Librería

Bonilla y Asociados

desde 1950

Título:

Autor: **Precio:** Desconocido

Editorial: **Año:** 2007

Tema: **Edición:** 1ª

Sinopsis **ISBN:** 9781590597842

Foundations of Security: What Every Programmer Needs to Know teaches new and current software professionals state-of-the-art software security design principles, methodology, and concrete programming techniques they need to build secure software systems. Once you re enabled with the techniques covered in this book, you can start to alleviate some of the inherent vulnerabilities that make today s software so susceptible to attack. The book uses web servers and web applications as running examples throughout the book. For the past few years, the Internet has had a wild, wild west flavor to it. Credit card numbers are stolen in massive numbers. Commercial web sites have been shut down by Internet worms. Poor privacy practices come to light and cause great embarrassment to the corporations behind them. All these security-related issues contribute at least to a lack of trust and loss of goodwill. Often there is a monetary cost as well, as companies scramble to clean up the mess when they get spotlighted by poor security practices. It takes time to build trust with users, and trust is hard to win back. Security vulnerabilities get in the way of that trust. Foundations of Security: What Every Programmer Needs To Know helps you manage risk due to insecure code and build trust with users by showing how to write code to prevent, detect, and contain attacks. * The lead author co-founded the Stanford Center for Professional Development Computer Security Certification. * This book teaches you how to be more vigilant and develop a sixth sense for identifying and eliminating potential security vulnerabilities. * You ll receive hands-on code examples for a deep and practical understanding of security. * You ll learn enough about security to get the job done. Table of Contents * Security Goals * Secure Systems Design * Secure Design Principles * Exercises for Part 1 * Worms and Other Malware * Buffer Overflows * Client-State Manipulation * SQL Injection * Password Security * Cross-Domain Security in Web Applications * Exercises for Part 2 * Symmetric Key Cryptography * Asymmetric Key Cryptography * Key Management and Exchange * MACs and Signatures * Exercises for Part 3.