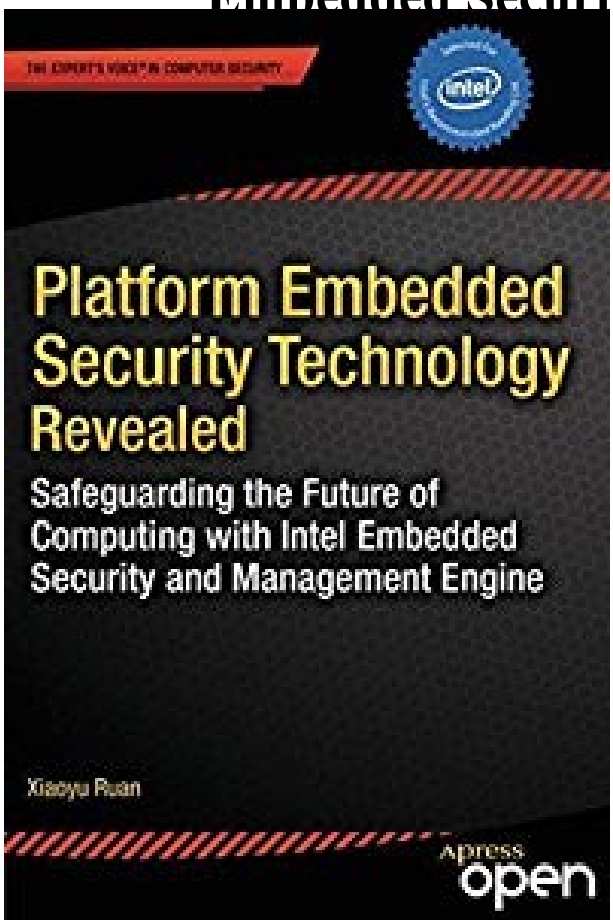
Platform Embedded Security Technology Revealed: Safeguarding the Future of Computing with Intel Embedded Security and Management Engine



ASIN	B00K6N4JU8
Pages:	272
Genre:	Uncategorized
Author:	Xiaoyu Ruan
Language	English
Goodreads Rating:	3.30
Published:	August 10th 2014 by Apress

Platform Embedded Security Technology Revealed is an in-depth introduction to Intel’s platform embedded solution: the security and management engine. The engine is shipped inside most Intel platforms for servers, personal computers, tablets, and smartphones. The engine realizes advanced security and management functionalities and protects applications’ secrets and users’ privacy in a secure, light-weight, and inexpensive way. Besides native built-in features, it allows third-party software vendors to develop applications that take advantage of the security infrastructures offered by the engine. Intel’s security and management engine is technologically unique and significant, but is largely unknown to many members of the tech communities who could potentially benefit from it. Platform Embedded Security Technology Revealed reveals technical details of the engine. The engine provides a new way for the computer security industry to resolve critical problems resulting from booming mobile technologies, such as increasing threats against confidentiality and privacy. This book describes how this advanced level of protection is made possible by the engine, how it can improve users’ security experience, and how third-party vendors can make use of it. It's written for computer security professionals and researchers; embedded system engineers; and software engineers and vendors who are

interested in developing new security applications on top of Intel’s security and management engine. It’s also written for advanced users who are interested in understanding how the security features of Intel’s platforms work. What you□ll learn The cyber security challenges behind the creation of the embedded security and management engine, and the solutions it presents The pros and cons of enforcing security in the embedded engine Basic cryptography and security infrastructure of the engine Security-hardening features of the engine Handling dynamically loaded applications How anonymous authentication works with enhanced privacy protection Content protection at the hardware level Secure boot with a hardware root of trust Firmware-based TPM Identity protection with a hardware-based, one-time password Who this book is for Computer security professionals and researchers; embedded system engineers; software engineers and vendors who are interested in developing new security applications on top of Intel’s security and management engine; OEM (such as Lenovo, HP, etc.) marketing and R&D staff.