CRIPTOGRAFIA OFENSIVA 2

Atacando y defendiendo organizaciones

Criptografía aplicada para programadores, analistas, cripto-agilistas y hackers éticos

Autor: Dr. Alfonso Muñoz

Prólogo Dr. María Isabel González Vasco

Primera edición

Madrid, España – julio 2024

Diseño de la portada: Alfonso Muñoz Muñoz

Título original: Criptografía ofensiva 2. Atacando y defendiendo organizaciones. Criptografía aplicada para programadores, analistas, cripto-agilistas y hackers éticos.

ISBN: 9798332214776
Imprenta/editorial: Independently published (Amazon KDP)

La primera versión de este libro fue escrita

de marzo a diciembre de 2020 en Madrid-España
durante una pandemia mundial (covid-19).

Este libro está dedicado a las almas que se fueron.
Su recuerdo y vida quedarán por siempre.

La esperanza es el único bien común a todos los hombres; los que todo lo han perdido la poseen aún –

Tales de Mileto (624 AC-546 AC)
Filósofo y matemático griego

"Harry, has pasado toda tu vida
escuchando las conversaciones de los demás.

Has justificado tu trabajo diciendo que no eres
responsable de lo que la gente dice o hace.

Pero ¿no te das cuenta del poder que tienes?

La capacidad de invadir la privacidad
de alguien es la capacidad de destruir su vida.

Cada palabra grabada, cada secreto revelado,
es una parte de su humanidad arrancada.

La privacidad no es solo un lujo, es una
parte fundamental de lo que nos hace
humanos. Y tú, más que nadie,
deberías entender el precio de violarla." – Stan

"The Conversation" (1974)

Índice de contenidos

Prólogo – Dr. María Isabel González Vasco

Criptografía Ofensiva parece un título agresivo; criptografía para atacar, adelantarse y acorralar al oponente, salir victorioso por utilizar las armas adecuadas, en la medida justa y el momento preciso. Nada más lejos desde las páginas de este libro que invitar a la agresión; más al contrario, su autor, Alfonso Muñoz, parte de la máxima (indiscutible en muchos ámbitos) de que la mejor defensa es un buen ataque. Con esa premisa nos invita a hacer acopio de un arsenal equipado con una gran variedad de herramientas criptográficas, modernas y "antiguas" [1] para hacer frente a los enormes retos que presenta el desarrollo de distintas tecnologías y su vertiginosa implantación en la sociedad actual.

No es sencillo dominar todos los aspectos que llevan a la correcta selección e implantación de una solución en criptografía; a menudo, el profesional se enfrenta a retos que parecen inalcanzables desde su experiencia y formación. Entender la base teórica que subyace a un diseño criptográfico con frecuencia exige amplios conocimientos de Matemáticas e Informática Teórica (Álgebra, Geometría, Teoría de Complejidad, Teoría de la Información), mientras que diseñar o evaluar una implementación criptográfica requiere experiencia en Diseño de Software/Hardware seguro, Arquitectura de Computadores o Redes de Comunicación. En uno u otro ámbito, todos los profesionales de la criptografía nos sentimos desorientados (típicamente, en varios), lo que a menudo se traduce en la ejecución fragmentada de proyectos en este entorno; organizando las tareas de manera disociada para que cada profesional se centre en su ámbito de especialización. Mantenerse cómodamente atrincherado en la zona de confort es, sin embargo, una receta infalible para el desastre en este contexto.

Este libro nos invita a perseguir una visión global de la criptografía de cara a situarnos en un suelo sólido desde el que entender las consecuencias de cada decisión tomada en el proceso de diseño e implantación de soluciones criptográficas. El primer capítulo del libro presenta la visión del usuario, eslabón final que, muchas veces, es el más débil de la cadena. El segundo capítulo se centra en los profesionales más próximos al desarrollo y uso de software criptográfico, invitándoles a adentrarse en los principios teóricos de la criptografía simétrica y asimétrica, con un lenguaje asequible salpicado de ejemplos para apoyar la comprensión del texto. Además de explicar herramientas muy establecidas como AES, RSA o ECDSA, en este capítulo

[1] En este contexto, antiguo es un término ambiguo; se aplica tanto a esquemas diseñados hace siglos como a aquellos que apenas han alcanzado la mayoría de edad

se realiza una introducción a diferentes temas menos habituales en este tipo de textos, como la criptografía cuántica y postcuántica, el blockchain o las tecnologías PET *(Privacy-Enhancing Technologies*). Otros temas de gran utilidad relacionados con cuestiones eminentemente prácticas (gestores de credenciales, librerías criptográficas, auditoría de código criptográfico) se entrelazan con conceptos más teóricos (seguridad demostrable, criptoagilidad) para dotar al lector de un abanico de nociones elementales muy completo, salpicado de referencias útiles para profundizar en cada una de las cuestiones tratadas en el texto.

El desarrollo de tecnologías cuánticas ha supuesto una enorme revolución en distintos ámbitos, siendo la criptografía quizá el más destacado. Sin duda, los profesionales que trabajan en Ciberseguridad se han visto en los últimos años sobrepasados ante la perspectiva de entender construcciones y contrarrestar ataques que se apoyan en los fundamentos de la Mecánica Cuántica. Este nuevo paradigma computacional exige una revisión profunda de nuestra concepción de la seguridad, y abre a la vez una infinidad de posibilidades para la implementación de herramientas criptográficas con propiedades de seguridad impensables en el pasado, derivadas del hecho de que *observar* o medir información cuántica tenga un impacto detectable sobre la misma. El tercer capítulo del libro nos invita a entender los peligros reales del desarrollo de herramientas cuánticas para el criptoanálisis, así como los pasos que la comunidad criptográfica está dando para enfrentarse a esta amenaza. A través de una breve introducción a la computación cuántica, que incluye una descripción didáctica del algoritmo de Shor y su uso para factorizar enteros, se presenta al lector de manera sencilla alguna de las soluciones exploradas hacia diseños criptográficos no basados en factorización de enteros ni en logaritmo discreto. En particular, se explican propuestas como el encapsulado de clave Crystals-Kyber o la firma Sphincs+, ambos esquemas a la cabeza en la carrera por convertirse en el estándar (oficial y, de facto) de la Criptografía postcuántica.

Los capítulos cuatro y cinco del libro recopilan y amplían el material que se expuso (en parte) en la anterior edición de este libro. Dicho material se ha actualizado y enriquecido siempre desde la perspectiva de uno de los mejores expertos nacionales en esteganografía y hacking ético. Por último, el libro concluye con un capítulo dedicado a la formación continua, que contiene una guía breve y completa para invitar al lector a profundizar y actualizar sus conocimientos.

Alfonso Muñoz ha conseguido recopilar, en apenas 400 páginas, punteros a la mayoría de las áreas de interés para los profesionales de la Ciberseguridad que quieren adentrarse en el fascinante mundo de la Criptografía. Su obra es

una puerta abierta a un mundo de ideas y construcciones en el que podemos deslizarnos sin demasiados conocimientos previos, y del que volver con importantes lecciones aprendidas. Aún más importante, traspasamos la puerta de vuelta con energías renovadas y menos reticencia para profundizar en la teoría y práctica de esta fascinante disciplina.

María Isabel González Vasco es licenciada en Matemáticas y doctora por la Universidad de Oviedo (obteniendo en ambos casos el Premio Extraordinario). Desarrolla su labor investigadora en el campo de la **Criptografía Matemática** desde el año 1999, en el que disfrutó de una estancia de investigación (Programa Leonardo da Vinci) en la empresa Philips Crypto B.V. (Eindhoven, Holanda). En los años siguientes su interés se centró en dos áreas de trabajo; funciones **Hard-Core y Criptografía basada en Teoría de Grupos.** En el primer campo, alcanzó importantes resultados (en colaboración con investigadores de la talla de Igor E. Spharlinski y M. Näslund) con implicaciones prácticas relativas a la seguridad del esquema de intercambio de clave de Diffie-Hellman. En cuanto a Criptografía basada en Teoría de Grupos, tema que centró su tesis doctoral, criptoanalizó numerosas propuestas para aplicar esta teoría al cifrado de mensajes y al intercambio seguro de claves criptográficas. Desde 2007 se interesa además por la seguridad demostrable de esquemas de **intercambio de clave multiusuario**, en concreto por la búsqueda de diseños que permitan a un conjunto de usuarios acordar una clave criptográfica segura común comunicándose exclusivamente a través de una red vulnerable. En ese marco, actualmente trabaja en desarrollos y modelos matemáticos para **criptografía postcuántica**, ámbito en el que codirige un proyecto del programa SPS de la OTAN.

Introducción - ¿Qué no es este libro?

WILL - Lo más triste de todo es que dentro de 50 años
empezarás a pensar por ti mismo, y te darás
cuenta de que solo hay dos verdades en la vida:
uno, que los pedantes sobran, y dos,
que has tirado 150.000 dólares en una educación
que te habría costado un dólar cincuenta por los retrasos
en la biblioteca pública.
CLARK - Sí, pero yo tendré un título, y tú servirás patatas fritas
a mis hijos
WILL - Es posible, pero yo seré una persona de verdad

Matt Damon –
El indomable Will Hunting

Cuando era un estudiante a tiempo completo disfrutaba enormemente de la estancia en bibliotecas públicas. A veces se nos olvida el poder de lo público y lo gratuito. Esa sensación de conocimiento concentrado y esa libertad de descubrir lo que ningún motor de inteligencia artificial podría, descubrir aquel libro que nunca nadie podría recomendarme simplemente porque "no me iba a gustar".

En esa etapa, descubrí un libro que me llamó poderosamente la atención *"La cultura. Todo lo que hay que saber"* de *Dietrich Schwanitz*, una especie de libro sagrado que resumía en un volumen los aspectos más significativos de disciplinas tan variadas como la filosofía, la historia del arte, la música, la historia de Europa, los griegos, la Ilíada, la antigüedad clásica, el renacimiento, la literatura contemporánea. Un libro que, al menos, te permitiría mantener *conversaciones de bar* pareciendo una persona leída y cultivada, y quizás, te permitiera aprender más rápido eliminando información, a priori, ornamental.

Nadie se convierte en un experto en ninguna materia por leer un libro. Pero la capacidad de síntesis de ese libro me pareció significativa y me permitió descubrir aspectos que desconocía y que, en principio, me parecían tremendamente aburridos, y poner foco en otros de manera intensiva.

La primera versión de este libro nació con este objetivo. Un libro de criptografía práctica que sirviera de referencia a la mayor cantidad de personas posibles independientemente de su conocimiento criptográfico y que le facilitara profundizar en cada área específica. Con ese planteamiento, el libro se configuró en diferentes capítulos que de manera breve y concisa reflejan múltiples aristas del uso de la criptografía en el mundo real, en su

uso práctico. Con una idea clara en la mente, la bibliografía proporcionada debería ser lo suficientemente amplia para permitir al lector profundizar en todo el detalle necesario, sin añadir nada que estuviera mejor escrito en otras obras. Referencias de diferente naturaleza, en español y en inglés, priorizando siempre aquellas de fácil acceso y sin coste. El lector debería sentir el mundo que se me abrió después de leer el libro de Dietrich hace unas décadas.

Desde la primera edición de este libro han pasado casi 4 años. Sigo convencido de la importancia de esta obra y era necesario su actualización. La estructura esencial del libro se mantiene pero con nuevos apartados, actualización de referencias, corrección de errores y nuevos capítulos cubriendo las nuevas tendencias alrededor de esta apasionante disciplina.

Siempre he creído que la criptografía y la esteganografía ayudan a construir una sociedad más libre y justa. Espero que una vez más este libro ayude en esa dirección.

Dr. Alfonso Muñoz es experto en ciberseguridad, área en la que trabaja profesionalmente desde hace 22 años. Su principal actividad se centra en proyectos/tecnologías técnicas avanzadas en seguridad defensiva y ofensiva (Global 500) y su colaboración con organismos públicos. Su especialización se centra en la seguridad ofensiva, la protección de comunicaciones (criptografía y esteganografía) y la investigación avanzada en ciberseguridad.

Su actividad profesional ha sido reconocida con múltiples reconocimientos académicos e industriales, entre ellos por reportar vulnerabilidades en productos de gran uso (Google, Microsoft, etc.). Destaca su perfil divulgador, entre otras áreas, en el área de la criptología. Es coautor de la red temática Criptored que difunde desde hace más de 22 años millones de documentos y formación online gratuita a toda la comunidad hispanohablante.

Contacto
Twitter: @mindcrypt
Telegram: t.me/criptored
Correo: alfonso@criptored.com