos de equipos, así como las especificaciones técnicas de los equipos adjudicados y por ende de la infraestructura que esta implementada a nivel de la Red Nacional de Semáforos.En la matriz Top-N de riesgos

encontrados en la visita de campo a la intersección La Valencia de Heredia, se pudo comprobar que los identificadores de red (SSID) se encuentra visibles y sin cifrado.

En la visita de campo a las instalaciones del MOPT se pudo comprobar lo siguiente:

- Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.
- Falta de conciencia acerca de la seguridad para los empleados que trabajan dentro del edificio.
- Falta de mecanismos de monitoreo, favoreciendo al procesamiento ilegal de los datos.

Toda esta información y omisiones en la configuración de la seguridad de los dispositivos de radio inalámbrico facilitaron mucho las etapas de reconocimiento y obtención de información y sirvió como la base fundamental para establecer un diseño de la infraestructura.

7.2. Problemas que afectan la disponibilidad

Como lo plantea el equipo de respuesta para el ciber crimen (ICS-CERT) el sistema operativo VxWork instalado en los controladores de semáforo inteligentes del MOPT dispone de una serie de vulnerabilidades conocidas que buscan materializar denegación de servicios gracias a que los servicios de depuración de errores se encuentran por defecto iniciados. Al estar el servicio de depuración habilitado se podría permitir un acceso completo a la memoria del dispositivo a un usuario remoto no autenticado. Por medio de un volcado de memoria se podría fácilmente revelar las contraseñas y la información de configuración. Un atacante podría utilizar el acceso de escritura para realizar ataques de denegación de servicio, o incluso ganar acceso total al controlador de semáforo y por ende efectuar manipulación de las luces del semáforo.

Un severo congestionamiento vial podría afectar la disponibilidad del servicio y causar efectos colaterales para el estado como lo son:

- Desperdicio de combustible, debido al alto flujo de tráfico vehicular.
- Interferir en el tránsito de vehículos de emergencia.
- Contaminación atmosférica por el exceso de gases emanados por los automóviles.
- Atrasos en el transporte, desplazamiento de empleados a sus hogares o trabajos, golpeando la salud de las personas y la reducción del tiempo efectivo para las actividades cotidianas.

Por otra parte, la manipulación de cámaras PTZ que conforman parte de la infraestructura de semáforos, podría derivar riesgos sistemáticos como restar control visual del nivel de tráfico en carretera, operativos policiales, entre otros. Así como el movimiento de las cámaras de posición hacia puntos focales ajenos a los que se desean controlar.

7.3. Problemas que afectan la integridad

La alteración de luces en el semáforo debido spoofing de sensores, o gran cantidad de datos enviado al controlador de semáforos, puede ser considerado un riesgo. Este se puede materializar durante eventos al aire libre que inyecten un alto volumen de tránsito vehicular en las intersecciones gobernadas por semáforos inteligentes. Por otra parte, la comunicación inalámbrica en banda ISM (de 900 Mhz a 5.8Ghz), la cual está implementada en los tramos inalámbricos de la infraestructura de red, deberá contemplar la técnica de Frecuency Hooping, que permite a los equipos de radio inalámbrico hacer saltos de banda aleatorios, haciendo por ende más difícil la tarea para que un ataque los pueda detectar. Si los equipos de radio no se configuran adecuadamente, es factible escanear el espectro de frecuencia y descubrir la infraestructura inalámbrica que se encuentra detrás de los APs deL MOPT, esto es posible desde una simple computadora portátil con una tarjeta inalámbrica Wifi.

Más a lo interno de la infraesctura, en el propio Centro de Monitoreo de la Red Nacional de Semáforos Inteligentes se detectaron los siguientes riesgos:

- Daño a los recursos resguardados en el edificio, por el ingreso de personal no autorizado a las áreas de acceso restringido o limitado, debido a la falta de controles de monitoreo automatizados del sistema de control de ingreso al edificio.
- Daño o pérdida de recursos de tecnología de información por incendio o inundación, debido a la falta de detectores de humo,humedad,temperaturas y extintores de incendio.
- Ingreso de personal no autorizado a través de puertas o ventanas que puedan ser violentadas fácilmente, causando daños o pérdidas en la información, equipo o recurso humano.
- Ingreso de personal no autorizado por la falta de puertas que cierren automáticamente luego de haber sido abiertas o por falta de alarmas sonoras, causando daños o pérdidas a la información o equipo.
- Pérdida de operatividad de los equipos, debido al uso no autorizado del equipo por falta de controles de acceso y monitoreo del centro de datos.

8. Recomendaciones

En relación a los resultados de este trabajo de investigación, se brindaran a continuación una serie de recomendaciones agrupadas en las categorías de Seguridad Lógica, Seguridad Física, Infraestructura Inalámbrica y Política de Gestión de la Seguridad.

8.1. Seguridad Lógica

En este apartado, se recomienda el cambiar la contraseña por defecto que traen los equipos que componen la red de comunicación, debido a que la mayoría de credenciales se encuentran disponibles en los manuales de usuario de

cada producto y estos son fácilmente accesibles mediante los sitios web de los fabricantes.

Adicional mente, es altamente recomendable contar con un plan de mantenimiento preventivo en el cual se actualice periódicamente el firmware de los dispositivos de la red de comunicaciones, debido a que los firmwares obsoletos poseen errores y vulnerabilidades conocidas que pueden ser explotadas por un atacante para ganar acceso al dispositivo, ademas el contar con un firmware actualizado provee siempre mejor estabilidad, seguridad y rendimiento por lo que se estaría disminuyendo la superficie de ataque.

Otro punto a considerar es realizar una encripcion del trafico que circula entre las diferentes intersecciones centralizadas y los equipos ubicados en el centro de control, de manera que si una persona no autorizada obtiene acceso a la red, no pueda ver el contenido de los paquetes que viajan en la red.

Uso de certificados (poco probable)

8.2. Seguridad Física

En cuanto a la seguridad física, iniciaremos con las instalaciones del Centro de Control de Trafico, para el cual se recomienda implementar una bitácora de acceso tanto al cuarto de servidores como al Centro de Monitoreo.

Es importante también adoptar medidas seguridad en los gabinetes que contienen los servidores y equipos de comunicaciones, los cuales deberán permanecer cerrados y bajo llave de manera que un usuario no pueda deliberadamente apagar o desconectar ya sea un servidor o equipo de comunicaciones.

8.3. Infraestructura Inalámbrica

La recomendación principal es realizar un hardening de la red inalámbrica, para lo cual podemos tomar en cuenta como elementos a proteger, el SSID, contraseña de la red, una red falsa.

Una etapa a implementar corresponde a no realizar el broadcast SSID o nombre de la red, de manera que no sea un elemento de entrada para el atacante.

Una segunda recomendación para el hardening de la red, corresponde a proteger con password el acceso a los enlaces inalámbricos, de manera que un equipo con una tarjeta de red inalámbrica no pueda fácilmente ganar acceso a la red.

8.4. Política de Gestión de la Seguridad

Adopción de un marco de gestión (Cobit / ITIL / ISO 27000)de la seguridad para la puesta en marcha de proyectos de infraestructura tecnológica.

9. Conclusiones

Dentro de los resultados encontrados en las pruebas realizadas durante la investigación, se evidenciaron una serie de vulnerabilidades que ponen en riesgo

los sistemas de control de tráfico inteligente del país, así como la continuidad de futuros proyectos dentro de esta red, dejando en evidencia la crítica situación que afronta el Ministerio de Obras Públicas y Transportes dentro de sus instalaciones, ya que no cuentan con las necesidades mínimas para albergar la administración de estos sistemas, por lo que es de suma importancia que las autoridades pertinentes tomen en consideración las recomendaciones brindadas para la mejora y fortalecimiento de la plataforma.

Referencias

Corporation, P. T. (2012, jan). Peek atc controller operating manual (4.ª ed.) [Manual de software informático]. (www.semex.com) pages 7

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., y Halderman, J. A. (2014, Aug). Green lights forever: Analyzing the security of traffic infrastructure. En *8th usenix workshop on offensive technologies (woot 14).* San Diego, CA: USENIX Association. Descargado de `https://www.usenix.org/conference/woot14/workshop-program/presentation/ghena` pages 7

MOPT. (2015). *Estructura organizacional* (Inf. Téc.). Ministerio de Obras Públicas y Transportes. (www.mopt.go.cr) pages 4

SEMEX, S. A. (2003). Controlador de semaforos serie c-200 modelos: C-208 - c-210 - c-216 [Manual de software informático]. (www.semex.com) pages 7

Semáforo. (2015). *Historia de semáforo* (Inf. Téc.). Wiki. (es.wikipedia.org/wiki/semaforo) pages 4