XV Jornadas de Ingeniería Telemática.
JITEL 2021.
Universidad de A Coruña.

Actas de las XV Jornadas de Ingeniería Telemática (JITEL 2021), A Coruña (España), 27-29 de octubre de 2021.

Modelado del Conocimiento de Ciberseguridad en Entornos Hospitalarios

Susel Fernandez, Luis Cruz-Piris, Ivan Marsa-Maestre, Jose Manuel Gimenez-Guzman.
Departamento de Automática,
Universidad de Alcalá
Escuela Politécnica Superior. Campus Universitario, Ctra. Madrid-Barcelona km. 33, 600. 28805. Alcalá de Henares. Madrid.
susel.fernandez@uah.es, luis.cruz@uah.es, ivan.marsa@uah.es, josem.gimenez@uah.es.

En la actualidad se está produciendo un considerable incremento en el número de ataques informáticos dirigidos a infraestructuras críticas en todo el mundo, entre las que destacan las infraestructuras de los centros hospitalarios. Estos ataques pueden tener graves consecuencias, desde el filtrado masivo de datos sanitarios confidenciales, hasta el colapso total de las infraestructuras TICs de las entidades sanitaras. Este trabajo se centra en la gestión del conocimiento de ciberseguridad en el entorno hospitalario y consiste en el desarrollo de una ontología que modele los principales conceptos y relaciones identificados en este dominio. El objetivo principal es poder contar con infraestructuras capaces de detectar estos ataques y establecer mecanismos de actuación que permitan mitigar sus efectos sobre los activos en un entorno tan crucial y vulnerable como es el entorno sanitario.

***Palabras Clave*- gestión de conocimiento, ontología, ciberseguridad.**

I. INTRODUCCIÓN

En los últimos años estamos asistiendo a un crecimiento en el número y tipología de las amenazas de seguridad, que afectan no sólo a los ordenadores de los usuarios, sino a todo tipo de dispositivos y sistemas. Se está produciendo un considerable incremento en el número de ataques informáticos dirigidos a infraestructuras críticas de todo tipo en todo el mundo. Entre estos destacan especialmente los ciberataques sobre las TICs en centros de atención hospitalaria [1]. La naturaleza de estos incidentes es cada vez más variada y compleja y va desde simples ataques de denegación de servicio (DoS) hasta infecciones por malware, como por ejemplo los ataques de tipo Ransomware [2] [3], donde los atacantes interrumpen las operaciones informáticas y solicitan dinero para "liberar" los recursos bloqueados. Los motivos para realizar estos ataques se basan fundamentalmente en la falta de seguridad de las instalaciones hospitalarias y en el gran impacto que puede tener la falta de acceso a los recursos informáticos en estas instituciones.

En mayo del 2017, una fracción significativa de hospitales en el Reino Unido fue atacada por un malware, que provocó una considerable afectación a las áreas de emergencias y retrasos en las cirugías [4]. Más recientemente, en septiembre de 2019, el Campbell County Memorial Hospital en Wyoming, EE. UU., fue golpeado por un ataque de malware más específico, que provocó la cancelación de muchos servicios como las cirugías y los exámenes de radiología.

En España, en el mes de enero de 2020, el Hospital Universitario de Torrejón, quedaba paralizado por un ataque informático de tipo Ransomware. Casi dos semanas después, el centro sanitario conseguía rescatar su sistema de citas automatizadas, pero otros tantos servicios permanecieron inactivos por más tiempo. El incidente colapsó por completo el sistema informático del hospital [5].

Esta creciente proliferación de incidentes de seguridad se debe a varios factores, entre los cuales se encuentra la conectividad de los diferentes dispositivos de las instituciones hospitalarias a las redes y por supuesto, a internet. Dentro de una red de atención médica, podemos encontrar en la actualidad una gran variedad de dispositivos, que van desde ordenadores portátiles, smartphones, hasta equipos médicos específicos, que generan y procesan datos médicos. Esta combinación de dispositivos heterogéneos junto con la ubicuidad deseada y la alta conectividad [6] implica un desafío complejo desde el punto de vista de la ciberseguridad.

Lo deseable sería poder contar con una infraestructura diseñada para reaccionar ante incidentes de seguridad, que limite la propagación del ataque y permita mitigar sus efectos de manera rápida y eficaz. Para lograr este objetivo, la gestión del conocimiento de seguridad en el entorno de las TICs en los centros hospitalarios es crucial.

Este trabajo está dirigido a abordar la necesidad de contar con un modelo del conocimiento lo suficientemente expresivo, que permita modelar las diferentes características de los ciberataques más comunes, sus relaciones con las vulnerabilidades y cómo afectan a los activos identificados en este dominio. Para el modelado de la base de conocimiento del sistema se ha desarrollado una ontología, que abarca los principales conceptos y relaciones del dominio de la ciberseguridad en el entorno hospitalario, así como una base de reglas para el mecanismo de razonamiento con la misma.

El documento está organizado de la siguiente manera. La sección II presenta los antecedentes y el estado actual del tema. En la sección III se presenta el modelado del conocimiento, que incluye la ontología y el mecanismo de razonamiento. En la sección IV se describen brevemente algunos escenarios de prueba y finalmente, las conclusiones y líneas de trabajo futuro se resumen en la sección V.

II. ANTECEDENTES Y ESTADO ACTUAL DEL TEMA

En el área de la ciberseguridad existen algunas bases de datos con información sobre vulnerabilidades, productos y componentes a los que afectan, especificaciones técnicas, impacto y vector de ataque. También hay herramientas para el análisis automático de vulnerabilidades, basadas en configuraciones recomendadas de seguridad (checklists) para sistemas y servicios, que van asociadas al nivel de protección necesario en función del tipo de sistema.

A. Bases de datos y clasificación de vulnerabilidades

En cuanto a las bases de datos de vulnerabilidades tenemos que mencionar a CVE (Common Vulnerabilities and Exposures) [7] y CWE (Common Weakness Enumeration) [8], ambas de MITRE Corporation. CVE, un diccionario público que proporciona un identificador único para cada vulnerabilidad, se ha convertido en un estándar y constituye la principal fuente de información sobre vulnerabilidades para otras bases de datos. Por su parte, CWE también es un estándar internacional y de libre uso, que proporciona un lenguaje común para describir vulnerabilidades de seguridad de software en arquitectura, diseño y codificación. Otra base de datos conocida es la del gobierno estadounidense, NVD (National Vulnerability Database) [9], que permite la automatización de la gestión de vulnerabilidades y la medición del nivel de seguridad. Incluye listas de comprobación de configuraciones de seguridad de productos y efectos en software relacionado.

Un elemento importante a la hora de abordar las vulnerabilidades es poder clasificarlas según su severidad para establecer estrategias efectivas de protección. CVSS (Common Vulnerability Scoring System) [10] es un sistema que permite calcular la severidad de una vulnerabilidad, de manera estricta a través de fórmulas matemáticas. Proporciona un estándar para comunicar las características y el impacto de una vulnerabilidad identificada con su código CVE.

En cuanto a la clasificación de vulnerabilidades, existe OWASP (Open Web Application Security Project), que es un proyecto de código abierto dedicado a determinar y combatir las vulnerabilidades en aplicaciones en el entorno Web. OWASP Top Ten [11] es un documento que se publica cada tres años, con los diez riesgos de seguridad más importantes en aplicaciones Web. Su objetivo es crear conciencia acerca de la seguridad en aplicaciones mediante la identificación de los riesgos más críticos que enfrentan las organizaciones.

B. Herramientas de análisis de vulnerabilidades

En cuanto a las principales herramientas disponibles, tenemos las que permiten realizar análisis de vulnerabilidades de código fuente. RATS (Rough Auditing Tool for Security) [12] es un analizador de código estático, *open source*, para detectar potenciales problemas de seguridad en varios lenguajes de programación como C/C++, Perl, PHP, Python y Ruby. Entre las herramientas para el análisis de vulnerabilidades de sistemas completos, tenemos MBSA (Microsoft Baseline Security Analyzer) [13], que permite analizar la seguridad de pequeñas redes formadas por equipos con Windows. Entre los escáneres de vulnerabilidades más completos tenemos OpenVAS (Open Vulnerability Assessment Scanner) [14], una herramienta *open source*, que abarca un espectro amplio de funciones, incluyendo varios protocolos industriales, escaneos a gran escala y un potente lenguaje de programación para implementar pruebas de vulnerabilidad. Por su parte, MITRE ATT&CK [15] es una base de conocimiento accesible a nivel mundial, para el desarrollo de modelos y metodologías de amenazas específicas de ciberseguridad en varios dominios.

C. Ontologías

Existen algunos modelos ontológicos dirigidos a abordar distintas áreas de la ciberseguridad. En [16] proponen una ontología de seguridad utilizando lógica descriptiva, destinada a organizar el conocimiento relacionado con la gestión de riesgos. En [17] se presenta una ontología diseñada para el análisis y la gestión de vulnerabilidades, que incluye las relaciones entre productos TIC, vulnerabilidades, atacantes, métricas de seguridad y contramedidas. En [18] introducen una ontología que captura información sensible a la privacidad para los Sistemas de Redes Sociales. La ontología permite detectar ausencia de políticas de protección de privacidad. Otras ontologías se centran en ataques específicos, como las amenazas persistentes avanzadas (ATP), que pueden materializarse a través de distintos tipos de malware en diversos entornos, como por ejemplo en dispositivos IoT [19, 20]

Aunque ha habido varias propuestas de ontologías en el estado del arte, la mayoría están en las primeras etapas de desarrollo y su reutilización para nuestro propósito es bastante limitada. Ninguna de las aproximaciones existentes ha demostrado ser lo suficientemente expresiva para cubrir el conocimiento necesario para responder de manera adecuada y rápida ante los ciberataques en entornos hospitalarios.

III. MODELADO DEL CONOCIMIENTO

Para el modelado del conocimiento se ha diseñado una ontología, que abarca los principales conceptos y sus relaciones en el entorno de la ciberseguridad en infraestructuras hospitalarias.

A. Ontología.

La ontología ha sido desarrollada en lenguaje OWL [21], utilizando la herramienta *Protégé* [22], que proporciona una interfaz gráfica interactiva y amigable para el trabajo con estas estructuras. La ontología diseñada se compone de tres bloques de conocimiento fundamentales: vulnerabilidades, amenazas y activos del sistema que pueden verse afectados por la materialización de las amenazas. La fig. 1, presenta una parte de la ontología diseñada, en la que se pueden apreciar los principales conceptos modelados en cada bloque de conocimiento y sus relaciones.

Como se puede observar en la figura, entre los principales activos del sistema, susceptibles a incidentes de seguridad se han identificado los sistemas de cuidado remoto, los dispositivos médicos en red, los sistemas de identificación, el equipamiento de red, los sistemas de información clínica interconectados, los datos y las instalaciones, entre otros.

En el bloque de conocimiento de las amenazas se recogen los principales ataques a los que suelen estar sometidos estos sistemas, entre los que destacan los ataques de robo de identidad, el *phishing*, la manipulación no autorizada de los dispositivos médicos, el secuestro de sesiones, el robo de datos, la denegación de servicio (DoS) y las infecciones por malware, que pueden llegar a ser muy variadas en cuanto a características, modos de infección y consecuencias sobre el sistema.

El otro bloque de conocimiento presentado es el que permite relacionar los ataques con los activos del sistema: las vulnerabilidades. En otras palabras, las vulnerabilidades pueden definirse como las debilidades que tiene el sistema que hacen posible que las amenazas se puedan materializar, causando daños sobre los activos. Las principales vulnerabilidades se han agrupado en dos categorías. La primera, vulnerabilidades de diseño e implementación, agrupa los conceptos relacionados con las debilidades del sistema provocadas por fallos en el desarrollo de las aplicaciones, ya sea en fase de diseño o de implementación, como por ejemplo el buffer overflow, el Cross-Site Scripting (XSS) o la inyección SQL, entre otros. La segunda categoría, se centra en los conceptos relacionados con las vulnerabilidades de configuración, que pueden ser por ejemplo un mal uso de los sistemas de autenticación, el uso de configuraciones predeterminadas, las cuentas de usuario no seguras, el almacenamiento de la información no cifrada, entre otros.

B. Razonamiento

El mecanismo de razonamiento es crucial cuando se trabaja con ontologías, porque es el proceso que permite realizar la inferencia de nuevo conocimiento a partir del conocimiento ya existente en la ontología.

En este trabajo hemos utilizado el razonador semántico *Pellet* [23], que permite además validar la consistencia de la ontología. Las reglas de razonamiento en la ontología propuesta, se han desarrollado utilizando el Lenguaje de Reglas de la Web Semántica SWRL [24]. Una vez poblada la ontología, con los individuos correspondientes a los diferentes escenarios de seguridad, la base de reglas permite realizar consultas para testar el nivel de expresividad de la ontología.

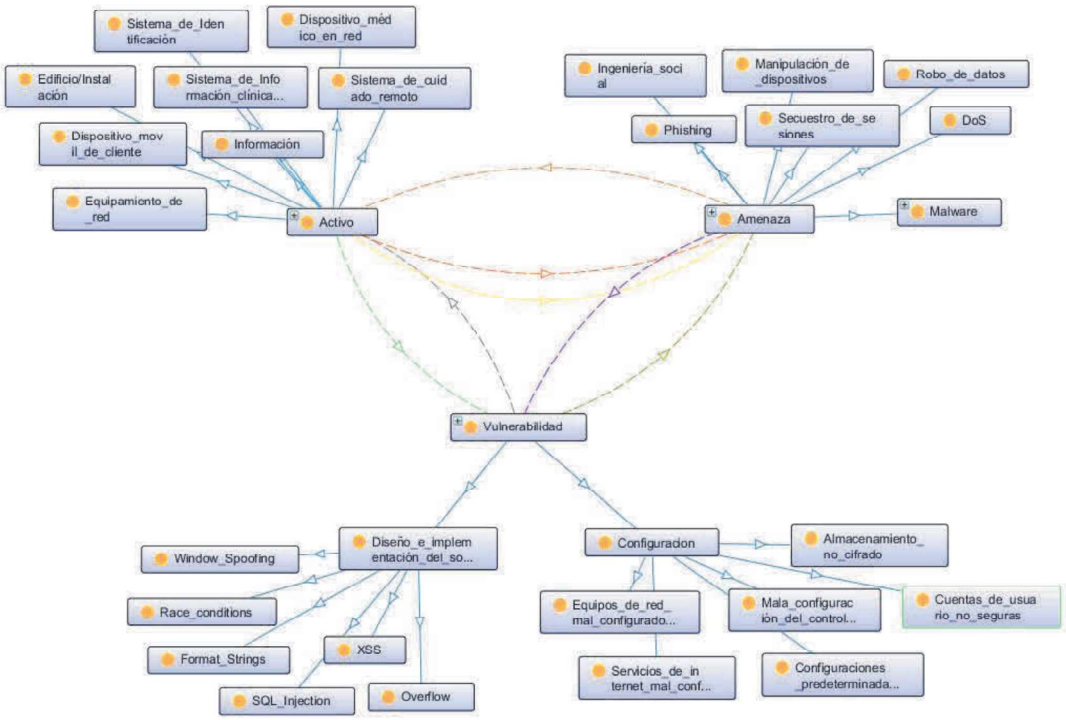

Fig.1 Ontología de ciberseguridad en infraestructuras hospitalarias

IV. Pruebas de expresividad de la ontología

El trabajo se encuentra actualmente en la fase de pruebas de la expresividad de la ontología. Para la realización de las pruebas se han definido varios escenarios que permiten obtener información de la ontología para prevenir ataques típicos a las TICs en infraestructuras hospitalarias. Las consultas a la ontología se han diseñado utilizando el lenguaje SQWRL [25]. Entre estas consultas se encuentran los listados o reportes de distintos tipos de amenazas y las vulnerabilidades que explotan, como por ejemplo:

- Amenazas de mala reputación en datos clasificados.
- Amenazas por errores involuntarios de usuarios.
- Amenazas de distribución de software malicioso por parte de los usuarios.
- Amenazas de ingeniería social.
- Malwares que utilizan una técnica especifica de ataque.
- Amenazas registrados sobre dispositivos médicos específicos.
- Amenazas que explotan vulnerabilidades específicas.
- Dispositivos con vulnerabilidades específicas conocidas.
- Listado de dependencias HW y SW para poder llevar a cabo el análisis de riesgos.

También se han definido consultas sobre políticas de seguridad tanto generales como específicas de distintos sistemas y dispositivo, permitiendo realizar un filtrado por distintas categorías.

V. Conclusiones

En este trabajo se presenta una ontología para la gestión del conocimiento de ciberseguridad en infraestructuras hospitalarias. El objetivo principal es proporcionar un modelo semántico lo suficientemente expresivo, que abarque las diferentes características de los ciberataques más comunes, sus relaciones con las vulnerabilidades y cómo afectan a los activos principales de este dominio. Esto permitirá contar con una infraestructura resiliente, que limite la propagación de cualquier ataque y facilite la mitigación de sus efectos de manera rápida y eficaz.

La expresividad de la ontología se encuentra actualmente en fase de pruebas. Para ello se han definido una serie de consultas en diferentes escenarios de ciberseguridad. Como trabajo futuro se pretende continuar mejorando la expresividad de la ontología, añadiendo más conceptos, relaciones y reglas de razonamiento y desarrollar una interfaz gráfica que facilite la gestión del conocimiento modelado de una manera más amigable.

Agradecimientos

Este trabajo ha sido parcialmente financiado por el proyecto ESCUDO- Sistema de gEStión del conocimiento de CibersegUridaD en entornos hOspitalarios. CCG20/IA-041, de la Universidad de Alcalá y el proyecto CloudWall-Cloud-enabled Resilience Framework PID2019-104855RBI00/AEI/10.13039/501100011033 del Ministerio de Ciencia e Innovación.

Referencias

[1] Safavi, S., Meer, A. M., Melanie, E. K. J., & Shukur, Z. (2018, November). Cyber Vulnerabilities on Smart Healthcare, Review and Solutions. In 2018 Cyber Resilience Conference (CRC) (pp. 1-5). IEEE.

[2] Verizon 2019 Data Breach Investigations Report. Available at https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf. Accedido el 10 de marzo de 2020.

[3] ENISA. Security and Resilience for Smart Health Service and Infrastructures. 2016. Available at https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals. Accedido el 10 de marzo de 2020.

[4] Smart, W. (2018). Lessons learned review of the WannaCry ransomware cyber attack. London: Skipton House.

[5] Noticia. El diario. https://www.eldiario.es/tecnologia/Desterrar-solucion-ciberataques-hospital-Madrid_0_990051221.html. Accedido el 10 de marzo de 2020.

[6] T. Walker, Interoperability a must for hospitals, but it comes with risks, Manag. Healthc. Exec. (2017) http://managedhealthcareexecutive.modernmedicine.com/.

[7] Common Vulnerabilities and Exposures. https://cve.mitre.org/. Accedido el 10 de marzo de 2020.

[8] Common Weakness Enumeration. https://cwe.mitre.org/. Accedido el 10 de marzo de 2020.

[9] National Vulnerability Database. https://nvd.nist.gov/. Accedido el 10 de marzo de 2020.

[10] Common Vulnerability Scoring System (CVSS) https://nvd.nist.gov/cvss.cfm. Accedido el 10 de marzo de 2020.

[11] Open Web Application Security Project. Top ten Web Application Security Risks. https://owasp.org/www-project-top-ten/. Accedido el 10 de marzo de 2020.

[12] Rough Auditing Tool for Security (RATS). https://security.web.cern.ch/security/recommendations/en/codetools/rats.shtml. Accedido el 10 de marzo de 2020.

[13] Microsoft Baseline Security Analyzer (MBSA). https://www.microsoft.com/en-us/download/search.aspx?q=MBSA. Accedido el 10 de marzo de 2020.

[14] Open Vulnerability Assessment Scanner (OpenVas). https://www.openvas.org/. Accedido el 10 de marzo de 2020.

[15] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. Technical report.

[16] Fenz, S. and Ekelhart, A. (2009) Formalizing Information Security Knowledge. Proc. 4th Int. Symp. Information, Computer, and Communications Security, Sydney, Australia, March 10–12, pp. 183–194. ACM, New York, USA.

[17] Wang, J.A. and Guo, M. (2009) OVM: An Ontology for Vulnerability Management. Proc. 5th Annual Workshop on Cyber Security and Information Intelligence Research, Tennessee, USA, January 8–10, pp. 1–4. ACM, New York, USA.

[18] Masoumzadeh, A. and Joshi, J. (2013) Privacy Settings in Social Networking Systems:What You Cannot Control. Proc. 8th ACM SIGSAC Symp. Information, Computer and Communications Security, Hangzhou, China, May 8–10, pp. 149–154. ACM, New York, USA.

[19] Han, W., Xue, J., Wang, Y., Zhang, F., & Gao, X. (2021). APTMalInsight: Identify and cognize APT malware based on system call information and ontology knowledge framework. Information Sciences, 546, 633-664.

[20] Liang, X., Ma, L., An, N., Jiang, D., Li, C., Chen, X., & Zhao, L. (2019, December). Ontology Based Security Risk Model for Power Terminal Equipment. In 2019 12th International Symposium on Computational Intelligence and Design (ISCID) (pp. 212-216). IEEE.

[21] M. Dean, and G. Schreiber, OWL Web Ontology Language Reference. http://www.w3.org/TR/2004/REC-owl-ref-20040210/; 2004.

[22] Protégé: http://protege.stanford.edu/

[23] Pellet http://clarkparsia.com/pellet/

[24] I. Horrocks, P. F. Patel-Schneider, H. Boley, S. Tabet, B. Grosof, M. Dean. SWRL: A Semantic Web Rule Language Combining OWL and RuleML, Submission to W3C, May 2004 http://www.w3.org/Submission/SWRL/

[25] O'Connor, M. J., & Das, A. K. (2009, October). SQWRL: a query language for OWL. In OWLED (Vol. 529, No. 2009).