https://repository.uaeh.edu.mx/revistas/index.php/xikua/issue/archive

XIKUA Boletín Científico de la Escuela Superior de Tlahuelilpan

Publicación semestral, Vol. 10, No. 19 (2022) 31-37

Xikua

ISSN: 2007-4948

Amenazas de seguridad a considerar en el desarrollo de software

Security treats to consider in software development

Gabriel Sánchez-Bautista [a], Lizbeth Ramírez-Chávez [b]

Abstract:

Software development should take into consideration the threats in terms of privacy and security of information. These threats can mean significant losses for organizations which lead into financial losses, access to confidential information by unauthorized users or the failure of systems. These threats take on special importance due to the great dependence that we have on information systems today. For example, the rise of electronic commerce has considerably increased the number of transactions carried out over the internet, which means that users provide sensitive data about payment methods and billing addresses. Likewise, users have to trust that they are providing information to a reliable system that will safely handle their data. Another example is the increasing use of cloud computing technology, in which users store private information on servers of external providers over which they have no control, and their information could be used for other purposes of which they are not aware. Similarly, the use of applications on mobile phones for internet banking services could pose a threat in terms of access to accounts by malicious users if there are no security mechanisms in user authentication. It is a reality that the lack of measures that guarantee information security can trigger catastrophic scenarios. For this reason, this article identifies the possible threats and vulnerabilities that must be taken into consideration in software development, in such a way that the software produced meets the necessary security characteristics in order to guarantee the availability of services and the information integrity.

Keywords:

Security, privacy, threats, access-control, software

Resumen:

El desarrollo de software debe tener en consideración las amenazas que existen en cuanto a la privacidad y seguridad de la información. Estas amenazas pueden significar grandes pérdidas para las organizaciones que se traducen en daños económicos, acceso a información confidencial por parte de usuarios sin autorización o la caída de los sistemas. Estas amenazas toman especial importancia debido a la gran dependencia que hoy en día tenemos en los sistemas de información. Por ejemplo, el auge del comercio electrónico ha incrementado considerablemente el número de transacciones que se realizan por Internet, lo cual conlleva que los usuarios proporcionen datos sensibles referentes a métodos de pago y direcciones de facturación. Así mismo, los usuarios tienen que confiar en que están proporcionando la información a un sistema confiable que manejará de forma segura sus datos. Otro ejemplo es el uso cada vez mayor de la tecnología *cloud computing*, en la que los usuarios almacenan información privada en servidores de proveedores externos sobre los cuales no tienen control y su información podría estar siendo utilizada para otros propósitos de los cuales no tienen conocimiento. De igual forma, el uso de aplicaciones en teléfonos móviles para servicios de banca por internet podría significar una amenaza en cuanto el acceso a cuentas por parte de usuarios malintencionados si no existen los mecanismos de seguridad necesarios para la autenticación de los usuarios. Es una realidad que la falta de medidas que garanticen la seguridad y privacidad de la información puede desencadenar en escenarios catastróficos. Por este motivo, este artículo identifica las amenazas y vulnerabilidades que deben ser tomadas en consideración para el desarrollo de software, de tal forma que se produzca software que cumpla con las características de seguridad necesarias a fin de garantizar la disponibilidad de los servicios y la integridad de la información.

Palabras Clave:

Seguridad, privacidad, amenazas, control de acceso, software

[a] Autor de Correspondencia, Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0002-9955-8711, Email: gabriel_sanchez@uaeh.edu.mx

[b] Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0002-1748-5126, Email: ra413046@uaeh.edu.mx

Fecha de recepción: 15/10/2021, Fecha de aceptación: 05/11/2021, Fecha de publicación: 05/01/2022

Introducción

La seguridad y privacidad de la información deben ser consideradas en el desarrollo de software. Tener en cuenta estos aspectos puede añadir características de calidad a los sistemas que se desarrollan, además de establecer restricciones sobre su operatividad. Ignorar los aspectos de seguridad en las etapas tempranas del desarrollo de software puede generar costos excesivos en las etapas posteriores e incluso podría requerir un rediseño del sistema. Por esta razón, los desarrolladores de software deben incorporar los requerimientos de seguridad junto con los requerimientos funcionales del sistema a fin de identificar las amenazas que podrían generar vulnerabilidades en su sistema.

En la actualidad, el software de las empresas se ha vuelto especialmente vulnerable debido a la proliferación de varios tipos de amenazas que surgen con el uso del internet. La información de las empresas está expuesta a ciberataques que pueden resultar en pérdidas en diversos ámbitos. Las pérdidas financieras pueden ser causadas por brechas de seguridad que no logran ser detectadas debido a que provienen de incidentes de seguridad en pequeña escala [1,2,3]. De ahí la importancia de conocer las amenazas e identificar su impacto con el propósito de tomar las medidas necesarias para prevenir ataques.

Las vulnerabilidades consienten en las debilidades de un sistema que pueden ser aprovechadas por un atacante para causar daño. De acuerdo con la Encuesta Anual en Ciberseguridad y Crimen Computacional [4], 74.3% de las pérdidas totales son causadas por virus, el acceso sin autorización y el robo de información personal. Cabe mencionar que de acuerdo con el portal *Data Insider* [5], la mayoría los ataques de fraude informático provienen de atacantes internos en vez de atacantes externos, que son sobre los cuales se basan la mayoría de los mecanismos de control de seguridad.

Por estas razones, una correcta identificación de las amenazas es necesaria para analizar el posible impacto en el software a desarrollar. En la siguiente sección, se analizan las amenazas más comunes.

Amenazas de seguridad

Las amenazas de seguridad están presentes en distintas formas de acuerdo con su propósito de ataque, es decir, hay ataques que buscan obtener datos sin autorización o dejar al sistema sin servicio. Entre los ataques más comunes podemos encontrar los siguientes.

Virus informáticos

El virus informático es un programa de computadora diseñado con la intención de propagarse desde el dispositivo que infecta hacia otros dispositivos. Comúnmente, tienen la intención de dañar el sistema o robar datos. Por ejemplo, los virus podrían dañar programas, borrar archivos, formatear el disco duro o incluso podrían hacer que el rendimiento de la computadora o dispositivo disminuya de tal manera que sea imposible realizar cualquier actividad. En la actualidad los virus se han diversificado en varios tipos como *gusanos*, *troyanos* y *ransomware* [6].

1. *Gusanos* son un tipo de virus que no requiere la acción de un usuario para propagarse de un dispositivo a otro.
2. *Troyanos* son un tipo de virus que oculta su propósito malicioso haciéndose pasar por un programa que parece ser legítimo.
3. *Ransomware* es un programa dañino que restringe el acceso a tus datos hasta que pagues lo equivalente a un rescate. Con el pago, tendrías acceso nuevamente a tus datos, por lo que también se conoce al *ransomware* como un software extorsionador.

Adware y Spyware

El adware es un software que busca rastrear datos acerca de tu historial de navegación en internet con el propósito de mostrarte anuncios y ventanas emergentes [7]. Es un software no deseado que busca mostrarte anuncios personalizados. El adware puede estar diseñado para analizar tu ubicación y páginas web que visitas y así mostrarte anuncios más enfocados a tus intereses. En la mayoría de los casos, el adware se instala sin que el usuario se dé cuenta ya que frecuentemente se hace pasar por otro tipo de programas.

El spyware es otro tipo de software que busca recopilar datos de los usuarios. Por ejemplo, puede incorporar *keyloggers* que registran los datos que los usuarios introducen por el teclado, incluyendo información personal como números de tarjetas de crédito o débito, contraseñas, números telefónicos, entre otros.

Denial of Service (DoS)

El ataque de denegación de servicio se caracteriza por dejar al sistema sin operar. Esto sucede debido a que se satura a los servidores que dan respuesta a las peticiones de los usuarios, lo que genera mucho tráfico en la red y de esta forma se logra sobrecargar a los recursos del sistema, lo que provoca que el sistema falle y no pueda responder a las peticiones legítimas de usuarios [8].

El ataque DoS también puede producirse en la modalidad *Distributed Denial of Service* (DDoS), en el cual varias máquinas atacan al mismo tiempo un mismo objetivo [9]. Para llevar a cabo este ataque es común hacer uso de un grupo de *bots,* al cual se denomina *botnet*, en donde cada *bot* envía varias peticiones de conexión al servidor por

atacar. Como resultado, se logra sobrecargar al servidor y por consiguiente una denegación del servicio a las peticiones de los usuarios legítimos que se ven afectados por los ataques de otros usuarios malintencionados.
La Figura 1 muestra el tipo de ataque DDoS, en el que un usuario malicioso ataca al servidor a través de múltiples peticiones provenientes de varias máquinas. El resultado es que se genera una sobrecarga en el servidor víctima y por lo tanto ya no puede responder a las peticiones de los usuarios legítimos.

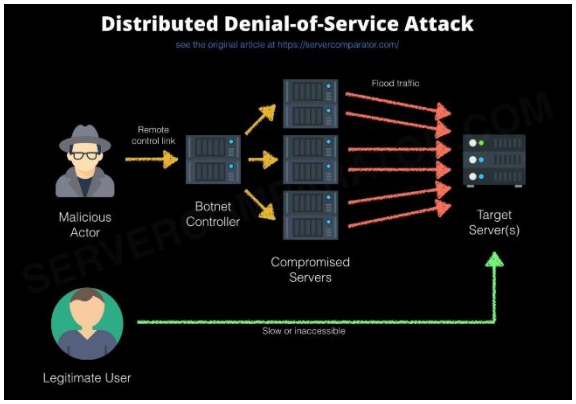

Figura 1. Ejemplo de un ataque DDoS [10].

Suplantación de identidad (Phishing)

El phishing es una forma de robo de identidad. Los atacantes intentan robar tus datos y obtener información personal para obtener acceso a tus cuentas o llevar a cabo crímenes usando tus claves de usuario y contraseñas. Frecuentemente, los atacantes buscan obtener información como números de empleado, números de seguridad social o números de tarjetas bancarias. Los ataques pueden venir en la forma de enlaces a páginas web que simulan ser de fuentes legítimas. Al dar clic en ese enlace, el usuario es dirigido a una página apócrifa en donde se le solicita que ingrese su usuario y contraseña. El usuario no se da cuenta que es una página falsa ya que tiene todas las características de una página real.
Algunas recomendaciones para tener en cuenta son: no introducir información personal en ventanas pop-up o en páginas web que provienen de enlaces que te solicitan proporcionar números de cuenta o claves de usuario. Hay que tener en consideración que las entidades bancarias nunca solicitan claves de usuario a través de enlaces vía correo electrónico. Lo recomendable es dirigirse a la página web principal de la empresa y desde ahí iniciar sesión. De acuerdo con el estudio realizado por *Ironscales* [11], la mayoría de las páginas falsas que los atacantes usan para persuadir a los usuarios de ingresar sus datos, son las que intentan provenir de las siguientes empresas que se muestran en la Tabla 1.

Tabla 1. Empresas de las cuales los atacantes crean más páginas falsas.

Empresa	Porcentaje del total de páginas falsas
PayPal	22%
Microsoft	19%
Facebook	15%
eBay	6%
Amazon	3%

Rootkit

El rootkit es un programa que el atacante busca instalar de forma oculta en la máquina de la víctima para obtener acceso continuo en ese equipo [12]. Consiste en tener control sobre el equipo en el que se instala, por ejemplo, para cambiar la configuración del sistema o para ejecutar archivos dañinos. La palabra rootkit proviene de dos palabras en inglés, *root* (usuario administrador) y *kit* (un conjunto de herramientas), por lo tanto, se traduce como el conjunto de herramientas para obtener permisos del administrador sin su autorización. En esta amenaza, se puede manipular la máquina de la víctima desde vía remota y sin que la persona se dé cuenta de que tiene ese software dañino instalado.

Inyección de código SQL

Este ataque consiste en insertar código SQL para propósitos maliciosos. El objetivo es que el servidor de la base de datos entregue información que de otra forma no mostraría, por ejemplo, contraseñas o nombres de usuarios. Comúnmente, este ataque se lleva a cabo en aplicaciones web donde el usuario puede introducir directamente sentencias para consultas en SQL (*Structured Query Language*) a través de cuadros de búsqueda en el sitio web no protegido. El peligro es que el atacante puede modificar o incluso borrar registros de la base de datos [13]. Para ejemplificar este tipo de ataque, la Figura 2 muestra como en el campo para introducir el nombre de usuario, se introduce además una sentencia *delete* para borrar un registro.
Los ataques de inyección de código se pueden llevar a cabo de distintas maneras. Una de las más comunes, es a través de la cláusula UNION, la cual permite unir a una consulta con otra y de esta forma extender los resultados que devuelve la consulta. Un ataque exitoso de inyección SQL resulta en la obtención de datos sensibles que el atacante podrá utilizar para propósitos maliciosos. Una manera de prevenir ataques de inyección de código es utilizar consultas parametrizadas (*prepared statements*), en las cuales no se concatenan las consultas, sino que se utiliza un conjunto de parámetros especificados. De esta

forma, la consulta es preparada con anterioridad y posteriormente solo recibe los valores para los parámetros que se definieron [15].

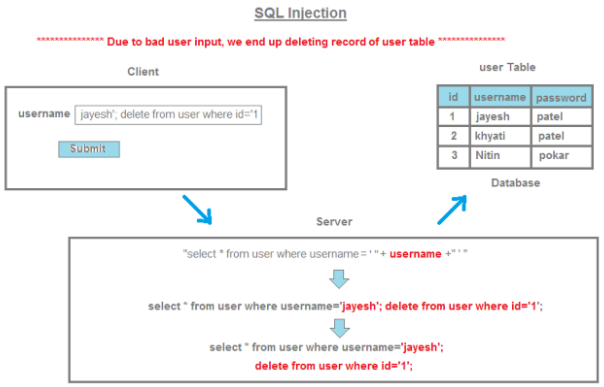

Figura 2. Ejemplo de un ataque de inyección de código [14].

Las consecuencias de un ataque de inyección de código pueden vulnerar las siguientes propiedades de un sistema.

1. **Confidencialidad**. Ya que las bases de datos pueden almacenar información sensible de los usuarios.
2. **Autenticación**. Ya que se puede tener acceso a nombres de usuarios y contraseñas y por consiguiente conectarse a un sistema utilizando claves de otros usuarios.
3. **Integridad**. Ya que se pueden hacer cambios o incluso borrar registros de la base de datos afectada.

Man in the Middle

El ataque de Man in the Middle (MitM) consiste en interceptar la comunicación entre dos usuarios o dispositivos que transfieren datos. El atacante se pone "en medio" de la comunicación de tal forma que intercepta los mensajes con el propósito de modificarlos o dirigirlos a otros destinos. Este tipo de ataque también se conoce como *eavesdropping* y es una de las razones para incorporar mecanismos de encriptación en las comunicaciones a fin de lograr que los datos sean protegidos de un extremo al otro [16]. MitM también se utiliza para robar información de datos de tarjetas de crédito, cuentas de usuario y passwords. En la mayoría de los casos, estos ataques suceden en redes Wi-Fi abiertas, en donde cualquier usuario puede conectarse a la red y en donde el atacante busca que la víctima ingrese a una conexión fraudulenta y de esta forma, el atacante obtiene el control sobre los datos que transfiere la víctima. Podemos ejemplificar este ataque en la Figura 3, en donde se muestra una comunicación normal y una comunicación que ha sido interferida por este tipo de ataque.

Figura 3. Ejemplo de un ataque MitM [17].

Para prevenir ataques MitM es importante verificar que las conexiones se lleven a cabo en navegadores web con HTTPS (*Hypertext Transfer Protocol Secure*), una combinación del protocolo HTTP con SSL, de tal forma que se asegura que la comunicación es a través del sistema de encriptación asimétrico que usa una llave pública y una privada [18]. También, se pueden usar redes privadas virtuales (*VPNs*) para crear un ambiente seguro para el intercambio de información a través de subredes, en las cuales incluso si el atacante obtiene acceso a una red compartida, no podrá descifrar lo que se transfiere en la red privada virtual.

Brute force

Estos ataques intentan obtener información a través del mecanismo de prueba y error. El atacante prueba sistemáticamente todas las combinaciones posibles hasta que obtiene la combinación correcta [19]. Este ataque se conoce como de fuerza bruta porque el atacante intenta utilizar de forma excesiva todos los mecanismos que le permitan obtener ese valor que puede ser el de una contraseña o el de una llave de encriptación. Cabe mencionar que esta forma de ataque no es nueva, pero resulta aún popular y efectiva entre los hackers, ya que dependiendo de la longitud y complejidad (por ejemplo, de una llave de encriptación), se puede obtener el valor después de un determinado número de intentos. Por ejemplo, para una llave de encriptación de 4 bits, tomará hasta 16 intentos encontrar el valor correcto a través de checar cada posible combinación, tal como lo ilustra la Figura 4.

Como podemos observar, un valor binario de 4 posiciones toma hasta 16 intentos para conocer el valor correcto debido a que $2^4 = 16$. Es decir, se toma el valor de la base (2 por ser un sistema binario) y se eleva al número correspondiente al tamaño, que en este caso es 4. Otro ejemplo es que para conocer el valor de una contraseña alfanumérica de longitud 8, el número de intentos tomaría lo correspondiente al número de caracteres disponibles en el alfabeto (27 caracteres en el alfabeto español) + el número de dígitos en el sistema numérico (10 si consideramos el sistema decimal), y ese valor elevado al

número correspondiente a la longitud de la contraseña, lo que equivale a $37^8 = 3{,}512{,}479{,}453{,}921$. Es decir, para obtener a través de un ataque de fuerza bruta el valor de una contraseña alfanumérica de 8 posiciones, tomaría hasta $3{,}512{,}479{,}453{,}921$ intentos. Por esta razón, es importante que, al definir una contraseña, utilicemos combinaciones de letras mayúsculas y minúsculas, números y caracteres especiales, ya que de esta manera disminuimos las posibilidades de ser víctimas de un ataque de fuerza bruta [20].

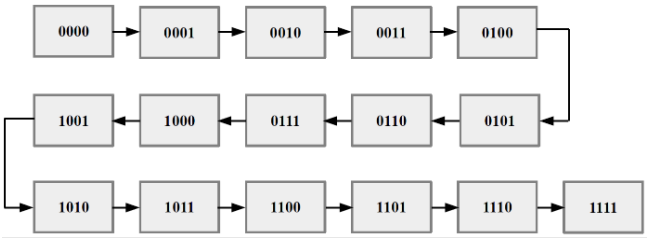

Figura 4. Ejemplo del número de intentos para un valor de 4 bits.

Otras medidas a considerar son las siguientes.

1. **Incrementar la longitud de la contraseña**. Entre mayor sea el número de caracteres que se utilicen, mayor será el tiempo que se necesite para perpetrar un ataque de fuerza bruta.
2. **Limitar el número de intentos para iniciar sesión**. Es recomendable que después de varios intentos fallidos de iniciar sesión, el sistema pida que el usuario espere cierto tiempo antes de continuar intentando ingresar al sistema. Esto disminuye las posibilidades de ser víctima de un ataque.
3. **Incorporar Captcha**. Captcha es un sistema que se utiliza para verificar que realmente es una persona quien intenta acceder al sistema, evitando así ataques sistematizados de fuerza bruta.
4. **Usar autenticación multifactorial**. Esto consiste en agregar un método adicional de autenticación además de la contraseña, por ejemplo, mediante el uso de un token dinámico.

Ataques del Internet de las Cosas

Los ataques del Internet of Things (IoT), se refieren a los ataques que se realizan a dispositivos comunes interconectados a una red. Estos dispositivos son objetos cotidianos que incorporan la capacidad de conectarse a internet, entre los que se encuentran impresoras, *smart TVs*, cámaras de seguridad, focos inteligentes, refrigeradores, cafeteras, cerraduras, timbres, termóstatos y demás aparatos de uso doméstico [21]. Un ejemplo son las denominadas *Smart Houses* (casas inteligentes), en las cuales existen muchos dispositivos que se controlan a través del internet. El problema es que muchas de las aplicaciones que se desarrollan para estos dispositivos inteligentes no cuentan con las medidas de seguridad suficientes que impidan los ataques de usuarios malintencionados. Cuando el atacante logra infiltrarse a la red a la cual están conectados, el atacante puede ser capaz de manipular otros equipos conectados a la misma red. Algunos de los motivos que hacen particularmente vulnerables a los dispositivos IoT son que la mayoría de los aparatos se comunican por redes Wi-Fi, en donde un hacker puede obtener información a través de un ataque de tipo *eavesdropping*. Además, la mayoría de estos aparatos domésticos no soporta esquemas de seguridad complejos debido a las limitaciones en sus recursos computacionales. La Figura 5 muestra la información que se puede obtener a través de ataques a dispositivos IoT. El atacante puede obtener información relacionada con passwords, emails, historial de búsqueda, ubicación, grabaciones de audio y video, entre otros.

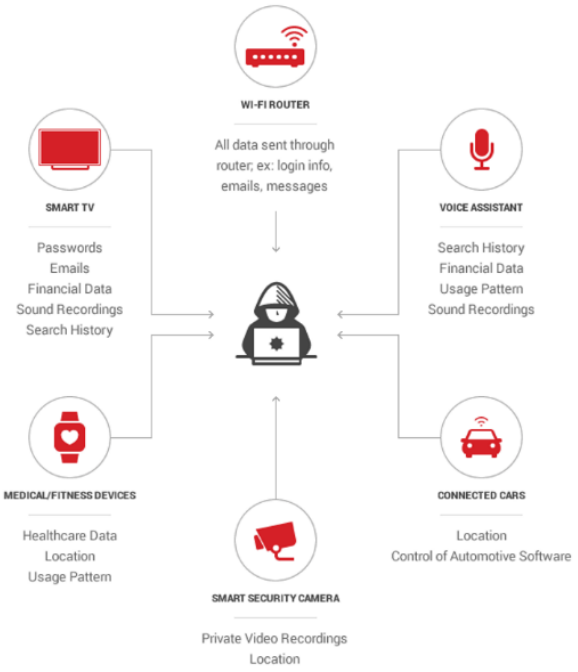

Figura 5. Datos obtenidos a través de ataques a dispositivos IoT [22].

Como podemos observar, son muchos los datos que se pueden obtener a través de este tipo de ataque. Por esta razón, algunas consideraciones para tener en cuenta son que los datos recopilados por estos dispositivos sean rastreables, es decir, se pueda saber con precisión para que se utiliza la información recopilada, y configurar a

cada dispositivo teniendo en cuenta aspectos de seguridad como autenticación multifactorial y sistemas de encriptación.

Conclusiones

La seguridad y privacidad de la información son aspectos importantes para considerar en el desarrollo de software. No tener en cuenta estos aspectos puede desencadenar en pérdidas considerables para las empresas y para los individuos. Identificar las amenazas en etapas tempranas del desarrollo de software ayudará a incorporar los mecanismos de seguridad necesarios para mitigar y hacer frente a estas amenazas, así como a hacer menos probable el hecho de ser víctimas de estos ataques.

Con el uso cada vez mayor del internet, se han diversificado los tipos y formas de ataques, los ataques pueden venir en la forma menos esperada. Los hackers aprovechan cualquier vulnerabilidad en el sistema para obtener información confidencial o hacer que los sistemas dejen de funcionar. Entre las recomendaciones para no ser víctimas de este tipo de ataques es desarrollar software que incorpore varios factores de autenticación, por ejemplo la autenticación de tres factores (algo que sabes, algo que tienes y algo que eres), incorporar *digital certificates* que garanticen la autenticidad del sitio web que se visita, utilizar firmas digitales (*digital signatures*), crear redes privadas virtuales (*VPNs*), así como incorporar diversos esquemas de encriptación con el propósito de proteger la información que se transfiere por la red.

Estos son los motivos para desarrollar sistemas que tomen en consideración a la seguridad como a un requisito fundamental. Sin las medidas de seguridad adecuadas, los sistemas no serán capaces de garantizar la integridad de la información ni de ofrecer todas las funcionalidades a los usuarios.

Referencias

[1] D. Martin, *Top 5 Information Security Threats and How to Prevent Them*, Residential tech today, 14 julio 2021. [En línea]. Available: https://restechtoday.com/top-5-information-security-threats-and-how-to-prevent-them/. [Último acceso: 17 septiembre 2021].

[2] StealthLabs, *Cyber Security Threats and Attacks: All You Need to Know*, 4 diciembre 2020. [En línea]. Available: https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/. [Último acceso: 20 septiembre 2021].

[3] O. Cassetto, *21 Top Cybersecurity Threats and How Threat Intelligence Can Help*, 25 junio 2019. [En línea]. Available: https://www.exabeam.com/information-security/cyber-security-threat/. [Último acceso: 20 septiembre 2021].

[4] L.A. Gordon, M.P. Loeb, W. Lucyshyn & R. Richardson, *CSI/FBI Computer Crime and Security Survey 2006*, 11th Annual CSI/FBI Computer Crime and Security Survey, 2006. [En línea]. Available: http://pdf.textfiles.com/security/fbi2006.pdf. [Último acceso: 21 septiembre 2021].

[5] N. Giandomenico & J. De Groot, *Insider vs. Outsider Data Security Threats: What's the Greater Risk?*, Data Insider, 18 septiembre 2020. [En línea]. Available: https://digitalguardian.com/blog/insider-outsider-data-security-threats. [Último acceso: 23 septiembre 2021].

[6] A. Tiwari, *What Is The Difference: Viruses, Worms, Ransomware, Trojans, Malware, Spyware, Rootkit*, Fossbytes, 15 marzo 2021. [En línea]. Available: https://fossbytes.com/difference-viruses-worms-ransomware-trojans-bots-malware-spyware-etc/. [Último acceso: 23 septiembre 2021].

[7] R. A. Grimes, *9 types of malware and how to recognize them*, Portal CSO, 17 noviembre 2020. [En línea]. Available: https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html. [Último acceso: 23 septiembre 2021].

[8] L. Irwin, *What is a DoS (denial-of-service) attack?*, Portal it governance, 22 enero 2021. [En línea]. Available: https://www.itgovernance.co.uk/blog/what-is-a-dos-denial-of-service-attack. [Último acceso: 24 septiembre 2021].

[9] J. Fruhlinger, *DDoS explained: How distributed denial of service attacks are evolving*, Portal CSO, 12 febrero 2021. [En línea]. https://www.csoonline.com/article/3222095/ddos-explained-how-denial-of-service-attacks-are-evolving.html. [Último acceso: 24 septiembre 2021].

[10] SQL-Server-Team, *Understanding Server Traffic logs and detecting Denial of Service Attacks*, Tech Community, 23 marzo 2019. [En línea]. https://techcommunity.microsoft.com/t5/sql-server/understanding-server-traffic-logs-and-detecting-denial-of/ba-p/385529. [Último acceso: 25 septiembre 2021].

[11] B. Roddas, *50,000+ Fake Login Pages Spoofing Over 200 Brands Worldwide*, Ironscales Safer Together, 24 agosto 2020. [En línea]. Available: https://ironscales.com/blog/fake-login-pages-spoof-prominent-brands-phishing-attacks/. [Último acceso: 27 septiembre 2021].

[12] I. Belcic, *Rootkits: qué hacen, cómo funcionan y cómo eliminarlos*, Avast Academy, 16 enero 2020. [En línea]. Available: https://www.avast.com/es-es/c-rootkit. [Último acceso: 28 septiembre 2021].

[13] S. Kost, *An Introduction to SQL Injection Attacks for Oracle Developers*, Integrigy Corporation. [En línea]. Available: https://web.archive.org/web/20151005235207/http://www.net-security.org/dl/articles/IntegrigyIntrotoSQLInjectionAttacks.pdf. [Último acceso: 30 septiembre 2021].

[14] JavaByPatel, *What is SQL Injection?*. [En línea]. Available: https://javabypatel.blogspot.com/2015/09/what-is-sql-injection.html. [Último acceso: 30 septiembre 2021].

[15] J. Ablon, *How to prevent SQL Injection vulnerabilities: How Prepared Statements Work*, 11 febrero 2020. [En línea]. Available: https://jaredablon-31568.medium.com/how-to-prevent-sql-injection-vulnerabilities-how-prepared-statements-work-f492c369614f. [Último acceso: 30 septiembre 2021].

[16] D. Swinhoe, *What is a man-in-the-middle attack? How MitM attacks work and how to prevent them*, Portal CSO, 13 febrero 2019. [En línea]. Available: https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html. [Último acceso: 5 octubre 2021].

[17] Veracode, *Man in the Middle (MITM) Attack Learn About Man-in-the-Middle Attacks, Vulnerabilities, and How to Prevent MITM Attacks*, Application Security Knowledge Base. [En línea]. Available: https://www.veracode.com/security/man-middle-attack. [Último acceso: 5 octubre 2021].

[18] J. Petters, *What is a Man-in-the-Middle Attack: Detection and Prevention Tips*, 8 octubre 2020. [En línea]. Available: https://www.varonis.com/blog/man-in-the-middle-attack/. [Último acceso: 6 octubre 2021].

[19] J. Petters, *What is a Brute Force Attack?*, 20 julio 2021. [En línea]. Available: https://www.varonis.com/blog/brute-force-attack/. [Último acceso: 8 octubre 2021].

[20] PasswordDepot, *Ataques de fuerza bruta*. [En línea]. Available: https://www.password-depot.de/es/know-how/ataque-de-fuerza-bruta.htm. [Último acceso: 8 octubre 2021].

[21] K. Hewitt, *7 Internet of Things Threats and Risks to Be Aware of*, Security Scorecard, 4 agosto 2021. [En línea]. Available: https://securityscorecard.com/blog/internet-of-things-threats-and-risks. [Último acceso: 10 octubre 2021].

[22] Devopedia, *IoT Security*, 25 junio 2021. [En línea]. Available: https://devopedia.org/iot-security. [Último acceso: 10 octubre 2021].