ENSAYOS

Isaias Simancas Diaz
Breiner Soler Torres
Airón Urrutia
Frank Torres

María Fernanda Toscano Galvis

Universidad Popular Del Cesar Secciona Aguachica
Ingeniería de Sistemas

Aguachica - Cesar
21 de noviembre 202

5.3 INTRUSOS:

INTRUSOS: EL IMPACTO DE ELEMENTOS EXTERNOS EN SISTEMAS DE GESTIÓN INFORMÁTICA

La seguridad y gestión de información han sido temas críticos en el desarrollo de sistemas informáticos. La presencia de intrusos, entendidos como elementos externos que alteran el propósito o la estructura original de un sistema, plantea desafíos técnicos y organizacionales. Este ensayo explora cómo los intrusos, sean roles no planificados o usuarios malintencionados, afectan los sistemas de gestión dinámica y personalizada, tomando como referencia el sistema descrito en el documento.

La Gestión De Roles Y Los Intrusos

En el desarrollo de herramientas como el generador de reportes del sistema GREHU, se observa cómo la falta de jerarquías claras en los roles de usuario puede derivar en problemas que asemejan intrusiones (Pérez Gort, 2012). Cuando un sistema no prevé la complejidad y dinamismo de las responsabilidades, los usuarios pueden actuar fuera de su rol, impactando negativamente en la estructura del sistema y generando conflictos en la distribución de tareas.

Intrusos En El Contexto De Seguridad

En el ámbito de la seguridad informática, los intrusos se asocian comúnmente a accesos no autorizados. Sin embargo, en la gestión de sistemas, pueden adoptar formas menos evidentes, como usuarios legítimos que alteran el diseño de plantillas o roles que no encajan en las jerarquías establecidas (Pérez Gort, 2012). Esto subraya la importancia de un módulo de gestión de roles robusto que identifique y controle el alcance de las acciones de cada usuario.

Soluciones Propuestas

Para mitigar los efectos de los intrusos, el sistema GREHU implementó módulos que incluyen gestión de plantillas dinámicas y personalizables, y roles de usuario claramente definidos. Esta aproximación permite una flexibilidad controlada y asegura que las acciones de los usuarios se ajusten a las políticas del sistema. Además, incorporar metodologías como la ingeniería de requisitos guiada por objetivos puede ayudar a anticipar problemas derivados de roles ambiguos o intrusos.

La presencia de intrusos en un sistema, ya sea en forma de usuarios malintencionados o dinámicas no previstas, refleja la necesidad de un diseño preventivo y adaptativo. Al definir roles claros y asegurar controles efectivos, los desarrolladores pueden minimizar el impacto negativo y optimizar la funcionalidad del sistema. Este enfoque no solo mejora la seguridad, sino que también eleva la aceptación del sistema por parte de los usuarios.

5.4 SOFTWARE MALIGNO:

SOFTWARE MALICIOSO: UNA AMENAZA CONSTANTE EN LA ERA DIGITAL

El software malicioso, conocido comúnmente como malware, es una de las mayores amenazas en el ámbito de la tecnología y la informática. Su capacidad de adaptarse, propagarse y evolucionar lo convierte en una herramienta peligrosa, utilizada por atacantes para vulnerar sistemas, robar información, causar daños o extorsionar a sus víctimas. Este ensayo explorará en profundidad qué es el malware, sus características, clasificación, métodos de propagación, impacto y medidas preventivas, basándose en el contenido detallado del documento proporcionado.

El malware se define como cualquier software diseñado para alterar el funcionamiento de un equipo, corromper o robar información, o tomar el control de sistemas de manera no autorizada. Este término, que incluye virus, gusanos, troyanos, spyware, ransomware y otras variedades, abarca un espectro más amplio que el de los virus informáticos.

Vulnerabilidades técnicas: Fallos en sistemas operativos o programas permiten que el malware se instale o propague sin restricciones.

Errores humanos: Los usuarios, por desconocimiento o exceso de confianza, suelen ejecutar archivos infectados, descargar software de fuentes no confiables o interactuar con enlaces sospechosos.

A menudo se piensa que ciertos sistemas, como Linux o MacOS, son inmunes al malware. Sin embargo, existen variantes diseñadas específicamente para estas plataformas, al igual que para dispositivos móviles como Android e iOS, lo que confirma que ningún sistema es completamente seguro.

Clasificación del Malware

El malware puede clasificarse desde múltiples enfoques:

1. Según su impacto sobre la víctima

Se distinguen tres niveles:

Bajo impacto: Cambios menores en configuraciones o molestias como publicidad emergente.

Impacto medio: Acciones que dificultan el uso del sistema, como modificaciones en el registro o bloqueos temporales.

Impacto alto: Robo de información crítica, secuestro de datos (ransomware) o control remoto del dispositivo.

2. Según la forma de propagación

Virus: Necesitan la intervención humana para ejecutarse y propagarse. Infectan archivos y se instalan en la memoria RAM, desde donde se replican.

Gusanos: Se propagan automáticamente por redes, sin necesidad de interacción del usuario, y buscan saturar recursos.

Troyanos: Simulan ser programas legítimos, pero permiten el acceso remoto no autorizado. No se replican automáticamente ni alteran otros archivos.

3. Según las acciones realizadas

Malware dañino: Diseñado para causar daño directo, como el ransomware, que cifra datos para exigir un rescate, o los keyloggers, que capturan pulsaciones de teclas para robar credenciales.

Malware no dañino: Aunque menos peligroso, puede ser molesto o actuar como puerta de entrada para otras amenazas, como ocurre con el adware, que muestra publicidad no deseada.

Métodos de Propagación

El malware utiliza diversas estrategias para propagarse:

Correo electrónico: Archivos adjuntos infectados o enlaces maliciosos dentro de mensajes aparentemente legítimos.

Redes locales o P2P: Archivos compartidos en redes pueden camuflar malware con nombres atractivos.

Páginas web comprometidas: Sitios que ejecutan scripts maliciosos al ser visitados por los usuarios.

Ingeniería social: Tácticas como el phishing, que engañan a las víctimas para que revelen datos confidenciales.

Un ejemplo emblemático es el gusano I Love You, que se propagó masivamente a través de correos electrónicos con un asunto atractivo, logrando infectar millones de sistemas.

El impacto del malware puede ser devastador. Para los usuarios individuales, implica la pérdida de datos personales, robo de información financiera o bloqueo de dispositivos. En el ámbito corporativo, las consecuencias son aún mayores, incluyendo interrupciones operativas, daño a la reputación y costos asociados con la recuperación.

Entre los tipos de malware más dañinos destaca el ransomware, que cifra archivos y exige un rescate económico, y el spyware, que roba información confidencial de manera silenciosa. Además, los backdoors permiten a los atacantes controlar remotamente los sistemas infectados, utilizándolos como herramientas para ataques más grandes.

La prevención del malware requiere un enfoque integral que combine tecnologías avanzadas y prácticas responsables:

Mantenimiento de software: Actualizar sistemas operativos y aplicaciones para corregir vulnerabilidades conocidas.

Uso de herramientas de protección: Antivirus, firewalls y sistemas de detección de intrusos son esenciales para monitorear y bloquear amenazas.

Educación del usuario: Fomentar la conciencia sobre tácticas de ingeniería social y la importancia de evitar fuentes no confiables.

Copias de seguridad: Implementar respaldos regulares para minimizar el impacto de ataques como el ransomware.

Políticas de seguridad: Definir reglas claras sobre el uso de redes y dispositivos en organizaciones para reducir riesgos.

El software malicioso es una amenaza constante y en evolución, diseñada para explotar las vulnerabilidades de sistemas y usuarios. Si bien las herramientas tecnológicas son esenciales para

combatir el malware, la verdadera defensa radica en un enfoque integral que combine soluciones técnicas, educación y prácticas responsables.

En última instancia, la ciberseguridad es una responsabilidad compartida entre desarrolladores, organizaciones y usuarios. Solo mediante un esfuerzo conjunto podremos mitigar el impacto del malware y construir un entorno digital más seguro y confiable para todos.

5.5 SISTEMAS DE CONFIANZA:

SISTEMAS DE CONFIANZA Y SEGURIDAD INFORMÁTICA

En la era digital, donde las interacciones y transacciones se realizan principalmente en entornos virtuales, los sistemas de confianza y las herramientas de seguridad informática desempeñan un papel crucial para proteger a los usuarios y sus datos. Este ensayo aborda las estrategias y tecnologías utilizadas para garantizar la seguridad en línea, centrándose en la prevención de amenazas, la navegación segura y las herramientas antimalware, basándonos en el contenido del documento proporcionado.

los virus, gusanos y troyanos pueden llegar a un equipo de diversas maneras:

Explotación de vulnerabilidades: Cada software instalado en un dispositivo puede contener debilidades que los atacantes aprovechan para introducir malware. Esto incluye sistemas operativos, navegadores web y aplicaciones de uso cotidiano como clientes de correo electrónico. La mejor defensa contra estas amenazas es mantener todo el software actualizado.

Ingeniería social: Los atacantes utilizan tácticas psicológicas para persuadir a los usuarios a realizar acciones perjudiciales, como abrir enlaces maliciosos. Ejemplo de ello son los correos de phishing o noticias falsas.

Archivos maliciosos y dispositivos extraíbles: Estos medios, como memorias USB, pueden contener malware que se ejecuta automáticamente al conectarse a un equipo. La desactivación del autoarranque y el análisis previo con un antivirus son medidas efectivas para prevenir infecciones.

Estas vías de infección subrayan la importancia de adoptar medidas preventivas sencillas pero efectivas, como evitar descargas de fuentes no confiables, analizar archivos antes de ejecutarlos y no interactuar con mensajes de remitentes desconocidos.

La navegación segura en Internet requiere un enfoque preventivo que incluya las siguientes prácticas:

Actualización del navegador: Los navegadores deben mantenerse al día para protegerse de vulnerabilidades conocidas.

Análisis de descargas: Todo archivo descargado debe pasar por un análisis antivirus antes de su ejecución.

Uso de cortafuegos: Los cortafuegos bloquean accesos no deseados, protegiendo al sistema de posibles intrusos.

Configuración de seguridad: Ajustar el nivel de seguridad del navegador para limitar la ejecución de scripts maliciosos o ventanas emergentes.

Precauciones en dispositivos ajenos: Cuando se utilizan equipos públicos, es esencial borrar cookies, historial y archivos temporales para proteger la privacidad.

Estas medidas son fundamentales para garantizar que la navegación no se convierta en una puerta de entrada para el malware. Además, el documento enfatiza el uso de conexiones seguras (https) al realizar transacciones financieras y el cierre de sesiones en equipos compartidos para evitar el acceso no autorizado.

Las herramientas antimalware son un componente esencial de cualquier sistema de confianza. Según el documento, se dividen en:

Antivirus De Escritorio:

Funcionan en modo residente, proporcionando protección continua frente a amenazas.

No requieren conexión a Internet para detectar amenazas, pero necesitan actualizaciones frecuentes para identificar nuevos tipos de malware.

Es crucial no instalar múltiples antivirus en un mismo equipo para evitar conflictos.

Antivirus En Línea:

Permiten realizar análisis adicionales cuando se sospecha que el antivirus principal no detecta una amenaza.

No previenen infecciones, pero son útiles para verificar el estado de seguridad de un sistema.

Ejemplos destacados incluyen Eset Online Scanner y Trend Micro HouseCall, los cuales ofrecen análisis detallados mediante navegadores web.

Estas herramientas complementarias permiten un enfoque dual: protección continua y detección secundaria para garantizar la seguridad.

Importancia de los Cortafuegos

Los cortafuegos, o firewalls, son otro pilar esencial en los sistemas de confianza. Su función es controlar el tráfico entrante y saliente, permitiendo únicamente las conexiones autorizadas. Los cortafuegos gestionan el acceso a los puertos TCP/IP, que son puntos de conexión lógica utilizados por aplicaciones para comunicarse en red.

Puerto abierto: Acepta conexiones y está asociado a una aplicación específica.

Puerto cerrado: Rechaza conexiones porque no hay aplicaciones asociadas o estas han sido bloqueadas.

Puerto bloqueado o sigiloso: No responde a solicitudes, dificultando que los atacantes identifiquen si el sistema está activo.

El documento subraya que el estado ideal para un cliente en Internet es tener los puertos en modo sigiloso, lo que se logra mediante configuraciones adecuadas del cortafuegos.

Los sistemas de confianza y las herramientas de seguridad informática no solo protegen los datos y la privacidad de los usuarios, sino que también fomentan un entorno digital más seguro y confiable. La combinación de medidas preventivas, como mantener el software actualizado, utilizar herramientas antimalware y configurar adecuadamente los cortafuegos, es esencial para prevenir amenazas y mitigar riesgos.

En un mundo cada vez más interconectado, la seguridad no debe ser vista como un lujo, sino como una necesidad básica para cualquier persona u organización que participe en la red. Solo a través de una adopción consciente de prácticas seguras y el uso de tecnologías avanzadas se podrá garantizar la protección frente a las crecientes amenazas cibernéticas.

5.7 SISTEMAS OPERATIVOS DE DISPOSITIVOS MÓVILES:

SISTEMAS OPERATIVOS DE DISPOSITIVOS MÓVILES

Los sistemas operativos (SO) de dispositivos móviles son fundamentales para el funcionamiento de smartphones, tabletas y otros dispositivos portátiles. Estos sistemas gestionan el hardware del dispositivo y permiten que las aplicaciones funcionen de manera eficiente, mientras ofrecen una interfaz amigable para el usuario. En un contexto donde los dispositivos móviles se han convertido en herramientas esenciales para la vida diaria, los sistemas operativos juegan un papel clave en su rendimiento, seguridad y accesibilidad.

Hoy en día, los sistemas operativos más utilizados en dispositivos móviles son Android, iOS y HarmonyOS.

- Android, desarrollado por Google, es el sistema más popular a nivel mundial. Su principal ventaja es que es de código abierto, lo que permite a los fabricantes personalizarlo según sus necesidades. Sin embargo, esto también genera problemas de fragmentación, ya que las actualizaciones no siempre llegan a todos los dispositivos al mismo tiempo.
- iOS, creado por Apple, es conocido por su estabilidad, seguridad y una experiencia de usuario uniforme. Al ser un sistema cerrado, solo se ejecuta en dispositivos Apple, lo que asegura un rendimiento optimizado, pero limita la personalización y la libertad de los usuarios.
- HarmonyOS, de Huawei, es un sistema relativamente nuevo que busca integrar dispositivos más allá de los teléfonos, incluyendo tablets, smart TVs y hasta automóviles. Aunque todavía está en desarrollo, se está posicionando como una alternativa interesante.

Los sistemas operativos móviles deben ser altamente eficientes en la gestión de recursos limitados como memoria, procesamiento y batería. Además, la seguridad es crucial, ya que los dispositivos almacenan una gran cantidad de datos personales. La compatibilidad con aplicaciones y una interfaz de usuario intuitiva son también esenciales para garantizar una buena experiencia.

Los sistemas operativos móviles han transformado nuestra forma de vivir, permitiendo acceso constante a la información, el trabajo remoto y la economía digital. Sin embargo, también han generado preocupaciones sobre la privacidad y el control de los datos personales. En el futuro, los sistemas operativos seguirán evolucionando, integrando tecnologías como la inteligencia artificial y la conectividad 5G, lo que abrirá nuevas posibilidades en áreas como la realidad aumentada y virtual.

Los sistemas operativos móviles son el pilar sobre el cual funcionan los dispositivos que usamos a diario. Android y iOS dominan el mercado, pero el surgimiento de nuevas alternativas como HarmonyOS indica que el panorama podría cambiar. Con el avance de la tecnología, los sistemas operativos móviles seguirán desempeñando un papel crucial en la evolución de la sociedad digital.

5.8 TENDENCIAS DE LA INDUSTRIA DE SOFTWARE MÓVIL:

TENDENCIAS EN LA INDUSTRIA DEL SOFTWARE MÓVIL

La industria del software móvil se encuentra en un constante estado de evolución, impulsada por avances tecnológicos, cambios en los hábitos de consumo y la creciente demanda de soluciones innovadoras. En este ensayo se exploran las tendencias predominantes en el desarrollo de software móvil y cómo estas moldean el panorama global, con un enfoque en el contexto colombiano según el informe analizado.

El software móvil ha pasado de ser una simple herramienta de comunicación a un eje central en la vida cotidiana y empresarial. Las aplicaciones móviles se han consolidado como el medio principal para acceder a servicios digitales, como el comercio electrónico, la banca y el entretenimiento. Esta transformación está respaldada por la rápida adopción de dispositivos como teléfonos inteligentes y tabletas, los cuales han superado las ventas de computadoras tradicionales.

A nivel mundial, el desarrollo de aplicaciones móviles se caracteriza por la integración de tecnologías emergentes como la inteligencia artificial, la computación en la nube y el análisis de big data. Estas herramientas potencian la capacidad de las aplicaciones para ofrecer experiencias personalizadas y eficientes. Por ejemplo, los asistentes virtuales como Siri y Google Assistant se basan en algoritmos de IA para interactuar con los usuarios de manera intuitiva.

Otro aspecto relevante es el auge de las aplicaciones multiplataforma. Herramientas como Flutter y React Native permiten a los desarrolladores crear aplicaciones que funcionen en sistemas operativos diferentes con un solo código base, reduciendo costos y tiempo de desarrollo.

En el contexto colombiano, la industria del software móvil enfrenta desafíos relacionados con la infraestructura tecnológica y la capacitación del talento humano. A pesar de estas barreras, el país ha mostrado un notable crecimiento en el desarrollo de software. Programas gubernamentales como FITI y Transformación Productiva han jugado un papel clave en la promoción de esta industria, apoyando tanto a empresas emergentes como a grandes desarrolladores.

El informe señala que Colombia tiene el potencial de convertirse en un exportador significativo de software móvil, siempre que continúe fortaleciendo sus políticas de apoyo a la innovación y la investigación tecnológica. En este sentido, la creación de clústeres tecnológicos y parques industriales ha sido identificada como una estrategia clave para fomentar la colaboración entre empresas y universidades.

A pesar del progreso, la industria del software móvil enfrenta desafíos como la brecha de habilidades en el mercado laboral, la falta de inversión en infraestructura digital y la competencia global. Sin embargo, estos retos también representan oportunidades para innovar y diferenciarse mediante el desarrollo de aplicaciones móviles que respondan a las necesidades específicas del mercado local e internacional.

En conclusión, las tendencias en la industria del software móvil apuntan hacia un futuro de innovación constante, donde la tecnología y la creatividad serán los principales motores del cambio. Colombia, con sus políticas de apoyo y talento emergente, tiene una oportunidad única para posicionarse como líder en este sector. Es crucial continuar invirtiendo en investigación, desarrollo y educación para aprovechar al máximo el potencial de esta industria en crecimiento.

5.6 CRIPTOGRAFÍA:

Desde tiempos antiguos, el ser humano ha tenido la necesidad de resguardar información sensible frente a terceros no autorizados. La criptografía, definida como el arte y la ciencia de ocultar información, ha evolucionado notablemente desde métodos clásicos como la esteganografía hasta complejos algoritmos actuales basados en la informática. Este ensayo aborda la historia, principios fundamentales y aplicaciones modernas de la criptografía, destacando su importancia en un mundo digital interconectado.

La criptografía tiene sus raíces en métodos antiguos, como la escítala lacedemonia, utilizada por los espartanos para codificar mensajes durante el siglo V a.C. Este dispositivo consistía en una vara de madera alrededor de la cual se enrollaba una tira de pergamino para escribir el mensaje, que solo podía ser leído con otra vara del mismo diámetro (Hernández Encinas, 2016, p. 24). Otro ejemplo relevante es el cifrado de César, donde cada letra del mensaje original se sustituía por otra desplazada un número fijo de posiciones en el alfabeto.

En el Renacimiento, la criptografía experimentó un avance con los discos cifradores de Leon Battista Alberti, que introdujeron la idea de utilizar alfabetos poli alfabéticos. Más tarde, Blaise de Vigenère propuso un sistema de cifrado basado en el uso de 26 alfabetos distintos, revolucionando la criptografía hasta que fue descifrado en el siglo XIX por Friedrich Wilhelm Kasiski (Hernández Encinas, 2016, pp. 42-43).

Los sistemas criptográficos modernos se clasifican en dos grandes categorías: criptografía de clave simétrica y criptografía de clave asimétrica. En el primer caso, el mismo código se utiliza para cifrar y descifrar la información, como ocurre en el algoritmo AES (Advanced Encryption Standard). Por otro lado, la criptografía de clave asimétrica utiliza un par de claves: una pública para cifrar y otra privada para descifrar, como en el algoritmo RSA, ampliamente usado en la seguridad de redes (Hernández Encinas, 2016, p. 98).

Además, los sistemas actuales no solo buscan mantener la confidencialidad de la información, sino garantizar también su integridad y autenticidad. Esto se logra mediante técnicas como los hashes criptográficos y las firmas digitales.

En la era digital, la criptografía es fundamental para garantizar la seguridad en comunicaciones electrónicas, comercio electrónico y sistemas bancarios. Los protocolos HTTPS, por ejemplo, utilizan certificados digitales y cifrado asimétrico para proteger las transacciones en línea. Asimismo, la criptografía es esencial en el desarrollo de tecnologías emergentes como el blockchain, donde los algoritmos criptográficos aseguran la integridad de las transacciones.

La criptografía ha pasado de ser una herramienta militar a convertirse en un pilar de la sociedad digital moderna. Su evolución refleja la necesidad constante de superar desafíos tecnológicos para proteger la privacidad y la seguridad en un mundo cada vez más conectado. En el futuro, tecnologías como la computación cuántica plantearán nuevos retos y oportunidades para este campo.

Referencias

Cheverria. (2011). *DETECCION DE INTRUSOS EN LA CAPA DE ENLACE PROTOCOLO 802.11.* Obtenido de HTTPS://ELlBRO.NET/ES/LC/BlBLlOUPC/TlTULOS/86025

Hernandez. (2016). *la Criptografia.* Obtenido de HTTPS://ELlBRO.NET/ES/LC/BlBLlOUPC/TlTULOS/41843

Huidobro. (2014). *Comunicaciones Moviles: Sistemas GSM, UMTS Y LTE.* Obtenido de https://elibro.neUes/lc/biblioupc/titulos/106423

MACMILLAN. (2013). *Seguridad Informatica.* Madrid España. Obtenido de https://elibro.net/es/ereader/biblioupc/43260