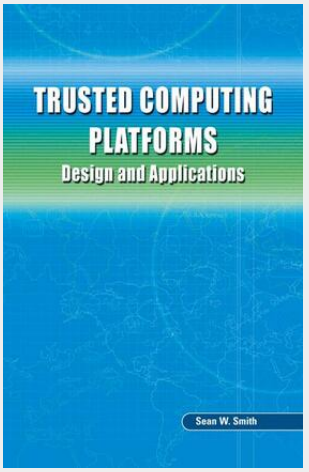
Smith

Trusted Computing Platforms

Design and Applications



How can one trust computation taking place at a remote site, particularly if a party at that site might have motivation to subvert this trust? In recent years, industrial efforts have advanced the notion of a "trusted computing platform" as a building block. Through a conspiracy of hardware and software magic, these platforms attempt to solve this remote trust problem, to preserve various critical properties against various types of adversaries. However, these current efforts are just points on a larger continuum, which ranges from earlier work on secure coprocessor design and applications, through TCPA/TCG, to recent academic developments. Without wading through stacks of theses and research literature, the general computer science reader cannot see this big picture. Trusted Computing Platforms: Design and Applications fills this gap. Starting with early prototypes and proposed applications, this book surveys the longer history of amplifying small amounts of hardware security into broader system security – and reports real case study experience with security architecture and applications on multiple types of platforms. The author examines the theory, design, and implementation of the IBM 4758 secure coprocessor platform and discusses real case study applications that exploit the unique capabilities of this platform. The author discusses how these foundations grow into newer industrial designs, and discusses alternate architectures and case studies of applications that this newer hardware can enable. The author closes with an examination of more recent cutting-edge experimental work in this area. Trusted Computing Platforms: Design and Applications is written for security architects, application designers, and the general computer scientist interested in the evolution and uses of this emerging technology.

How can one trust computation taking place at a remote site, particularly if a party at that site might have motivation to subvert this trust? In recent years, industrial efforts have advanced the notion of a "trusted computing platform" as a building block. Through a conspiracy of hardware and software magic, these platforms attempt to solve this remote trust problem, to preserve various critical properties against various types of adversaries. However, these current efforts are just points on a larger continuum, which ranges from earlier work on secure coprocessor design and applications, through TCPA/TCG, to recent academic developments. Without wading through stacks of theses and research literature, the general computer science reader cannot see this big picture. Trusted Computing Platforms: Design and Applications fills this gap. Starting with early prototypes and proposed applications, this book surveys the longer history of amplifying small amounts of hardware security into broader system security – and reports real case study experience with security architecture and applications on multiple types of platforms. The author examines the theory, design, and implementation of the IBM 4758 secure coprocessor platform and discusses real case study applications that exploit the unique capabilities of this platform. The author discusses how these foundations grow into newer industrial designs, and discusses alternate architectures and case studies of applications that this newer hardware can enable. The author closes with an examination of more recent cutting-edge experimental work in this area. Trusted Computing Platforms: Design and Applications is written for security architects, application designers, and the general computer scientist interested in the evolution and uses of this emerging technology.

106,99 €
99,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9780387239163
Medium: Buch
ISBN: 978-0-387-23916-3
Verlag: Springer Nature Singapore
Erscheinungstermin: 10.12.2004
Sprache(n): Englisch
Auflage: 2005. Auflage 2004
Produktform: Gebunden
Gewicht: 1200 g
Seiten: 239
Format (B x H): 162 x 242 mm

Kundenservice Fachmedien Otto Schmidt
Neumannstraße 10, 40235 Düsseldorf | kundenservice@fachmedien.de | 0800 000-1637 (Inland)