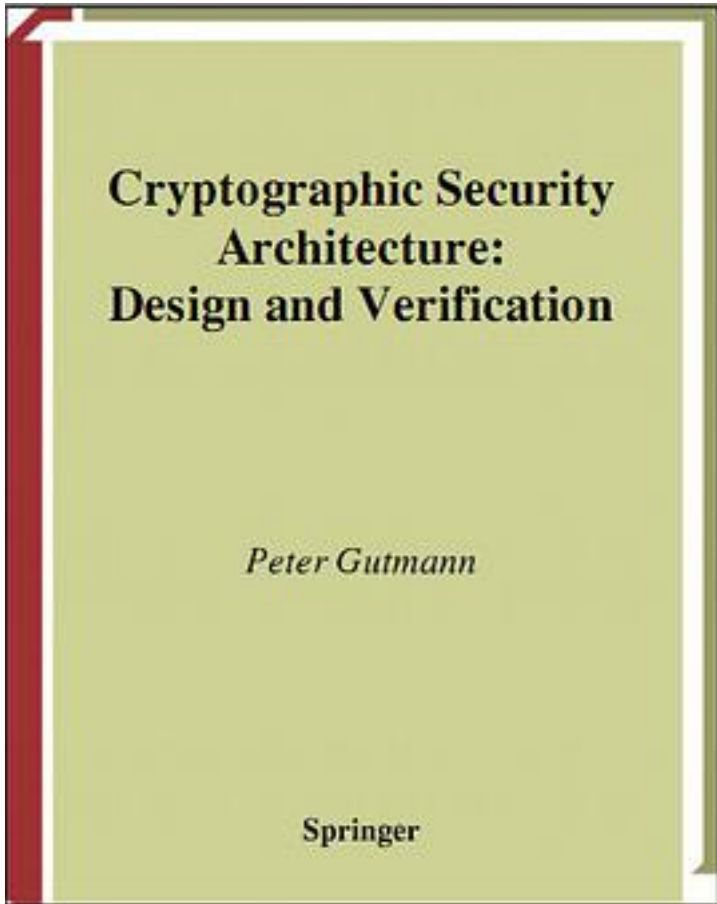# Cryptographic Security Architecture: Design and Verification

[Cryptographic Security Architecture: Design and Verification_下载链接1_](#)

著者:Peter Gutmann

出版者:Springer

出版时间:2003-10-1

装帧:Hardcover

isbn:9780387953878

A cryptographic security architecture is the collection of hardware and software that protects and controls the use of encryption keys and similar cryptovariables. It is the

foundation for enforcing computer security policies and controls and preempting system misuse.

This book provides a comprehensive design for a portable, flexible high-security cryptographic architecture, with particular emphasis on incorporating rigorous security models and practices. "Cryptographic Security Architecture" unveils an alternative means of building a trustworthy system based on concepts from established software engineering principles and cognitive psychology. Its novel security-kernel design implements a reference monitor that controls access to security-relevant objects and attributes based on a configurable security policy.

Topics and features:

* Builds a concise architectural design that can be easily extended in the future

* Develops an application-specific security kernel that enforces a fully customizable, rule-based security policy

* Presents a new verification technique that allows verification from the high-level specification down to the running code

* Describes effective security assurance in random number generation, and the pitfalls associated therewith

* Examines the generation and protection of cryptovariables, as well as application of the architectural design to cryptographic hardware

The work provides an in-depth presentation of a flexible, platform-independent cryptographic security architecture suited to software, hardware, and hybrid implementations. Security design practitioners, professionals, researchers, and advanced students will find the work an essential resource.

作者介绍:

目录:

Cryptographic Security Architecture: Design and Verification_下载链接1_

标签

评论

[Cryptographic Security Architecture: Design and Verification_下载链接1_](#)

书评