LOS ALGORTIMOS CRIPTOGRÁFICOS COMO RESPUESTA A LAS CIBERAMENAZAS EN IOT

Los Algortimos Criptográficos como respuesta a las Ciberamenazas en IOT

Flores Montaño Luis Alberto
Estudiante de Maestría en Informática SEPI UPIICSA
Email: luisfloresmontano@hotmail.com

Dra.Vicario Solorzano Claudia Marina
Profesor de Maestría en Informática SEPI UPIICSA
Email: marina.vicario@gmail.com

Dr. Álvarez Cedillo Jesús Antonio
Profesor de Maestría en Informática SEPI UPIICSA
Email: jaalvarez@ipn.mx

Resumen

Este artículo es un ensayo de reflexión acerca de la importancia de la ciberseguridad en la actualidad, en diferentes sectores de la sociedad, incluyendo los sistemas de cómputo y también los dispositivos del internet de las cosas, (que día a día tiene cada vez más relevancia en la vida cotidiana). Adicionalmente se hace énfasis a la importancia que implica desarrollar un algoritmo para defendernos de distintos ciberataques o ciberamenazas. Por otro lado, se hace un recuento de diversas organizaciones internacionales, acerca de cómo se está tomando en cuenta el tema de seguridad y que se ha hecho al respecto sobre esto; a pesar de los esfuerzos de dichas organizaciones, no se ha podido hacer nada para seguir evitando los ciberataques, si no que al contrario año con año han aumentado los casos de virus informáticos que atacan a todo tipo de sistema de cómputo, incluyendo al Internet de las cosas (IoT).

I. Introducción

Una nueva ola de avances tecnológicos en la comunicación inalámbrica está haciendo posible un ecosistema dinámico de dispositivos conectados diseñados para mejorar la forma en que vivimos y trabajamos.

El Internet de las Cosas (IoT) implica información enlazada a redes integradas por sensores y otras tecnologías incrustadas en objetos físicos, como refrigeradores, medidores electrónicos, etiquetas electrónicas, sistemas de automatización del hogar, etc. Algunas estimaciones sugieren que El Internet de las Cosas podría conectar hasta 50 billones de dispositivos o aproximadamente seis dispositivos por persona en el planeta.

IoT es el dominio de la aplicación de comunicaciones máquina a máquina (M2M), y proporciona la "plomería" o conectividad que habilita el ecosistema IoT; como se verá en el ensayo la conectividad es de gran relevancia en temas que se tocan dentro de diversas conferencias y

organizaciones nacionales e internacionales, para una mejora en la calidad de vida dentro de la comunidad.

Los expertos anticipan que la mayor parte de esta nueva conexión en el M2M; dependerá del entorno de la tecnología inalámbrica.

Las empresas de toda la industria inalámbrica compiten por desarrollar e introducir nuevos usos de M2M que enriquezcan nuestros recursos personales y vida laboral. Al mismo tiempo, la sensibilidad de los datos involucrados en la entrega de soluciones M2M hace que la privacidad y la seguridad sean una prioridad para el continuo el crecimiento del mercado M2M. Garantizar la seguridad es monumentalmente importante para el éxito de los servicios M2M.

Por esta razón las empresas del ecosistema M2M están trabajando para mantenerse a la vanguardia ante amenazas a la seguridad de los datos. Estos avances han dado hincapié a un nuevo ámbito de hostilidades en el ciberespacio, como es el robo de identidad y amenazas a la privacidad de cada individuo, para propósitos delictivos o sabotaje. Esta nueva amenaza global apunta a la seguridad de los Estados.

> *La amenaza es más sofisticada, más sutil, no usa armas ni municiones ni ejércitos, pero es capaz de someter gobiernos, quebrar economías y desquiciar tanto a grupos sociales como a cualquier persona* (Badillo, 2011).

La seguridad informática ha cobrado relevancia, para prever ataques informáticos (robo de información sensible y amenazas de la privacidad) dentro del ciberespacio, ante la fuerza destructiva de novedosas herramientas informáticas inteligentes.

II. Contenido del artículo

El acceso a la información y sus consecuencias sobre el uso del internet es un tema de interés para diferentes cumbres como es el caso de la Cumbre Mundial sobre la Sociedad de la Información (Por sus siglas en inglés-WSIS) de las Naciones Unidas, el plan de acción nacional o cumbres de la OCDE. Acorde a estas cumbres de diferentes organizaciones el internet ha tenido su mayor auge en las últimas dos décadas a consecuencia de esto surge una problemática acerca de que tan seguro es navegar por el ciberespacio, sin el problema de sufrir una falla en cuanto a la implementación de la seguridad.

El tema de seguridad informática ha sido tema para discutir en los últimos años, ya que acorde con WISIS y la OCDE, el acceso a la internet, debe ser discreto y confiable, al momento de introducir información personal, ya sea de texto o media; no importando el sistema operativo, plataforma, aplicación o página web que se esté usando.

Por otro lado, tenemos los principios de Geneva también de (WSIS), la cual menciona que

> *La comunicación es un proceso social fundamental, una necesidad humana básica y el fundamento de toda organización social; en la cual todos puedan crear, consultar, utilizar y compartir la información y el conocimiento* (WSIS, 2003).

Así, las tecnologías de la información y la comunicación (TIC) tienen inmensas repercusiones en prácticamente todos los aspectos de nuestras vidas, y se espera que en un futuro próximo el internet de las cosas tenga un impacto similar y tal vez mayor; con el fin de un progreso económico y social de los países y bienestar de la comunidad. Adicionalmente la declaración de principios enfatiza el tema de seguridad informática como una prioridad, es decir el fomento de un clima de confianza, incluyendo la seguridad de la información y la seguridad de las redes, la autenticación, la privacidad y la protección de los consumidores, para promover la confianza entre los usuarios de las TIC; ya que se considera necesario evitar que las tecnologías y los recursos de la información se utilicen para fines criminales o terroristas, respetando siempre los derechos humanos por ejemplo WSIS actualmente considera el envío masivo de mensajes electrónicos no solicitados ("spam") como uno de los problemas de ciberseguridad para los usuarios. Un claro ejemplo de un problema con los correos spam y que es conveniente abordar, son los diversos tipos de virus pueden ser enviados por medio de los correos electrónicos. Es de suma importancia cuidar los correos denominados spam, para evitar riesgos ante ciertas situaciones, por ejemplo lo ocurrido en el presente año (2017); la empresa Telefónica, declaró públicamente que un virus fue esparcido, a través de un correo electrónico el cual fue abierto; posteriormente infiltrándose por los equipos de esta empresa, destacando también que diversas empresas les ocurrió algo muy similar, dicho virus fue bautizado con el nombre de WannaCry; el cual infecto a miles de dispositivo a nivel global.

Por otro lado, la Estrategia Digital Nacional, la cual se ha denominado también como un plan de acción, pretende implementar la construcción de un México Digital en donde la tecnología y la innovación contribuyan a alcanzar las grandes metas de desarrollo del país. Este también destaca la cooperación entre gobiernos y el sector privado para detectar y responder ante la ciberdelincuencia, fortaleciendo de esta forma el marco de confianza y seguridad con iniciativas complementarias y de apoyo mutuo en los ámbitos de la seguridad en el uso de las TIC, con iniciativas en cuanto a el derecho a la privacidad y la protección de los datos de los consumidores.

De esta forma se estaría apoyando la economía (en términos digitales), como es el caso del desarrollo en el mercado de bienes y servicios digitales, un claro ejemplo de esto es el Bancomer Móvil, una aplicación donde un usuario con cuenta Bancomer puede checar el estatus de sus estados de cuenta, movimientos y hacer transacciones, relacionando esto con la ciberseguridad, se toma como prioritario en dispositivos móviles; ya que el robo de identidad o alteraciones en cuentas bancarias serían de gran repercusión para los usuarios, por lo que ocasionaría una fuerte perdida en términos económicos, adicionalmente ocasionando desconfianza ante los usuarios de usar los dispositivos móviles, para este tipo de acciones.

Otro punto de este plan de digitalización en el país es impulsar el intercambio de información de los Sistemas de Información de Registro Electrónico para la Salud, entre los que se encuentran los Expedientes Clínicos Electrónicos, para apoyar la convergencia de los sistemas de información de salud, entre ellos está el dispositivo conocido como "health patch" el cual es un parche , considerado un dispositivo del Internet de las Cosas, el cual permite obtener información acerca del paciente, como son los pulsos vitales, del corazón, y analizar la situación de salud en el que se encuentra el individuo; con este producto en términos de ciberdelincuencia se pudiera manipular los expedientes clínicos ya que el dispositivo haciendo uso de la red, puede ser crackeado para fines "delictivos", o simplemente para jugar alguna clase de broma, por lo que de antemano se debe prever esta situación ya que cualquier error en el registro médico puede ser vital para cualquier persona. A todo esto, el proyecto el cual está familiarizado puede ayudar a encriptar la información que se manda, y así la información podría ir por un canal mucho más seguro aún.

Las cibertendencias también involucran el cambio de paradigma en cuanto a las defensas y ataques, dentro del gobierno de un territorio nacional, como es el caso de China y Estados Unidos, los cuales tienen una guerra no con armamento si no con ataques de hackeo constante en el ciberespacio, por lo que esto puede ser aún más devastador para un país si es que se llega infiltrar información sensible.

Algo parecido pero con menos gravidez es el caso de los empresarios y compradores vía online ya que, al realizar este tipos de compras, se beneficia a una empresa con la venta de sus productos, y no solo a empresas sino también a personas comunes que a diario suben productos como dispositivos informáticos, utensilios del hogar , automóviles y hasta casas, que quieren vender o en el caso del último ejemplo que quieran rentar, en plataformas de servicio web como es el caso de Mercado Libre , E-bay , Amazon entre muchas otras plataformas, este tipo de comercio se define más claramente en el libro de las 7 cibertendencias del siglo XXI de C. M. Martín*;* donde menciona que *"los productos se convierten en mercancías; el cliente se convierte en datos; por lo tanto surgen comunidades de experiencia y el aprendizaje se lleva a cabo en tiempo real; todo esto antes mencionado está basado en la cibereconomia, como se ha clasificado en los últimos años"* (Martin,1999). Como dato adicional, se tiene que el internet logró 50 millones de usuarios en 4 años. Considerando al mercado bastante amplio y contando con gran cantidad de usuarios, existiendo una sincronización y comportamiento de consumo corporativo que ha hecho posible el desprendimiento de la información.

A todo esto, de la cibereconomía y la ciberseguridad se prevé que en el próximo año (2018) **la propiedad y el acceso a *los datos o metadatos "se conviertan en puntos de debate y de verdadera discordia"*** (DIR&GE, 2016)**.**

Otras cibertendencias en este mercado que marcarán el futuro próximo y que además se consideraron pertinentes para la elección de tema de tesis *en cuanto a ciberseguridad del Internet de las Cosas son:*

- **El impulso de la inteligencia de la seguridad cibernética como elemento predictivo.** El sector de la ciberseguridad está continuamente innovando, por lo que permanece reactivo, siendo la seguridad en la red más predicativa.
- **El Internet de las Cosas, es fuente del Big Data.** *Big Data se va actualizando de manera progresiva en gran medida gracias a El Internet de las Cosas. Esta tecnología permite examinar patrones específicos sobre resultados, en tiempo real.*

Finalmente, una organización importante que se tiene a nivel mundial es "La Organización para la Cooperación y el Desarrollo Económico" (OCDE), que agrupa a 35 países miembros y su misión es promover políticas que mejoren el bienestar económico y social de las personas alrededor del mundo. La OCDE, menciona que el Internet ha crecido y difundido rápidamente en todo el mundo, con importantes beneficios a las economías y sociedades. La información que proporciona esta organización, y al igual que otras que se mencionaron anteriormente, muestran que en efecto el internet mejora la economía, y que adicionalmente es importante la confianza y la seguridad por la que se tienen que ir los cibernautas.

La Reunión sobre la Economía Digital, hace hincapié en continuar el diálogo y mantener a las naciones en movimiento hacia adelante, juntos, en esta era digital, por lo que se enfocan en 4 puntos importantes; La apertura de internet, Trabajos y habilidades, La conectividad Global y finalmente la Confianza (refiriéndonos a la innovación digital); como este ensayo se enfoca a la seguridad del Internet de las Cosas, se toma más a fondo la parte de Conectividad Global y a la Confianza, , ya que este último pretende conectar todos los dispositivos que se utilizan a diario, en nuestras actividades cotidianas , y adicionalmente habla de la confianza ya que existen diversas personas, que no confían plenamente en hacer pagos o compras por medio del internet, o en otras palabras, hacerlo de una forma digitalizada, como es el caso de mandar solicitudes de compra o de pago. La confianza en la economía digital permite una mayor cooperación para proteger a los consumidores y gestionar los riesgos de privacidad y seguridad.

Con el aumento de la interconexión, se ha desarrollado un mercado de comercio electrónico dinámico e innovador, ya que *los consumidores han desempeñado un papel más activo, y de esta forma ha surgido una economía de compartir* (OECD, 2016).

Pero a medida que estos mercados en línea crecen y el paisaje para los consumidores se vuelve más complejo, la regulación y los desafíos de la protección del consumidor están surgiendo. La provisión de protecciones de consumidores bien adaptadas puede fomentar la confianza y proporcionar la oportunidad para que el mercado en línea, incluyendo la economía compartida, prospere. Así la creciente interdependencia en red de nuestras sociedades, las preocupaciones de privacidad y seguridad son más frecuentes que nunca y se convertirán en un diferenciador competitivo. Los gobiernos y las empresas pueden establecer las condiciones para una mayor cooperación en el desarrollo e implementación de marcos de gestión de riesgos de privacidad y seguridad que estén alineados con la visión estratégica económica y social para la economía digital.

Así, la meta principal de OCDE es estimular el uso de las tecnologías digitales mediante la creación de los marcos adecuados de inversión y políticas para apoyar la innovación y el crecimiento, en particular entre las PYME, así como la prosperidad social, al tiempo que se minimizan los impactos sobre el empleo.

III. Conclusiones

Se concluyó que queda mucho trabajo por hacer en el área de la seguridad en general no solo de las IOT, tanto por vendedores como por usuarios finales, y también por instituciones gubernamentales y no gubernamentales. Es importante que para los próximos estándares se deba abordar las deficiencias de los mecanismos actuales de seguridad de IoT. Como trabajo futuro para todas las organizaciones y conferencias que atienden los temas de digitalización, el objetivo debe ser obtener una comprensión más profunda de las amenazas que enfrenta la infraestructura de IoT, así como identificar la probabilidad y las consecuencias de las amenazas contra las IoT; definiciones de mecanismos de seguridad adecuados para control de acceso, autenticación, gestión de identidad y un marco de gestión de confianza flexible ser considerado en el temprano desarrollo del producto de digitalización.

Se espera que este ensayo sea útil para hacer énfasis a identificar los principales problemas en la seguridad de IoT y proporcionar una mejor comprensión de las amenazas y sus atributos que provienen de varios intrusos como organizaciones y agencia de inteligencia.

Referencia y Recursos Electrónicos

1. Miguel A. Badillo, (2011). http://www.contralinea.com.mx/archivo-revista/2011/08/07/guerra-cibernetica-la-nueva-amenaza/
2. DIR&GE,(2016).http://directivosygerentes.es/digital/articulos-digital/las-tendencias-del-sector-tic-2017
3. Chuck Martin, (1999). Las 7 ciber tendencias del siglo xxi, McGrawHill
4. OECD, (2016). http://www.oecd.org/internet/ministerial/
5. WSIS, (2003). http://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en&id=1161|0