Security policy in system-on-chip designs: Specification, implementation and verification

Ray, Sandip, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=9999920521672&lokasi=lokal

----

Abstrak

This book offers readers comprehensive coverage of security policy specification using new policy languages, implementation of security policies in Systems-on-Chip (SoC) designs – current industrial practice, as well as emerging approaches to architecting SoC security policies and security policy verification. The authors focus on a promising security architecture for implementing security policies, which satisfies the goals of flexibility, verification, and upgradability from the ground up, including a plug-and-play hardware block in which all policy implementations are enclosed. Using this architecture, they discuss the ramifications of designing SoC security policies, including effects on non-functional properties (power/performance), debug, validation, and upgrade. The authors also describe a systematic approach for "hardware patching", i.e., upgrading hardware implementations of security requirements safely, reliably, and securely in the field, meeting a critical need for diverse Internet of Things (IoT) devices.
- Provides comprehensive coverage of SoC security requirements, security policies, languages, and security architecture for current and emerging computing devices;
- Explodes myths and ambiguities in SoC security policy implementations, and provide a rigorous treatment of the subject;
- Demonstrates a rigorous, step-by-step approach to developing a diversity of SoC security policies;
- Introduces a rigorous, disciplined approach to "hardware patching", i.e., secure technique for updating hardware functionality of computing devices in-field;
- Includes discussion of current and emerging approaches for security policy verification.