Seguridad informática de un sistema basado en ontología de control vía Web de dispositivos domóticos

Informatic security of a based system on control ontology via web of domotic devices

Luis Vladimir Urrelo Huiman[1]

Recibido: 02 de noviembre de 2015
Aceptado: 18 de diciembre de 2015

Una ontología puede mantener reglas de inferencia en un servidor web para controlar remotamente sistemas de automatización de viviendas, conocidos como sistemas domóticos, pero cuenta con falla en la seguridad informática debido a que expone conceptos y relaciones que representan los elementos reales. Para mitigar este riesgo es necesario asegurar la data y estructura de la ontología y su comunicación con un controlador central de un sistema domótico, siendo una alternativa el mantener un criptosistema simétrico. Pero debemos estudiar los componentes de un sistema domótico, los conceptos de ontología domótica, así como las técnicas que podrían aplicarse para asegurar una ontología controladora vía web de un sistema domótico.

Los sistemas domóticos son un conjunto de sistemas de automatización de una vivienda con fines de gestión energética, seguridad, bienestar y comunicación; integrados por controladores, actuadores y sensores. (Carrero Vázquez, 2013, p. 190), pudiendo ser gestionados remotamente desde un servidor web, tal y como lo afirman García Sánchez y Moreno Martín (2013, p. 8), y mediante un a ontología.

Las ontologías son componentes de la Web semántica que, según Lera, Juiz, & Puigjaner (2006), implementan conceptos relacionados, razonamiento y reglas de inferencia en la Web (p.27). Un ejemplo es DogOnt desarrollada como una ontología que representa conceptos de ambientes y dispositivos referidos a una vivienda domótica, tal y como lo exponen Bonino, Corno, & Razzak (2011), la que complementada con la ontología DogPower que el mismo Bonino en colaboración con Procacianti (2014) permite medir el consumo de energía de cada dispositivo de un sistema domótico y según el patrón de comportamiento de cada persona (Hong, D'Oca, Turner, & Taylor-Lange, 2015, pág. p.199) de manera remota desde un servidor web y, en una configuración adecuada, reducir el consumo de energía de múltiples viviendas, teniendo en cuenta la reutilización de componentes ante usuarios concurrentes en un mismo ambiente con actividades parecidas o priorizables. (Hong, et al, 2015, p.772)

Sin embargo, la complejidad inherente al desarrollo de aplicaciones web de hoy, como las basadas en ontologías que controlarían remotamente a los sistemas domóticos en viviendas automatizadas, trae consigo una falla en la seguridad informática, vulnerabilidad que es propia de la Web semántica expuesta por Garzón, Coronel y Alfredo (2015) y Razzaq, Anwar, Ahmad, Latif, & Munir (2014), quienes indican que los ataques informáticos, en un futuro próximo, se centrarán en modificar el significado de conceptos incluidos en una ontología de la Web semántica para permitir la intrusión en los sistemas, por ejemplo, de automatización de vivienda.

Por lo expuesto, es necesaria una revisión de técnicas que mantengan la seguridad informática en el sistema ontología-controlador central domótica. Según Bhargavan, Fournet, & Gordon (2005), las principales técnicas de seguridad informática relacionada con el software y su vulnerabilidad son las

1.Docente de la Facultad de Ingeniería de la Universidad Privada Antenor Orrego

firmas digitales, la criptografía y los certificados digitales. La firma digital está orientada a asegurar la integridad parcial o total de un archivo, en caso de su necesaria exposición, mientras que los sistemas encriptados o criptosistemas están orientados a entornos donde el emisor y receptor mantienen la integridad de la comunicación. Los certificados digitales, por otro lado, requieren de un tercero para su validación.

La criptografía tiene una clasificación que divide a los criptosistemas en simétricos o de claves privadas y asimétricos o de claves públicas; siendo los criptosistemas simétricos basados en XML Encryption con el Advanced Encryption Standard los más apropiados para encriptar una ontología según Périssé (2008) y Ammari, Lu, & Aburrous (2014, p. 614). Esto debido a que únicamente se necesitan claves privadas para asegurar la ontología en los servidores web y las consultas en el controlador central de un sistema domótico, debiendo trasmitir la comunicación del servidor web al controlador domótico dentro de un marco de desarrollo y ECC Mixed Coordinates Cryptography para encriptar el mensaje apoyándose en OWL / OWL-S. (Nabil & Mohamed, 2012, pág. p. 190)

Por eso se concluye que, para mitigar el riesgo informático de una ontología controladora de sistemas domóticos de manera remota expuesta desde un servidor web, es necesario un criptosistema simétrico basado en el lenguaje XML Encryption con el Advanced Encryption Standard con un marco de desarrollo y ECC Mixed Coordinates Cryptography para encriptar el mensaje apoyándose en OWL / OWL-S, debido a su capacidad de asegurar, mediante clases privadas, las reglas de inferencia y consultas en leguaje plano que intercambian el servidor web con el controlador central del sistema domótico. Se debe realizar el estudio de qué parte de la ontología justifica ser encriptada, ya que el proceso de encriptación consume recurso computacional reflejado en tiempo ante el usuario.

REFERENCIAS BIBLIOGRÁFICAS

Ammari, F. T., Lu, J., & Aburrous, M. (2014). Intelligent Banking XML Encryption Using Effective Fuzzy Logic. En E. Inc., *Emerging Trends in ICT Security* (págs. 591-617). Abu Dhabi, UAE. doi:http://dx.doi.org/10.1016/B978-0-12-411474-6.00037-2

Bhargavan, K., Fournet, C., & Gordon, A. D. (2005). A semantics for web services authentication. *Theoretical Computer Science*, págs. 102 – 153. doi:10.1016/j.tcs.2005.03.005

Bonino, D., Corno, F., & Razzak, F. (2011). Enabling machine understandable exchange of energy consumption information in intelligent domotic environments. *Energy and Buildings*, págs. 1392 - 1402. doi:10.1016/j.enbuild.2011.01.013

Bonino, D., & Procaccianti, G. (2014). Exploiting semantic technologies in smart environments andgrids:Emerging roles and case studies. *Science of Computer Programming*, págs. 112–134. doi:http://dx.doi.org/10.1016/j.scico.2014.02.018

Carrero Vázquez, S. (2013). Diseño de un sistema de gestión técnica centralizada para el control del clima y la iluminación del bloque habitacional de un hotel. *Tercer Congreso Virtual, Microcontroladores y sus Aplicaciones*.

García Sánchez, C. M., & Moreno Martín, F. (2013). *Una panorámica de la inteligencia artificial aplicada a la Domótica, págs. 8-9.* Madrid: Universidad Carlos III.

Garzón, B., Coronel , M., & Alfredo, C. (03 de 2015). *Seguridad informática y la prevención de amenazas informáticas del futuro.* Obtenido de http://repositorio.espe.edu.ec/handle/21000/6026

Hong, T., D'Oca, S., Taylor-Lange, S. C., Turner, W. J., Chen, Y., & Corgnati, S. P. (2015). An ontology to represent energy-related occupant behavior in buildings. Part II: Implementation of the DNAS framework using an XML schema. *Building and Environment*, págs. 196 - 205.

Hong, T., D'Oca, S., Turner, W. J., & Taylor-Lange, S. C. (2015). An ontology to represent energy-related occupant behavior in buildings. Part I: Introduction to the DNAs framework. *Building and Environment*, págs. 764 - 777.

Lera, I., Juiz, C., & Puigjaner, R. (2006). Performance-related ontologies and semantic web applications for on-line performance assessment of intelligent systems. *Science of Computer Programming*, 27–37. doi:10.1016/j.scico.2005.11.003

Nabil, S., & Mohamed, B. (2012). *Security Ontology for Semantic SCADA.* Mentouri Constantine University & SONELGAZ Group.

Périssé, M. C. (2008). *Firma digital en la Web semántica: Aplicación en la biblioteca digital.* Obtenido de http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/cifrado_xml/cifrado_xml.htm

Razzaq, A., Anwar, Z., Ahmad, H. F., Latif, K., & Munir, F. (2014). Ontology for attack detection: An intelligent approach to web application security. *ScienceDirect*, págs. 124 -146.