Lecture Notes in Electrical Engineering 203

Sang-Soo Yeo · Yi Pan
Yang Sun Lee · Hang Bae Chang *Editors*

Computer Science and its Applications

CSA 2012

Springer

Lecture Notes in Electrical Engineering

Volume 203

For further volumes:
http://www.springer.com/series/7818

Sang-Soo Yeo · Yi Pan
Yang Sun Lee · Hang Bae Chang
Editors

Computer Science and its Applications

CSA 2012

Springer

Editors
Sang-Soo Yeo
Department of Electrial Engineering
and Computer Science
Mokwon University
Daejeon
Republic of South Korea

Yi Pan
Department of Computer Science
Georgia State University
Atlanta, GA
USA

Yang Sun Lee
Division of Computer Engineering
Mokwon University
Daejeon
Republic of South Korea

Hang Bae Chang
Division of Business Administration
Sangmyung University
Seoul
Republic of South Korea

ISSN 1876-1100 ISSN 1876-1119 (electronic)
ISBN 978-94-007-5698-4 ISBN 978-94-007-5699-1 (eBook)
DOI 10.1007/978-94-007-5699-1
Springer Dordrecht Heidelberg New York London

Library of Congress Control Number: 2012949371

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Orgainzation Committee

Welcome Message from the General Chairs

CSA 2012

Welcome to the 4th FTRA International Conference on Computer Science and its Applications (CSA 2012), going to be held in the Jeju Island, Korea.

CSA 2012 is the next event in a series of highly successful International Conference on Computer Science and its Applications, previously held as CSA 2008 (Australia, October, 2008), CSA 2009 (Jeju, December, 2009), and CSA 2011(Jeju, December, 2011).

The CSA 2012 will be the most comprehensive conference focused on the various aspects of advances in computer science and its applications. The CSA 2012 will provide an opportunity for academic and industry professionals to discuss the latest issues and progress in the area of CSA.

We would like to thank all authors of this conference for their paper contributions and presentations; and we would like to sincerely appreciate the following prestigious invited speakers who kindly accepted our invitations, and helped to meet the objectives of the conference:

- **Dr.Yi Pan**

Georgia State University, USA

We also sincerely thank all our chairs and committees, and these are listed in the following pages. Without their hard work, the success of CSA 2012 would not have been possible. Finally, we would like to thank the SGSC 2012, NT3CA 2012, WMS 2012, WPS 2012 workshop chairs, and special session organizers of SS-STS, SS-CASDAI, SS-SPIVN, for their great contributions.

With best regards,
Looking forward to seeing you at CSA 2012
Sang-Soo Yeo, Mokwon University, Korea (Leading Chair)
Odej Kao, Technische Universitat Berlin, Germany
Yi Pan, Georgia State University, USA
CSA 2012 General Chairs

Welcome Message from the Program Chairs

CSA 2012

On behalf of the CSA 2012 organizing committee, it is our pleasure to welcome you to the 4th International Conference on Computer Science and its Applications (CSA 2012).

The success of a conference is mainly determined by the quality of its technical program. This year's program will live up to high expectations due to the careful selection by the Program Committee. They have spent long hours in putting together an excellent program and deserve a big applause.

The conference received 163 submissions, and all were reviewed by the Program Committee. In the review process, we assigned at least three Program Committee members to each paper. After careful deliberation and peer reviews, we selected 52 papers for presentation and inclusion of the conference proceedings, whose acceptance rate is around 32 %.

There are many people who contributed to the success of CSA 2012. We would like to thank the many authors from around the world for submitting their papers. We are deeply grateful to the Program Committee for their hard work and enthusiasm that each paper received a thorough and fair review. Finally, we would like to thank all the participants for their contribution to the conference.

Sincerely yours,

Yang Sun Lee, Mokwon University, Korea
Gregorio Martinez, University of Murcia, Spain
Hong Ji, BUPT, China
Jinhua Guo, University of Michigan-Dearborn, USA
Robert C. H. Hsu, Chung Hua University, Taiwan
CSA 2012 Program Chairs

Conference Organization

CSA 2012

Organizing Committee

Steering Chairs

James J. (Jong Hyuk) Park, Seoul National University of Science and Technology, Korea
Han-Chieh Chao, National Ilan University, Taiwan
Mohammad S. Obaidat, Monmouth University, USA

General Chairs

Sang-Soo Yeo, Mokwon University, Korea
Odej Kao, Technische Universitat Berlin, Germany
Yi Pan, Georgia State University, USA

General Vice-Chair

Changhoon Lee, SeoulTech, Korea

Program Chairs

Yang Sun Lee, Mokwon University, Korea
Gregorio Martinez, University of Murcia, Spain
Hong Ji, BUPT, China
Jinhua Guo, University of Michigan - Dearborn, USA
Robert C. H. Hsu, Chung Hua University, Taiwan

Workshop Chair

Hangbae Chang, Sangmyung University, Korea
Weili Han, Fudan University, China
Waltenegus Dargie, Technical University of Dresden, Germany
WenZhan Song, Georgia State University, USA

International Advisory Board Committee

Hamid R. Arabnia, The University of Georgia, USA
Doo-soon Park, SoonChunHyang University, Korea
Hsiao-Hwa Chen, Sun Yat-Sen University, Taiwan
Philip S. Yu, University of Illinois at Chicago, USA
Yi Pan, Georgia State University, USA

Salim Hariri, University of Arizona, USA
Leonard Barolli, Fukuoka Institute of Technology, Japan
Jiankun Hu, RMIT University, Australia
Shu-Ching Chen, Florida International University, USA
Lei Li, Hose University, Japan
Victor Leung, University of British Columbia, Canada

Publicity Chairs

Amiya Nayak, University of Ottawa, Canada
Weiwei Fang, Beijing Jiaotong University, China
Sung-Bae Cho, Yonsei University, Korea
Min-Woo Cheon, Dongshin University, Korea

Local Arrangement Chair

Sang Oh Park, KISTI, Korea
Taeshik Shon, Ajou University, Korea
Namje Park, Jeju National University, Korea
SoonSeok Kim, Halla Universty, Korea

Program Committee

Hoon Choi, Chungnam National University, Korea
Evi Syukur, University of New South Wales, Australia
Prakash Veeraraghavan, La Trobe University, Australia
M. Dominguez-Morales, University of Seville, Spain
Min-Woo Cheon, Dongshin University, Korea
Gregorio Martinez, University of Murcia (UMU), Spain
Fei Yan, Wuhan University, China
Chan Yeob Yeun, Khalifa University of Science, Technology & Research (KUSTAR), UAE
Neal N. Xiong, Georgia State University, USA
Yasuhiko Morimoto, Hiroshima University, Japan
Dieter Gollmann, TUHH, Germany
Jordi Forne, Technical University of Catalonia, Spain
Jose Onieva, University of Malaga, Spain
Jan de Meer, Brandenburg Technical University(BTU), Germany
HeeSeok Kim, Korea University, Korea
Zubair Baig, King Fahd University of Petroleum and Minerals, Saudi Arabia
El-Sayed El-Alfy, King Fahd University of Petroleum and Minerals, Saudi Arabia
Mohammed Houssaini Sqalli, King Fahd University of Petroleum and Minerals, Saudi Arabia
Talal Mousa Alkharobi, King Fahd University of Petroleum and Minerals, Saudi Arabia
Chih-Lin Hu, National Central University, Taiwan
Atul Sajjanhar, Deakin University, Australia
Tanveer Zia, Charles Sturt University, Australia
Claudio Ardagna, University of Milan, Italy
Chuan-Ming Liu, National Taipei University of Technology, Taiwan
Yao-Nan Lien, National Chengchi University, Taiwan
Honggang Wang, University of Massachusetts, USA
Yuh-Shyan Chen, National Taipei University, Taiwan
Rongxing Lu, University of Waterloo, Canada
Chang Wu Yu, Chung Hua University, Taiwan ROC
Chih-Shun Hsu, Shih Hsin University, Taiwan ROC
Qingyuan Bai, Fuzhou University, China
Anirban Mondal, Indraprastha Institute of Information Technology, Delhi India
Ramamohanarao Kotagiri, The University of Melbourne, Australia
Debajyoti Mukhopadhyay, Balaji Institute of Telecom & Management Pune, India
Biswajit Panja, University of Michigan, USA
Ashkan Sami, Shiraz University, Iran
Mei-Ling Shyu, University of Miami, USA
Choochart Haruechaiyasak, NECTEC, Thailand
Masao Ohira, Nara Institute of Science and Technology, Japan

Han Xu, InfoQ (www.infoq.com/cn), P.R. China
Mazeiar Salehie, Lero-The Irish Software Engineering Center, Ireland
Yeong-Deok Kim, Woosong University, Korea
Chao-Tung Yang, Tunghai University, Taiwan
Rajkumar Buyya, University of Melbourne, Australia
Andrzej M. Goscinski, Deakin University, Australia
Jehn-Ruey Jiang, National Central University, Taiwan
Chin-Fu Kuo, the National Kaohsiung University, Taiwan
Hiroyuki Tomiyama, Nagoya University, Japan
Jun Wu, National Pingtung Institute of Commerce, Taiwan
Shengquan Wang, University of Michigan Dearborn, USA
Liang-Teh Lee, Tatung University, Taiwan
Jen-Wei Hsieh, National Taiwan University of Science and Technology, Taiwan
Yuan-Tse Yu, National Kaohsiung Normal University, Taiwan
Yashu Chen, National Taiwan University of Science and Technology, Taiwan
Yo-Ping Huang, National Taipei University of Technology, Taiwan
Simone Ludwig, North Dakota State University, USA
Shu Chen Cheng, Southern Taiwan University, Taiwan
Chuan-Kang Ting, National Chung Cheng University, Taiwan
Antonina Dattolo, University of Udine, Italy
Tzung-Pei Hong, National University of Kaohsiung, Taiwan
Chang-Shing Lee, National University of Tainan, Taiwan
Thanos Vasilakos, University of Western acedonia, Greece
Don-Lin Yang, Feng Chia University, Taiwan
Jen Li, North Dakota State University, USA
Kevin Grant, University of Lethbridge, Canada
Jemal H. Abbawajy, Deakin University, Austrailia
Constantinos Mourlas, University of Athens, Greece
Farhad Arbab, CWI, Netherlands
Kuan-Ching Li, Providence University, Taiwan
Massimo Cafaro, University of Salento, Italy
Sun-Yuan Hsieh, National Cheng Kung University, Taiwan
Hae-Duck Joshua Jeong, Korean Bible University, Korea
Cho-Chin Lin, National Yilan University, Taiwan
Ruay-Shiung Chang, National Dong Hwa University, Taiwan
Guandong Xu, Victoria University, Australia
Chia-Hung Yeh, National Sun Yat-sen University, Taiwan
Guan-Ling Lee, National Dong Hwa University, Taiwan
Yao-Chung Chang, National Taitung University, Taiwan
Kuei-Ping Shih, Tamkang University, Taiwan
Jui-Feng Yeh, National Chia-Yi University, Taiwan
Jae-Ho Choi, Yonsei University, Korea
Zhenglu Yang, University of Tokyo, Japan
JIanwei Zhang, Kyoto Sangyo University, Japan
Andrew Kusiak, The University of Iowa, USA

Alton Chua Yeow Kuan, Nanyang Technological University, Singapore
Theng Yin Leng, Nanyang Technological University, Singapore
Margaret Tan, Nanyang Technological University, Singapore
Richi Nayak, Queensland University of Technology, Australia

Welcome Message from the Workshop Chairs

NT3CA 2012

It is our pleasure to welcome you to The 2012 FTRA International Workshop on New Technology Convergence, Cloud, Culture, and Art (NT3CA 2012) that is being held in Jeju, Korea, November 22–25, 2012.

The 2012 FTRA International Workshop on International Workshop on New Technology Convergence, Cloud, Culture, and Art (NT3CA 2012), co-sponsored by FTRA will be held in Jeju, Korea, November 22–25, 2012. The NT3CA 2012 is a workshop for scientists, engineers, researchers, and practitioners throughout the world to present the latest research, new trends of IT such as cloud computing or social network, culture technology, ideas and applications in all areas of new technology convergence, cloud, culture, and art. The topic can be many related services based on cloud computing environment such as security, social network, communication technique, evaluation, technical tuning, virtualization, framework, software technique, and so on. This workshop will be a good chance to discuss the opinions among the experts. The NT3CA 2012 is co-sponsored by FTRA. In addition, the conference is supported by KITCS.

We would like to send our sincere appreciation to all participating members who contributed directly to NT3CA 2012. We would like to thank all Program Committee members for their excellent job in reviewing the submissions. We also want to thank the members of the organizing committee, all the authors and participants for their contributions to make NT3CA 2012 a grand success.

Sincerely yours,
Jin-Mook Kim, Sunmoon University, Korea
NT3CA 2012 General Chair

NT3CA 2012 Workshop Organization

Organizing Committee

General Chairs

Sang-Soo Yeo, Mokwon University, Korea
Jin-Mook Kim, Sunmoon University, Korea

Program Chairs

Juyeon Jo, University of Nevada, USA
Hwa-Young Jeong, Kyung Hee Unversity, Korea

Program Committee

Jeong-Woo Byun, Kyung Hee university, Korea
Gi-Hwon Kwon, Kyong Gi University, Korea
Jae-Soo Yoo, Chung Buk National University, Korea
Hwang-Rae Kim, Kong Ju National University, Korea
Koo-Rack Park, Kon Ju National University, Korea
Young-Ae Jeong, Sunmoon University, Korea
Jong-hee Kim, Sunmoon University, Korea
Sung-Sik Hong, Hyejeon Colleage, Korea
Woon-Ho Choi, Seoul National University, Korea
Kim Dong-Kun, Kyung Hee University, Korea
Jeong-Won An, Osan University, Korea
Hyun-Jung Yoon, Yewon Art University, Korea
Hye-Jung Jung, Pyeong Taek University, Korea
Chang-Yong Lee, Kong Ju National University, Korea
Sunny Kim, Texas Tech University, USA

Welcome Message from the Workshop Chairs

SGSC 2012

On behalf of the program chairs and technical program committees, it is our pleasure to welcome you to the Workshop on Smart Grid Security and Communications (SGSC-2012). This workshop is in conjunction with the 4th FTRA International Conference on Computer Science and its Applications (CSA 2012), to be held in Jeju, Korea, November 22–25, 2012. This workshop aims at bringing together researchers from academic and industry laboratories for a face-to-face meeting to discuss common research interests. This activity is a catalyst for discussing relevant research questions and engagement in the growing area of smart grid and related to the major area of cyber security and communication. SGSC 2012 is not an end in itself but a means by which research communities achieve their new funding streams and novel collaborations, and establish a long-lasting research network. We hope to continue last year's success and have another great event this year. We would also like to thank the program committee of SGSC 2011 and the external reviewers for their constant support. It is our great honor to invite you to attend this workshop. Enjoy the program and your stay in Jeju!

Sincerely yours,
Bo-Chao Cheng, National Chung-Cheng University, Taiwan
SGSC 2012 General Chair

SGSC 2012 Workshop Organization

Organizing Committee

General Chairs

Garry W. Chang (FIEEE), National Chung-Cheng University, Taiwan
James J. (Jong Hyuk) Park, SeoulTech, Korea

Organizing Chair

Bo-Chao Cheng, National Chung-Cheng University, Taiwan

Program Chairs

Steven Low, Caltech, USA (FIEEE)
Paolo Tenti, University of Padova, Italy (FIEEE)
Boming Zhang, Tsinghua University, China (FIEEE)
Huy Kang Kim, Korea University, Korea

Publicity Chairs

Ping-Hai Hsu, ITRI, Taiwan
Ezendu Ariwa, London Metropolitan University, UK

Program Committee

Huan Chen, National Chung-Hisng Univerity, Taiwan
Kwang Hyuk Im, PaiChai University, Korea
Abdelmajid Khelil, TU Darmstadt, Germany
Chang Oh Kim, NCSOFT, Korea
Ibrahim Korpeoglu, Bilkent University, Turkey
Jung-Shian Li, National Cheng-Kung University, Taiwan
Kwang-Hui Lee, Changwon National University, Korea
Yong-hoon Lim, KEPRI, Korea
Jiunn-Liang Lin, ITRI, Taiwan
Young Hoon Moon, Korea Telecom, Korea
Jiyoung Woo, Korea University, Korea
James C.N. Yang, National Dong Hwa University, Taiwan
Chien-Chung Shen, University of Delaware, USA

Contents

Part I
Computer Science and its Applications

Utilizing TPM Functionalities on Remote Server

Norazah Abd Aziz and Putri Shahnim Khalid

Abstract Trusted Platform Module (TPM) has become an essential functionality in the information security world today. However, there are legacy computers that do not have TPM onboard and would still want to use the TPM functionalities without having to replace the hardware. Also, TPMs are not available for virtual machines hence there is a need to provide integrity of the virtual machine platforms. This paper introduces a framework to provide a remote server with TPM capabilities for the legacy computer and also virtual machines to be able to utilize TPM functionalities. In this framework, there is also a need to provide fault tolerance mechanism to ensure reliability of the server and also scalability feature is incorporated to cater for growing number of users. The main component of the framework is the 'vTPM Manager' module which resides in the remote TPM server. This vTPM Manager handles the creation and deletion of virtual TPMs, providing fault tolerance mechanism and also scalability feature for the whole system. By using this framework, users who do not have a TPM residing in their device would be able to remotely access the TPM server to utilize the TPM functionalities with the assurance of a fault tolerance mechanism and the number of users is unlimited since it is scalable.

Keywords Fault-tolerance · Scalability · TPM instances · Migration · vTPM Manager · Virtual TPM

N. Abd Aziz (✉) · P. S. Khalid
MIMOS Berhad, Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia
e-mail: azahaa@mimos.my

P. S. Khalid
e-mail: shahnim.khalid@mimos.m

S.-S. Yeo et al. (eds.), *Computer Science and its Applications*,
Lecture Notes in Electrical Engineering 203, DOI: 10.1007/978-94-007-5699-1_1,

1 Introduction

Trusted Computing (TC) is a technology developed and promoted by non-profit industry consortium. The technology aims to enhance the security of hardware and software building blocks. The consortium known as Trusted Computing Group (TCG) [1] has come up with specifications on Trusted Platform Module (TPM) which has potentials to be used for security and trust related services like remote attestation and key management. In order to utilize the Trusted Computing functionalities, new PCs and laptops are equipped with a TPM [2] on the motherboard by many hardware manufacturers.

However, legacy computers and older motherboards do not have TPMs onboard. This poses a problem for users wanting to utilize the Trusted Computing functionalities without having to replace all the equipments. Furthermore, most virtual machine environments are not equipped with a TPM. Since virtual machines are used widely in cloud computing environment, it is necessary to apply TPM functionalities to provide integrity of the virtual machine platforms.

In this paper, we introduce a framework to provide a remote server with TPM capabilities in the form of hardware TPM and/or software based TPM. Software based TPM in this context is referred as virtual TPM (vTPM) in this paper. Users can connect to the remote server and use the trusted computing capabilities. We will discuss about fault tolerance mechanisms to ensure users can connect to the server at all times through virtual TPM (vTPM) instances. In addition, we also discuss on the scalability of the servers in order to cater for high number of users and their associated vTPM instances at one time.

This paper is organized as follows. Section 1 starts with this brief introduction and followed by current related work in Sect. 2. Section 3 of the paper explains about the fault tolerance mechanism and scalability of the server. The basic framework of the attempt implementation containing the process flow of system requirement is presented in Sect. 4. The paper continues to describe the concept of remote server with TPM capabilities implementation handled by a vTPM Manager module. Finally Sect. 5 describes the current implementation. The paper ends with a conclusion.

2 Related Work

A system which enables the trusted computing for an unlimited number of virtual machines was proposed by [3]. Their approach is to virtualize the TPM, so the TPM functionalities are available to operating systems and applications running in virtual machines. We adopted their approach which provides added functions to create and destroy virtual TPM instances as well as to maintain the migration of a virtual TPM instance with its respective virtual machine. The difference is they

implement multiplexing of request from clients to their associated vTPM instances but our approach only interacts with the clients during initialization process.

The paper in [4] is extended from [3] by adding built-in attestation mechanism. They have introduced a ticket-based remote attestation scheme. Compared to our framework, their vTPM instances management resides in Virtual Machine (VM). But, similar with our approach, the software TPM is also always protected by the hardware TPM. During vTPM spawns, its PCR values are initialized with values from the underlying hardware TPM.

The security and reliability issues in client virtualization were also discussed in [5]. Their proposed solutions leverage on Intel vPro and TPM in order to overcome the issues and using trusted VM container through remote attestation protocol verification. Our approach is not limited to the Intel technology and platform and hence is more feasible.

In [6], the paper describes their approach to secure cloud-based system using trusted computing. Their design mainly focuses on the virtual DRTM (Dynamic Root of Trust for Measurement). By virtualizing the DRTM, they control the locality by modifying the Xen vTPM Manager. Locality is based on the memory addressing which corresponds to different levels in a system, for example security kernel at Locality 0 while application at Locality 3 and so on. Our approach differs in that we are not modifying the way the guest OS access the data based on these locality using a certain algorithm that has to be embedded in the hypervisor (such as Xen).

3 Fault Tolerance, Scalability and Attestation

3.1 Fault Tolerance

Fault-tolerance is the property of a software or hardware that enables a system to operate continuously in the event of failure of (or one or more faults within) some of its components [7]. In other word, it is designed to recover from failure immediately with no loss of service. There are a few levels of fault tolerance based on the ability to continue operation in the event of a power failure in time basis. The levels are defined by whether the fault tolerance feature is provided by software, embedded in hardware, or by both combinations.

A fault-tolerance mechanism consists of three types: replication, redundancy and diversity. Fault-tolerance replication is requesting or directing tasks in parallel from multiple identical instances of the same system or subsystem based on the best output [7]. Similarly, fault-tolerance redundancy is also providing multiple identical instances but switching to one of the remaining instances in case of a failure [8]. In other word, it uses multiple nodes that are ready to provide service in order to recover from service failure of a single node. In contrast to replication and

redundancy type, diversity provides multiple different implementations of the same specification.

In this paper we focus on fault tolerance using hardware which is provided to ensure the TPM server is available at all times. As mention earlier, trust and security is the main concern for the framework, hence replication of the vTPM instances is required to ensure users can connect to the server at all times even when there is a failure.

3.2 Scalability

According to [9], scalability is desirable in technology as well as business settings because both benefit significantly from the ability to easily increase volume without impacting the contribution margin. Scalability is the ability of a hardware or system to adapt to increasing demand due to the growing amount of context volume or size in order to meet user capacity. Our framework is designed to be scalable in the sense that the system can be upgraded easily and transparently to the users without shutting down the system. Hence, further investment to the system for adding new processors, devices and storage to the system has no additional cost.

Scalability can be measured in various dimensions [9], but this paper focus on load scalability. It means that the system easily expands and organizes its resource to sustain heavier or lighter number of inputs for modification and deletion activities. In our approach, the network scalability addresses the issue of retaining performance levels while adding additional servers to a network. Additional servers are typically added to a network when additional processing power is required.

3.3 Attestation

One of the most important uses of TPM is to enable a computing platform to attest its integrity to another entity. The attestation protocol involves measuring various ‘properties’ of the platform and storing the values in the TPM. When a remote entity asks for assurance of the integrity of the platform, the measurements are verified and sent over to the other entity. Our framework is designed to implement this feature in virtualization environment which is used to assure users of the integrity of the spawned vTPM. In our framework attestation protocol is run by enhanced virtualization API named as TMCI and a vTPM to verify the integrity of the associated VM. When a request for a VM is received, the TMCI will first ask the vTPM to attest the integrity of the VM. The VM will be created and given to the user if the attestation is successful. Otherwise another VM has to be created.