

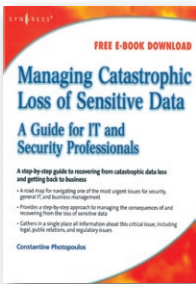
MODERN CRYPTANALYSIS Techniques for Advanced Code Breaking

Autor: Christopher Swenson
Editorial: Wiley
Año: 2008 – 236 páginas
ISBN: 978-0-470-13593-8
www.wiley.com

Esta obra, elaborada por **Christopher Swenson**, profesor de seguridad, telecomunicaciones y criptoanálisis en la Universidad norteamericana de Tulsa, proporciona los fundamentos del criptoanálisis tradicional, examina cifradores basados en la teoría de números, explora cifradores de bloques, y muestra las bases del criptoanálisis moderno, tanto el diferencial como el lineal. El manual, dirigido tanto a profesionales noveles en la materia como a los más veteranos, realiza al comienzo una aproximación a la ciencia en la que se sustenta: la criptología, entendida como el

arte de proteger la transferencia de información, que se divide a su vez en dos ramas: la criptografía, o creación de códigos para ocultar la información; y el criptoanálisis, consistente en el desarrollo de técnicas para descifrar esos códigos.

En cuanto a la estructura de la obra, ésta consta de siete capítulos cuyos epígrafes son: **1. Cifradores Simples; 2. Cifradores de la Teoría de Números; 3. Logaritmos Factorizados y Discretos; 4. Cifradores de Bloques; 5. Métodos Generales de Criptoanálisis; 6. Criptoanálisis Lineal; y 7. Criptoanálisis Diferencial.**



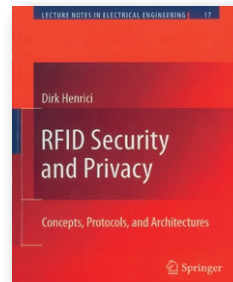
MANAGING CATASTROPHIC LOSS OF SENSITIVE DATA A Guide for IT and Security Professionals

Autor: Constantine Photopoulos
Editorial: Syngress
Año: 2008 – 293 páginas
ISBN 13: 978-1-59749-239-3
www.syngress.com

Managing Catastrophic Loss of Sensitive Data es una guía escrita por **Constantine Photopoulos**, el socio director de la práctica nacional Sarbanes-Oxley de los Estados Unidos, del Grupo SOX, que enseña, paso a paso, a crear programas de seguridad de datos, controles de protección, y procedimientos y salvaguardas técnicas contra varias posibles fuentes de fuga de información.

El libro también se detiene en otros aspectos de interés como son los de limitar el alcance del incidente, así como en el controvertido ámbito de la notificación de brechas de seguridad, acción que considera crítica con el fin de cumplir con los requisitos legales, gestionar la reputación y el riesgo legal de la organización, y permitir a las víctimas adoptar medidas de protección frente a las consecuencias del robo de identidad o el fraude.

El volumen se divide en nueve capítulos, en el primero de los cuales se explican algunos términos ligados a este tipo de incidentes, avanzando igualmente los contenidos de los apartados restantes: **2. Clasificación de Datos; 3. Controles y Salvaguardas; 4. Política de Seguridad de Datos; 5. Programa de Respuesta; 6. Detección y Reporte; 7. Evaluación y Respuesta; 8. Revelación y Notificación y 9. Cierre**, en el que se contempla la fase final del proceso, en la que se tienen en cuenta las lecciones aprendidas, el análisis de costes, el análisis de la causa raíz, un plan de acciones correctivas, informes de seguimiento, y documentación al respecto del evento de seguridad. Finalmente, en el apéndice, se recogen legislaciones y regulaciones internacionales relacionadas con las fugas de datos.



RFID SECURITY AND PRIVACY Concepts, Protocols and Architectures

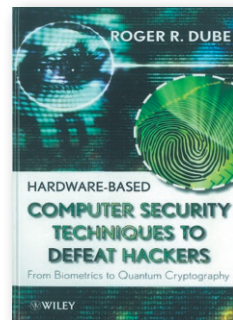
Autor: Dirk Henrici
Editorial: Springer
Año: 2008 – 269 páginas
ISBN: 978-3-540-79075-4
www.springer.com

Esta obra analiza con detalle los trabajos que actualmente están llevando a cabo los investigadores del ámbito de la Identificación por Radio Frecuencia (RFID), para afrontar los diversos problemas que esta tecnología presenta, en relación con la seguridad y la privacidad.

En el texto se examina también el punto de vista de los atacantes, sus fortalezas, y los distintos tipos de ataques. Asimismo se comentan problemáticas concretas, como la de aportar seguridad a las comunicaciones inalámbricas entre las etiquetas y los lectores de éstas; se indaga en una serie de funcionalidades que necesitan ser implementadas en las tarjetas; y se introduce, además,

un número de protocolos que proveen de seguridad y garantizan la privacidad al utilizar sistemas RFID, como por ejemplo el protocolo conocido como "*Hash-based ID variation*".

Es asimismo destacable que la obra dedique varias páginas a las infraestructuras de pseudonimización, que son propuestas por el autor como medio para obtener información adicional sobre una etiqueta de RFID, sin revelar la identidad de la organización responsable de ésta y, por otra parte, en el texto se extiende el modelo del sistema de RFID, para dar apoyo a otros sistemas de RFID inter-organizacionales, con el fin de alcanzar los requisitos de privacidad y seguridad identificados.



HARDWARE-BASED COMPUTER SECURITY TECHNIQUES TO DEFEAT HACKERS From Biometrics to Quantum Cryptography

Autor: Roger R. Dube
Editorial: Wiley
Año: 2008 – 227 páginas
ISBN: 978-0-470-19339-6
www.wiley.com

La presente obra parte del hecho de que proteger la información personal valiosa contra el robo es un problema creciente y serio en la actual comunidad de los negocios electrónicos, aunque tiempo atrás han sido muchas las acciones que desde los departamentos de Inteligencia y Defensa se han llevado a cabo, utilizando en buena parte de las ocasiones dispositivos de seguridad basados en hardware para construir sistemas que sean impenetrables para los *hackers*. En este sentido, la obra después de proporcionar un repaso por conceptos básicos de seguridad informática y técnicas de análisis, se adentra en el terreno de las tecnologías de seguridad basadas en hardware, deteniéndose en aspectos como los generadores de números aleatorios basados en física, dispositivos biométricos, sistemas informáticos de confianza, o criptografía

cuántica, entre otros.

Asimismo, de forma específica, realiza un amplio análisis sobre los siguientes temas: elementos de seguridad informática; aproximaciones y ataques a la criptografía; generación y distribución de claves, aproximaciones y ataques; las cualidades de las soluciones de seguridad viables; coprocesadores seguros; carga de auto-iniciación segura; gestión de memoria segura y tecnología de ejecución confiable; el módulo de plataforma de confianza; matriz de puertas programables; autenticación basada en hardware; biometría; *tokens*; y tecnologías de localización. Como broche final, la obra incluye un capítulo dedicado a mostrar a los lectores cómo pueden ellos implementar las estrategias y tecnologías tratadas en el texto, y concluye con dos ejemplos de implementaciones seguras.