Problemas recientes en la ciberseguridad robótica

Mtro. Flores Montaño Luis Alberto
luisfloresmontano@hotmail.com

Mtra. Esther Viridiana Vázquez Carmona
evazquezc1801@alumno.ipn.mx

Mtro. Rodrigo Vázquez López
rodrigo_em2@hotmail.com
Dr. Juan Carlos Herrera Lozada
jlozada@ipn.mx

Instituto Politécnico Nacional
Centro de Innovación y Desarrollo Tecnológico en Cómputo

Resumen

Hoy en día la ciberseguridad no tiene una alta prioridad durante el diseño y la fabricación de todo tipo de sistemas robóticos, a diferencia de los sistemas embebidos o integrados como se les conoce, a estos últimos se le ha dado mayor prioridad en cuanto a costos de desarrollo y funcionalidad dirigida los consumidores. Sin embargo, la fabricación de sistemas robóticos continúa creciendo en toda la industria, como es el caso de robots destinados al cuidado de los adultos mayores, o para fines militares, manufactureros, médicos, y en los mercados de ensamblaje automotriz; por lo que, en un futuro cercano, se deberá prestar más atención a la ciberseguridad robótica. Esta investigación identifica las ciberamenazas actuales y potenciales que pueden ser aplicados a los sistemas robóticos, siendo más específico en las amenazas del hardware, firmware /sistemas operativos y niveles de aplicación; finalmente, se identifican escenarios de ataque en los componentes ya mencionados.

Summary

Today cybersecurity is not a high priority during the design and manufacturing of all types of robotic systems, unlike embedded or embedded systems as they are known, the latter have been given higher priority in terms of consumer driven development and functionality. However, the manufacture of robotic systems continues to grow throughout the industry, as is the case of robots intended for the care of the elderly, or for military, manufacturing, medical, and automotive assembly markets; therefore, in the near future, more attention should be paid to robotic cybersecurity. This research identifies current and potential cyber threats that can be applied to robotic systems, being more specific on hardware, firmware / operating system threats and application levels; finally, attack scenarios are identified in the aforementioned components.

Keywords: Palabras clave: Ciberseguridad, ciberataque, economía, pandemia, hardware, firmware.

I Introducción

Los robots se han utilizado en la fabricación durante más de 50 años. La firma de automóviles General Motors utilizó por primera vez el robot llamado “Unimate” en 1961, para ayudar en la producción de automóviles; desde entonces, las aplicaciones robóticas han sido explotadas en la fabricación hasta la actualidad. Cabe destacar que en la última década los robots son utilizados cada vez más para aplicaciones que benefician la vida diaria, como es el caso de drones que resguardan seguridad y defensa de algunas naciones. También existe la distribución de suministros y bienes utilizando drones, tal como la empresa Amazon planea implementar en un futuro cercano. Otro ámbito que hay que tomar en cuenta es el uso de robots para atención médica y de ancianos, para esto, empresas como Tesla y Google han estado investigando y desarrollando vehículos automatizados.

Un análisis de 280 empresas por parte del Departamento de Comercio en Competitividad de los Estados Unidos mostró una tasa de crecimiento del 20 % en promedio del uso de sistemas robóticos destinados a la fabricación, servicios y atenciones médicas; también han tenido una tasa de crecimiento de 72 % en los mercados de asistencia sanitaria y de personas mayores. Basándose en estas estadísticas, es claro que la robótica es una industria que está creciendo rápidamente y por lo tanto el uso de robots continuará volviéndose cada vez más esencial en la vida cotidiana.

Debido al incremento del uso de sistemas robóticos, los fabricantes deben de enfocarse en la ciberseguridad de estos, específicamente durante la etapa de diseño. Otros fabricantes de sistemas, como los de sistemas embebidos, sí implementan una seguridad más eficiente, con una alta prioridad en los costos de desarrollo, velocidad de comercialización, y proporción de características a los clientes.

La ciberseguridad es una baja prioridad en los sistemas robóticos debido, en parte, a que la seguridad no es una consideración principal para diversos clientes; estos últimos valoran más el costo, la usabilidad, las características y la funcionalidad de los mismos. Sin embargo, debido a su interacción directa con los seres humanos, en la robótica se debe exigir aplicaciones más seguras que en otros sistemas conocidos.

Este documento se enfoca en la identificación de amenazas potenciales y actuales de los sistemas robóticos, tomando en cuenta su impacto en la economía y en la seguridad humana; posteriormente se consideran algunas sugerencias para mediar ante las amenazas ya mencionadas. También se presenta una categorización de distintos niveles de ciberataques en sistemas embebidos y un análisis de cómo estos pueden afectar en aplicaciones robóticas. Por otro lado, se ejemplifican posibles escenarios donde los sistemas robóticos son parte de los ciberataques, como lo pueden ser drones y vehículos automatizados, y como a su vez perjudican a la manufactura robótica destinada al cuidado de ancianos. Posteriormente, se describe el impacto de ciberataques tanto a nivel económico como en la seguridad humana. Finalmente, se sugieren posibles contramedidas para evitar los ciberataques a robots.

II Categorización de ciberataques en sistemas embebidos

Ün sistema embebido es un sistema informático el cual está integrado en un sistema más grande, diseñado para funciones específicas; estos sistemas consisten en una combinación de hardware, software y de partes mecánicas”.

”Los sistemas robóticos se pueden definir como una combinación de estructuras mecánicas, sensores, actuadores y software de computadora que gestiona y controla estos sistemas”.

Por lo tanto, se puede considerar que los sistemas robóticos son un tipo de sistemas embebidos que pueden ser susceptibles a los ciberataques dirigidos contra estos. En este documento, los ataques a sistemas embebidos serán clasificados en función de la capa de destino de la arquitectura de estos sistemas, como es el caso de: hardware, firmware / sistema operativo y aplicación.

A. Ataques de hardware

Los sistemas embebidos son vulnerables a los ataques de hardware, cuando se fabrican, y en el campo de uso. Los ataques más comunes en hardware son los “backdoor”, troyanos, y “fault injection”.

Los sistemas robóticos también son susceptibles a ataques de hardware tanto en tiempo de producción cómo durante su uso. Al igual que con otros sistemas embebidos, los sistemas robóticos son producidos en masa para reducir costos; esto da oportunidad a que atacantes puedan realizar ingeniería inversa en los componentes y posiblemente insertar troyanos en el hardware durante el proceso de fabricación. Los atacantes también podrían agregar “kill switches” o hardware “backdoor” nivelados para obtener acceso a estos sistemas mientras estén en uso [6].

B. Ataques de firmware / sistemas operativos

En la mayoría de los sistemas embebidos, el código de firmware se almacena en la memoria flash para permitir actualizaciones en el sistema operativo de forma remota a través de los controladores de internet, teniendo así, un sistema operativo con vulnerabilidades de distintos tipos.

Los sistemas embebidos tienen sistemas operativos que son susceptibles a ataques, tal es el caso del sistema operativo Linux, el cual se ha demostrado que es vulnerable a ataques, como la denegación de servicios, la ejecución de código y acceso de nivel raíz del sistema. Un ejemplo de esto se informó en septiembre de 2016 cuando los piratas informáticos usaron 1.5 millones de dispositivos que en su mayoría eran cámaras de seguridad, con el propósito de formar una Botnet y realizar un ataque DDoS en KrebsonSecurity.com. Los atacantes aprovecharon una vulnerabilidad en la raíz o “root” en el sistema operativo Linux, el cual permitió el control total en los dispositivos.

C. Ataques de aplicaciones

Los sistemas embebidos también contienen programas de software para realizar tareas específicas. Algunos ataques comunes a nivel de aplicación son los virus, gusanos, software troyanos y desbordamiento de búfer.

Los sistemas embebidos también contienen programas de software para realizar tareas específicas. Algunos ataques comunes a nivel de aplicación son los virus, gusanos, software troyanos y desbordamiento de búfer.

III Ejemplos de aplicación de ataques a robots

Este documento presenta cuatro variedades de robots: a) Para el cuidado de ancianos, b) Vehículos automáticos, c) Drones militares y d) Fabricación. Para cada tipo de sistema robótico, se discuten los distintos tipos de ataques y los escenarios que posiblemente tengan estos sistemas.

A. Robots para el cuidado de ancianos

En un futuro, los robots residirán en distintos hogares, con distintos propósitos; uno de suma importancia es el cuidado de ancianos o robots de asistencia a domicilio. Estos robots de cuidado de ancianos como el Care- O-Bot [10] serán los responsables de realizar diversas tareas del hogar, como es el caso de la asistencia de movilidad y desempeño de mantenimiento. Además, estos tipos de robots pueden comunicar el estado de salud con los médicos, distribuir medicamentos programados y notificar al personal de emergencia cuando se necesite dicha asistencia.

Debido a su presencia física en el hogar, estos robots necesitarán el más alto nivel de seguridad con respecto a los ciberataques. Las posibles motivaciones para un ataque cibernético contra un robot de cuidado de ancianos van desde mostrar las habilidades que puede tener un atacante, hasta motivos más específicos, como el de obtener beneficios o información de una persona (a cuánto asciende su herencia, por ejemplo), o bien monitorear a su usuario en busca de datos sensibles como la información de sus tarjetas de crédito o cualquier tipo de robo de identidad. Para ello, se podría manipular el control de un robot a través de ataques informáticos, provocando de esta manera daños e incluso muerte al usuario; adicionalmente, la persona responsable de esto podría estar libre de cualquier tipo de sospecha.

Escenario de ataque: considerando que una persona mayor vive sola, la función principal de un robot de cuidado es permitir que la familia del usuario pueda monitorearse y localizarse en caso de una crisis médica o de salud. El robot está conectado a la internet a través de una red inalámbrica del hogar y equipada con una cámara de video, micrófono y altavoz para que la familia pueda ver y comunicarse con el usuario. Un atacante con motivación financiera podría realizar un ataque de nivel aplicación para introducirse a la red doméstica y así buscar la dirección IP del robot, accediendo así al nombre de usuario y contraseña entrada. Posteriormente usando un ataque de desbordamiento de búfer, el atacante podría usar la entrada del inicio de sesión para desbordar la pila con código malicioso e insertar una dirección de retorno que apuntará a un código malicioso.

Una vez ejecutado, el atacante podría tener el control total del robot. y luego sería libre de monitorear a la víctima a través de la cámara o micrófono buscando información como datos de tarjeta de crédito para ser utilizado con fines de lucro.

B. Vehículos automatizados

El 29 de septiembre de 2016, en el estado de California, Estados Unidos, se aprobó un proyecto de ley que permite la prueba de vehículos autónomos donde un humano no requeriría un controlador

como respaldo, como es el caso de un volante, pedal de freno o acelerador. Por lo tanto, pronto habría robots operando de forma autónoma en las vías públicas de ciertas ciudades; sin embargo, los cibercriminales podrían estar fuertemente motivados a cometer ataques críticos a este tipo de infraestructuras robóticas; por lo que, una vez que sean ampliamente utilizadas estas infraestructuras, podrían tener una consecuencia de amenaza potencial; teniendo por ejemplo, las calles congestionadas y vehículos que podrían usarse para atacar directa o indirectamente a miembros del gobierno.

Escenario de ataque: Los propietarios de un auto "Tesla motors" reciben un aviso de tráfico en una carretera federal, teniendo una alerta de reparación ya que se tiene una alerta de posible causa de incendio; una vez advertido esto, "Tesla motors" pudo completar la reparación de unos 29,222 vehículos, todo esto a través de actualizaciones de software.

La capacidad de "Tesla motors" para realizar este tipo de actualizaciones de software a sus vehículos crea a su vez un potencial ciberataque a nivel de firmware / sistema operativo. Un ataque hipotético podría involucrar un enfoque de dos fases donde un atacante primero obtiene acceso al fabricante, específicamente en el sistema de actualización de aire, y, posteriormente la obtención de una versión corrupta del firmware del vehículo, permitiendo así, el control remoto sobre el vehículo, para posteriormente obtener el control sobre toda una legión de vehículos automatizados.

C. Drones militares

Los drones militares son vehículos aéreos no tripulados (en inglés UAV) controlados remotamente por un piloto. Pueden usarse para monitorear y atacar objetivos enemigos. Así, en enero del 2014, el ejército de EE. UU. informó que tenía 7,362 "Ravens", 990 "WASPs", 1,137 pumas, 306 T-Hawks pequeños, también conocidos como UAS (sistemas de aeronaves no tripuladas), 246 depredadores y águilas grises, 126 "reapers", 491 "shadows y 33 Global Hawks. Esto equivale a un pequeño ejército de robots de control a distancia o no tripulados, siendo así un elemento de gran interés para los enemigos de los EE. UU. ya que el fin de dichos enemigos es desarrollar ciberataques contra los vehículos remotos o no tripulados, provocando consecuencias mortales por parte de los robots que transportan misiles y municiones.

Escenario de ataque: Suponiendo que una operación militar está siendo realizada por el gobierno chino, al sur de dicho país y, por otro lado, el ejército de los EE. UU. está monitoreando las acciones militares del gobierno chino, todo esto a través de drones. Suponiendo que algunos de los drones fueron fabricados por un proveedor chino el cual fue aprobado por el ejército americano. Adicionalmente, con el fin de reducir costos se subcontrató a una empresa china para los componentes de los microcontroladores. Todo esto puede provocar un ataque potencial de un hardware, donde un atacante chino tiene la oportunidad de introducir un "backdoor" o un troyano durante la producción.

Suponiendo que el atacante agregó un interruptor de interrupción de operaciones. que está habilitado cuando se detectan ciertas coordenadas en el GPS. Por lo que, a través de la suplantación de este último los atacantes podrían desactivar los drones.

D. Fabricación de robots

Los robots son comunes en la fabricación de todo tipo de industria; recientemente en un artículo en línea del Wall Street Journal informó que en el año 2014 hubo cerca de 1.6 millones de robots industriales en operación en todo el mundo. Y se proyecta que ese número crecerá en años venideros, representando así una gran parte de actividades laborales de fabricación realizadas por robots.

Los ciberataques contra sistema robóticos industriales pueden ser económicos o motivados por un actor extranjero interesado en interrumpir cadenas de suministro, causando caos económico. Las consecuencias de un ataque prolongado de una armadora, ya sea automovilística o del procesamiento de alimentos, podría ser de gran gravedad.

Escenario de ataque: suponiendo la situación de un sistema de fabricación con robots para una instalación de procesamiento de pan, responsable de envasar este producto. La instalación utiliza un mínimo de trabajo humano y un PLC para controlar los robots. Los PLC reportan datos comerciales a un servidor a través de "modbus". El atacante es un gobierno extranjero preparándose para la guerra contra los EE. UU.; realizando un ataque militar, el actor extranjero quiere causar caos económico e interrumpir el suministro de alimentos a las tropas militares.

Un método combinado de ataques como Stuxnet han sido planeados por varios años. Eso comienza con un correo electrónico infectado enviado a una recepcionista corporativa que instala malware en la

red corporativa al abrir el correo, el malware permitirá acceso al atacante, así como la capacidad de buscar la red y el servidor recopilando los datos empresariales. Posteriormente el malware permitiría al atacante, comenzar un ataque a nivel de aplicación que utiliza las comunicaciones “modbus” entre el servidor y los PLC; después de esto se podrían escribir datos de control en el PLC, provocando que los robots destruyan los brazos robóticos. Finalmente, el resultado de todo esto, provocaría la detención del proceso, y a su vez el suministro de pan sería interrumpido hasta el momento en que las instalaciones se pusieran en línea nuevamente.

IV. Conclusiones

En este artículo, se presenta una categorización con el objetivo de identificar ciberataques comunes en sistemas embebidos y aplicados en robots. Usando esta categorización, se discute de los distintos ataques cibernéticos contra robots, así como escenarios de ataque en robots para el cuidado de ancianos, drones, vehículos automatizados y fabricación. También se da una perspectiva del impacto económico que se tendría en la fabricación y la cadena de suministro debido a ciberataques provocados, comparándolos a su vez con los efectos del absentismo laboral como los de una pandemia. Finalmente, se describe el impacto de la seguridad humana debido a un ciberataque, con respecto al transporte militar y robots en el cuidado de ancianos.

Referencia y Recursos Electrónicos

1. Hockstein N., Gourin C., Faust R., and Terris D.J. (**2007**). *A history of robots: from science fiction to surgical roboticsJournal of robotic surgery, vol. 1* no. 2, pp. 113–118.

2. Christensen H. I., Batzinger T., Bekris K., Bohringer K., Bordogna J.,. Bradski G, Brock O., Burnstein J., Fuhlbrigge T., Eastman R. et al (**2009**). *A roadmap for us robotics: from internet to robotics-Computing Community Consortium*

3. Mirjalili S. H. y Lenstra A. K., (**2008**). *Security observance throughout the life-cycle of embedded systemsin Proceedings of the 2008 International Conference on Embedded Systems and Applications*ESA 2008, pp. 186–192.

4. Papp D., Ma Z., y Buttyan L., (**2015**). *Embedded systems security: Threats, vulnerabilities, and attack taxonomyin Privacy, Security and Trust (PST), 2015 13th Annual Conference on. IEEE*145–152.

5. Morante S., Victores J. G., y Balaguer C., (**2015**). *Cryptobotics: Why robots need cyber safetyFrontiers in Robotics and AI* vol. 2, p. 23

6. Wang X., Mal-Sarkar T., Krishna A., Narasimhan S., y Bhunia S., (**2015**). *Software exploitable hardware trojans in embedded processorin Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012 IEEE International Symposium on. IEEE*pp. 55–58.

7. Elmiligi H., Gebali F., y El-Kharashi M. W (**2016**). *Multi-dimensional analysis of embedded systems securityMicroprocessors and Microsystems*vol. 41, pp. 29–36

8. Franceschi-Bicchierai L. (**2016**). How 1.5 million connected cameras were hijacked to make an unprecedented botnet[En línea]. Disponible: https://motherboard.vice.com/read/15-millionconnected- cameras-ddos-botnet-brian-krebs

9. Falliere N., Murchu L. O., y Chien E(**2011**). *W32. stuxnet dossier," White paper, Symantec CorpSecurity Response*vol. 5, p. 6.
Hans M., Graf B., y Schraft R (**2002**). *Robotic home assistant care-o-bot: Past-present-future in Robot and Human Interactive Communication, 2002. Proceedings. 11th IEEE International Workshop on. IEEE*2002, pp. 380–385.

10. Baron E (**2016**). Fully autonomous cars get lift from gov. jerry brown.[En línea]. Available: http://www.mercurynews.com/2016/09/29/fullyautonomous-self-driving-cars-get-lift-from-governor/

11. Brisbourne A., (**2014**).Teslas over-the-air fix: Best example yet of the internet of things?Wired. http://www. wired. com/insights/2014/02/teslas-airfix-best-example-yet-internet-things.

12. Osborn K (**2014**).Pentagon plans for cuts to drone budgets.Available http://www.dodbuzz.com/2014/01/02/pentagonplans- for-cuts-to-drone-budgets

13. Peterson S. y Faramarzi P., (**2011**). *"Exclusive: Iran hijacked us drone, says iranian engineer (video-Christian Science Monitor*Dec, vol. 15.

14. Hagerty J. (**2015**). *Meet the new generation of robots for manufacturingWall Street Journal* pp. 3–4.

15. Frase P. (**2016**). *Class struggle in robot utopiain New Labor Forum*vol. 25, no. 2. SAGE Publications, pp. 12–17.

16. Frey T. (**2013**). *Hi, i'm a robot and i'm here to take your jobJournal of environmental health*vol. 76, no. 2, p. 46

17. Ford M. (**2015**). *Rise of the RobotsTechnology and the Threat of a Jobless Future*Basic Books