DE GRUYTER

Dengguo Feng, Yu Qin,
Xiaobo Chu, Shijun Zhao

TRUSTED COMPUTING

PRINCIPLES AND APPLICATIONS

ADVANCES IN COMPUTER SCIENCE 2

DE G

清華大學出版社
TSINGHUA UNIVERSITY PRESS

Prominent threats on computers and networks usually originate from the situation in which computer architecture lacks the protection against malicious code. Thus it is a core issue to form an immune system in the computer architecture and ensure a computer platform runs securely. Trusted computing is a new kind of security technology proposed under this background. It aims at establishing system transfer trust by improving the security of the computer architecture, so as to ensure the security of computing platforms and solve the trust problems of man-to-program, man-to-computer and man-to-man relations.

The authors of this book have more than ten years of experience in research on trusted computing. They carried out in-depth and systematic research on key technologies of trusted computing and made breakthroughs in several key aspects of trusted computing. Based on their research, this book summarizes key concepts, theories and technologies in trusted computing, e.g. TPM, TCM, mobile trusted modules, chain of trust, trusted software stack, etc., and discusses remote attestation and trust network connections. It also collects and comments on the most representative works from all over the world, which gives a deep and comprehensive perspective of trusted computing. In addition, this book emphasizes application in practice, extending readers from computer science and information science researchers to industrial engineers.

THE SERIES: ADVANCES IN COMPUTER SCIENCE

The series is devoted to the publication of high level monographs in all aspects of computer science with focuses on emerging topics such as network security, human-computer-interaction, software engineering, database and bioinformatics etc. Theoretical research and industrial applications are well balanced, making the series a valuable reference for both university researchers and industrial R&D engineers.

www.degruyter.com
ISBN 978-3-11-047604-0
ISSN 2509-7253

ACS 2

Dengguo Feng, Yu Qin, Xiaobo Chu, Shijun Zhao

TRUSTED COMPUTING

DE G

Dengguo Feng, Yu Qin,
Xiaobo Chu, Shijun Zhao

Trusted Computing

Principles and Applications

DE GRUYTER

清華大學出版社
TSINGHUA UNIVERSITY PRESS

This work is co-published by Tsinghua University Press and Walter de Gruyter GmbH.

Authors

Dengguo Feng
Yu Qin
Xiaobo Chu
Shijun Zhao
Institute of Software, Chinese Academy of Science.

ISBN 978-3-11-047604-0
e-ISBN (PDF) 978-3-11-047759-7
e-ISBN (EPUB) 978-3-11-047609-5
Set-ISBN 978-3-11-047760-3
ISSN 2509-7253

Library of Congress Cataloging-in-Publication Data
A CIP catalog record for this book has been applied for at the Library of Congress.

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.dnb.de.

Typesetting: Integra Software Services Pvt. Ltd.
Printing and binding: CPI books GmbH, Leck
♾ Printed on acid-free paper
Printed in Germany

www.degruyter.com

Dengguo Feng, Yu Qin, Xiaobo Chu, Shijun Zhao
Trusted Computing

Advances in Computer Science

—

Volume 2

Preface

With further development of computer network, the three most prominent threats are gradually highlighted, including attacks from malicious code, illegal stealing of information and illegal corruption of data and system. Within these threats, attacks from malicious code have surpassed traditional computer virus to be the predominant threat to private information of computer users. These threats originate from the situation that computer architecture lacks an immune system against malicious code. Thus, it is a core issue to accommodate immune system in computer architecture and ensure a computer platform to run securely and trustworthily.

Trusted computing is a kind of technique proposed under this background. By establishing a mechanism of integrity measurement, trusted computing enables computing platforms to distinguish between trusted programs and untrusted programs. In this way, computing platforms employ reliable countermeasures to prevent untrusted programs from disrupting.

I led a team starting research in trusted computing technique as early as 2003. Since 2006, I have been the chairman of TCMU (Trusted Cryptography Module Union) of China. I actively promote research, development and industrialization of trusted computing in China, and have achieved satisfactory results. Our team has taken a number of national research projects, including projects from Chinese 863 Program, industrialization projects of high technique from National Development and Reform Committee and major programs from National Natural Science Foundation. We have made breakthrough in several key aspects of trusted computing, including establishing and repairing technique of chain of trust, remote attestation protocol based on TCM and automatic generation method of test use cases based on reduction. We have also proposed a series of products, including advanced security supporting platform of trusted computing with self-owned intellectual property and test and evaluation system of trusted computing that supports compliance test, security test and performance test of trusted computing. These products have obtained good social and economic benefits now. Our research result "Research and Application on the Security Supporting Platform and Key Technique for Trusted Computing" achieved the first prize of Information Science Technique awarded by Chinese Institute of Electronics in 2010. In the future, we will continue our work and strive for better achievements and greater honor.

This book includes eight chapters. Chapter 1 is introduction. We introduce the research background, development status of technique and our contributions. Chapter 2 introduces trusted platform module, including TPM, TCM and MTM (Mobile Trusted Module). Chapter 3 focuses on establishing techniques of chain of trust, including root of trust, systems based on static and dynamic chain of trust and chain of trust in virtualization platforms. Chapter 4 discusses trusted software stack, including TSS (TCG Software Stack), TSM (TCM Service Module) and development of trusted application.

DOI 10.1515/9783110477597-202

Chapter 5 describes trusted computing platform, such as PC, server, trusted mobile platform, trusted virtualized platform and applications of trusted computing platform. Chapter 6 introduces test and evaluation of trusted computing, including test and evaluation of trusted platform module, analysis of trusted computing security mechanism, certification and evaluation of trusted computing and comprehensive test and analysis system of trusted computing platform. Chapter 7 introduces remote attestation, and Chapter 8 proposes trusted network connection.

The main content of this book comes from my formal monograph "Trusted Computing – Theory and Practice" (ISBN:9787302314226), which is written in Chinese and published by Tsinghua University Press in 2013. We've made our effort to translate the monograph,make corrections on its contents which are outdated and add a few new technologies, so as to present the highest quality collection of trusted computing technology. A group of my colleagues and doctor candidates have participated in writing and proofreading this book, including Yu Qin, Xiaobo Chu, Shijun Zhao, Jing Xu, Dexian Chang, Jianxiong Shao, Weijin Wang, Bo Yang, Bianxia Du and Wei Feng. We have also got great help from many researchers and editors. We want to express my sincere thanks to them here.

Dengguo Feng
March 17, 2017.

Contents

1 Introduction

With rapid development of cloud computing, Internet of Things and mobile Internet, information technology has changed society management and public life profoundly, and ubiquitous information has already been treated as important digital assets of a nation, an enterprise or a person. Considering widespread computer virus, malicious software and enhanced hacker technique, these important assets are facing more and more practical threats. It is no doubt a preferential security requirement from nation, enterprise and person that a trustworthy computing environment should be built to maintain confidentiality, integrity, authenticity and reliability of information. Traditional security technologies like firewall, IDS and virus defense usually focus on server-side computing platforms, thus relatively vulnerable client-side terminals are gradually becoming the weak link of an information system. Against these requirements and threats, trusted computing (TC) technology aims at establishing a trust transfer system by improving the security of computer architecture, so as to ensure the security of platform and solve the trust problem of man-to-program, man-to-computer and man-to-man.

Trusted computing is an emerging technology under this background. Up to now, there exist many different ways of understanding of "trusted." Several authoritative organizations, such as ISO/IEC, IEEE and TCG (Trusted Computing Group), have made efforts to establish their own explicit definitions [1–3]. TCG has further proposed a novel and widely accepted solution for enhancing security of computer system by embedding TPM (Trusted Platform Module) into hardware platform. In this book, our point of view is similar to that of TCG. We argue that a "trusted" computer system should always act in an expected way, and this property could be achieved by a trusted computing environment established upon a dedicated security chip.

Early in the middle of 1990s, some computer manufacturers began to research security solutions based on trusted computing technology. By adding a security chip into computer hardware, these solutions implement a series of mechanisms, such as the root of trust, secure storage and chain of trust, and achieve the secure goal of trusted computing environment. This kind of technical schemes was widely accepted by the IT industry, and as a result TCPA (Trusted Computing Platform Alliance, a mainstream industry alliance of trusted computing technique) was founded in 1999. After TCPA proposed TPM1.1 specifications in 2001, trusted computing products proposed by some mainstream IT manufacturers were gradually accepted by market and industry society. In 2003, TCPA was renamed to TCG and owned about 200 members, including nearly all international mainstream IT manufacturers. Technical specifications proposed by TCG had already formed a systematic architecture, which involves major IT areas like security chip, PC, server and network, and four core specifications were accepted as ISO standards in 2009. By 2010, TPM had already been a standard component of laptop and desktop, and mainstream PC-related manufacturers such as Microsoft and Intel also had adopted trusted computing in their core products.

DOI 10.1515/9783110477597-001

As a country with special security requirements and supervision rules, China has made achievement on both products and specifications of trusted computing. TCM, referred to as DNA of Chinese information security, is the most important contribution of China in trusted computing area. Upon its own cryptographic algorithm, China has established TCM-centered specification architecture of its trusted computing technology. Broadly speaking, development of Chinese trusted computing technology has undergone the following three phases.

From 2001 to 2005, China concentrated on tracking and absorbing concepts of TCG technology. Manufacturers like Lenovo and SinoSun published TCG-compliant products, and Work Group 1 of National Information Security Standardization Technical Committee (TC260) founded a special trusted computing workgroup that greatly impulsed trusted computing standard research.

From 2006 to 2007, China established architecture of its own trusted computing theory, technology and standards. In these years, China carried out research on trusted computing technical solution based on its own cryptography algorithms and proposed "cryptographic application scheme for trusted computing." China also set up a special workgroup on researching application of trusted computing technology. Later, this group changed its name to China TCM Union (TCMU). TCMU published TCM-centered specification "Technical Specification of Cryptographic Support Platform for Trusted Computing" [4] and "Functionality and Interface Specification of Cryptographic Support Platform for Trusted Computing" in December 2007.

After 2008, China focused on promoting its trusted computing industry. A series of TCM products have been put on the market and well accepted by governments, military troops and civilian areas. TCMU has nearly 30 members now, including Lenovo, Tongfang and NationZ, and has greatly given impulse to Chinese trusted computing industry with the support of Chinese government. Until 2010, TCMU established a comprehensive trusted computing industry system, including security chip, trusted computer, trusted network, trusted application and test/evaluation of trusted computing products. To promote industrialization of trusted computing, special committee of information security of China Information Industry Association has founded China Trusted Computing Union (CTCU) in 2008.

1.1 Related Work

The purpose of trusted computing technology is to improve computer architecture by introducing trusted computing security chip so as to enhance trustworthiness of common computing platform and network. TCG embeds TPM into PC or server's motherboard and provides several novel security mechanisms [5]. Microsoft has started NGSCB [6] plan. In NGSCB, a trusted execution environment based on microkernel is built to enhance Windows security and privacy. Meanwhile, Intel dedicates to TXT [7] hardware security technology to implement trusted computing through a series of hardware, including CPU, chipset and IO devices. China also manages to release