Mensajes ocultos en código

Este artículo explora las aplicaciones emergentes de la ocultación de datos, más allá de la comunicación encubierta. Se abordan usos innovadores como la procedencia de datos en IoT, la detección de intrusiones, la seguridad en redes eléctricas inteligentes y el almacenamiento seguro de secretos (caliptografía), destacando su potencial y las nuevas amenazas asociadas.

[ILUSTRACIÓN: OLEG LYFAR / ISTOCK]

Desde los mensajes tatuados en la cabeza de un esclavo, usados en la antigua Grecia, hasta las complejas técnicas digitales actuales, la necesidad de ocultar información ha sido una constante en la historia de la humanidad. Este deseo de confidencialidad ha dado lugar a dos grandes disciplinas dentro del ámbito de la seguridad de la información: la criptografía y la ocultación de datos (data hiding). Aunque, a menudo, se las considera relacionadas, sus fundamentos y objetivos son distintos.

La criptografía, cuyo nombre deriva de las palabras griegas *kryptos* (oculto) y *graphein* (escribir), se centra en transformar la información para hacerla ininteligible a terceras partes no autorizadas. A través de técnicas como el cifrado o las firmas digitales, la criptografía busca proteger el contenido del mensaje, asegurando su confidencialidad, integridad y autenticidad.

La ocultación de datos, por su parte, abarca dos ramas principales: la esteganografía y las marcas de agua digitales (*watermarking*). Derivada de las voces griegas *steganos* (cubierto u oculto) y, nuevamente, *graphein*, la esteganografía se basa en ocultar la existencia misma de un mensaje. Para eso, lo camufla dentro de un medio aparentemente inocuo, como una imagen, un archivo de audio o los protocolos de red, con el objetivo primordial de que pase desapercibido, en lugar de que sea incomprensible.

A diferencia de la esteganografía, el *watermarking* digital incrusta información perceptible o imperceptible directamente en el contenido (imagen, audio, video, texto) con objetivos distintos, como la autenticación, la protección de los derechos de autor, la verificación de integridad o el seguimiento de la distribución –en lugar de buscar el secreto absoluto de un mensaje oculto–.

¿Para qué sirven?

Más allá de sus aplicaciones tradicionales, estas técnicas de ocultación de datos, a menudo desconocidas, están expandiendo sus fronteras hacia áreas de desarrollo y aplicación emergentes que prometen transformar diversos ámbitos. Mientras las imágenes de redes sociales pueden albergar mensajes secretos y el *watermarking* digital se presenta como un aliado contra la desinformación, la capacidad de integrar información de forma invisible está generando soluciones innovadoras y, lamentablemente, nuevas amenazas.

Una de estas áreas emergentes se centra en la procedencia de los datos, especialmente crítica en el internet de las cosas (IoT), que básicamente significa conectar objetos de uso cotidiano (como una nevera o un reloj) a internet para que recojan y compartan información. En estos entornos, donde la información de sensores se recopila de múltiples fuentes y se procesa a través de diversos nodos, garantizar la integridad de los datos y

rastrear su origen es fundamental para asegurar la fiabilidad de las decisiones tomadas.

Datos protegidos en el internet de las cosas

Sin embargo, las limitaciones de recursos computacionales y energéticos de las redes IoT plantean desafíos importantes. Para abordarlos, se han propuesto algunas soluciones innovadoras basadas en el concepto de zero-watermarking. A diferencia de la incrustación directa, esta técnica genera una marca de agua "adjunta" a los datos a partir de ciertas características inherentes de estos y de la red, así como de información relativa a su procedencia.

Al no modificar los datos originales, el zero-watermarking permite aplicar esta técnica a cualquier tipo de datos, a la vez que proporciona robustez ante ataques y eficiencia en el uso de recursos, y permite mejorar la detección de intrusiones en redes, convirtiéndose en un aliado inesperado para la ciberseguridad.

Otra área emergente importante es la relativa a la seguridad de las redes eléctricas inteligentes (*smart grids*). Los contadores inteligentes de nuestros hogares, que registran el consumo de energía con gran detalle, son un componente fundamental de estas redes, pero también plantean desafíos de seguridad y privacidad.

La protección de los datos de los contadores inteligentes es esencial y, por ello, se han desarrollado diversas soluciones para estos sistemas, combinando *watermarking* reversible y criptografía. De esta manera, es posible proteger tanto la seguridad como la privacidad de los datos de los usuarios, con soluciones altamente eficientes. Cabe preguntarse si estas estrategias nos ayudarán en un futuro cercano a defendernos de un hipotético ciberataque cuyo objetivo sea provocar un nuevo apagón, similar al que ha afectado recientemente a la península ibérica.

Mensajes secretos

La ocultación de datos también se puede aplicar al almacenamiento seguro de secretos, como archivos de contraseñas o claves de criptomonedas. Para ello, se ha propuesto la caliptografía, un nuevo enfoque que se inspira en el uso de claves en la criptografía y en el uso de un contenido multimedia en la esteganografía, aunque difiere de ambas técnicas significativamente.

La caliptografía, cuyo nombre deriva de las palabras griegas *kalypto* (cubrir u ocultar) y *graphein*, utiliza una imagen (u otro contenido similar) como medio para obtener una clave que protege el secreto oculto. El objetivo es evitar el acceso no autorizado al secreto utilizando la clave derivada de la imagen de referencia para su recuperación, sin modificar la imagen original de manera alguna para no comprometer su integridad, atraer la atención o facilitar la detección del secreto mediante estegoanálisis.

En el ámbito de la seguridad forense, las técnicas de *watermarking* han evolucionado significativamente. Más allá de la detección de manipulaciones en imágenes o vídeos, los nuevos sistemas permiten localizar las áreas alteradas con una precisión sorprendente, incluso a nivel de píxeles individuales. Esta precisión sin precedentes abre un abanico de posibilidades en entornos como las cámaras de vigilancia, cuyas grabaciones podrían utilizarse en procedimientos judiciales sin la necesidad de que un perito tenga que confirmar su autenticidad, agilizando así los procesos legales y aumentando la fiabilidad de la evidencia digital.

Rastreo de precisión

Las marcas de agua en el flujo de red (*network flow watermarking*) representan otra novedad interesante. Esta técnica consiste en incrustar información modificando sutilmente el contenido, el tiempo, el tamaño o la tasa del tráfico de red en una comunicación, de manera que la información oculta pueda extraerse en otro punto de internet. Si bien esta aplicación puede tener usos legítimos, como el rastreo de ataques cibernéticos

o el diagnóstico de problemas en la red, también abre la puerta a usos maliciosos, como la inferencia de los sitios web que visitamos, el rastreo de nuestras llamadas o ataques a entornos de nube.

De manera similar, la esteganografía de red (*network steganography*) utiliza los protocolos de red como portadores de datos ocultos, pero, a diferencia del *watermarking*, el objetivo aquí es transferir un mensaje secreto de forma completamente indetectable.

La esteganografía en voz sobre IP (VoIP) también ha atraído atención recientemente con el desarrollo de métodos para ocultar una señal de voz dentro de otra. La limitada capacidad de ocultación en este contexto representa un desafío significativo, pero también ofrece un «disfraz» inesperado para estas transmisiones, ilustrando la tendencia actual hacia comunicaciones secretas cada vez más sofisticadas.

Arma de doble filo

En su vertiente más tenebrosa, no obstante, la esteganografía usada por criminales y terroristas sigue siendo una preocupación creciente. La facilidad con la que ocultan comunicaciones permite a los grupos delictivos coordinar actividades ilícitas, compartir información y distribuir contenido ilegal. El aumento de este uso criminal en los últimos años requiere que las autoridades desarrollen una formación especializada en análisis forense avanzado de las comunicaciones.

En último lugar, la inyección de malware mediante esteganografía (*stegomalware*) constituye una amenaza emergente, a la vez que inquietante. El *malware* –programa informático que se ejecuta sin el conocimiento del usuario del equipo infectado y realiza funciones perjudiciales en el sistema– que se oculta en archivos multimedia permite establecer canales encubiertos en tráfico de red aparentemente inofensivo, disimular comandos de control en etiquetas HTML o incluso incrustar código JavaScript malicioso manipulando el espacio de color de las imágenes.

Estas sofisticadas técnicas se emplean para propagar *ransomware* –tipo de *malware* que toma el control del equipo bloqueando o cifrando la información del usuario para, a continuación, pedir dinero a cambio de liberar o descifrar los ficheros– o sustraer datos sensibles de los dispositivos atacados de manera tan sigilosa que casi siempre se esquivan los sistemas de protección tradicionales.

En conclusión, la ocultación de datos está experimentando una rápida evolución, ofreciendo soluciones prometedoras para la procedencia de la información, la seguridad en entornos complejos como el IoT y las redes eléctricas inteligentes, el almacenamiento seguro de secretos (caliptografía) y la detección de intrusiones. No obstante, estos avances también implican la aparición de nuevos riesgos que demandan una vigilancia constante y el desarrollo de contramedidas efectivas para protegernos de sus usos dañinos.

Faraj, O., Megías, D., & Garcia-Alfaro, J. "*ZIRCON: Zero-watermarking-based approach for data integrity and secure provenance in IoT networks*" en Journal of Information Security and Applications (2024, Vol. 85, 103840). Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S221421262400142X

Kabir, F., Araghi, T. K., & Megías, D. "*Privacy-preserving protocol for high-frequency smart meters using reversible watermarking and Paillier encryption*" en Computers and Electrical Engineering (2024, Vol. 119 Part A, 109497). Disponible en: https://www.sciencedirect.com/science/article/pii/S0045790624004245

Megías, D. "*Esteganografía y cibercrimen: ¿hay motivos para la alarma?*" en Revista TELOS ((2019, Núm. 111. pp. 88-92). Disponible en:

https://telos.fundaciontelefonica.com/telos-111-analisis-david-megias-esteganografia-y-cibercrimen-hay-motivos-para-la-alarma/

Megías, D. "*Este cóctel tecnológico puede combatir la desinformación en internet*" en The Conversation (2024). Disponible en: https://theconversation.com/este-coctel-tecnologico-puede-combatir-la-desinformacion-en-internet-222431