Progress
Chinese Science Bulletin
Computer Science
December 2012 Vol.57 No.35: 4529–4532
doi: 10.1007/s11434-012-5550-z

Recent advances on trusted computing in China

DONG Wei[1*] & CHEN LiQian[1,2]

[1] *School of Computer, National University of Defense Technology, Changsha 410073, China;*
[2] *National Laboratory for Parallel and Distributed Processing, Changsha 410073, China*

Received September 9, 2012; accepted October 15, 2012

This article highlights some recent research advances on trusted computing in China, focusing mainly on the methodologies and technologies related to trusted computing module, trusted computing platform, trusted network connection, trusted storage, and trustworthy software.

trusted computing, information security, trustworthy software, research advance

Citation: Dong W, Chen L Q. Recent advances on trusted computing in China. Chin Sci Bull, 2012, 57: 4529–4532, doi: 10.1007/s11434-012-5550-z

Trusted computing leads an emerging trend in information technology towards improving the trustworthiness and security of computer systems. It has attracted great worldwide attention from both academia and industry in recent years. In particular, computer scientists in China have devoted considerable effort to this challenge and have made substantial achievements, which enables them to be at the forefront of this area. This article gives a review of some recent research progress in the methodology and technology of trusted computing in China. We summarize the major advancements in this field from two aspects: trusted computing infrastructure and trustworthy software.

1 Trusted computing infrastructure

Trusted hardware infrastructure provides a basis for trusted computing. Shen et al. [1] systematically summarized the achievements in trusted computing module (TCM) and trusted computing platform (TCP) made in China before 2010. In 2003, Jetway, cooperating with Wuhan University, developed the first TCM chip (named J2810) and the first trusted computer in China. In 2007, ZTE IC developed a TCM chip following the specifications of China in trusted computing. Meantime, other IT companies in China such as Lenovo and Great Wall were also devoted to developing trusted computers.

Cryptography is a key technology for trusted computing and cryptographic support platform provides a fundamental support for trusted computing platform. In the field of Cryptography, researchers in China have made a lot of progresses in recent years [2–5], which certainly provides a strong support for the development of trusted computing. In December 2007, State Cryptography Administration Bureau of China published the functionality and interface specification of cryptographic support platform for trusted computing [6], which marks a new stage of the development of trusted computing in China. Many IT companies in China such as Lenovo, Sinosun and ZTE IC have developed a number of cryptographic support platforms which have passed the certification of the State Cryptography Administration Bureau of China [1]. In academic regard, Feng et al. [7] analyzed the problems of the current property attestation and proposed a new property attestation protocol on bilinear map for trusted cryptographic module by exploiting the cryptographic feature of trusted cryptographic module. The protocol is built based on the property attestation model with the online trusted third party, which has the advantages of simplifying the verification of property revocation and causing less computation cost.

Testing, verification and evaluation play important roles in improving and guaranteeing the quality of trusted com-

*Corresponding author (email: wdong@nudt.edu.cn)

puting products, which is critical for putting them into market. In this regard, Zhang et al. [8] proposed a formal analysis method of the chain of trust, an automated random test case generation method of TCG (Trusted Computing Group) software stack, and an architecture for testing and evaluating system on TCP. Experiments showed some valuable results: some flaws were found in the design of the architecture of the present TCG computing platform and also in some products of existing trusted computing platforms. By exploiting formal verification techniques that have been successfully used for verifying the correctness of hardware, Liu et al. [9] presented a formal proof for the correctness of sequential and parallel prefix-based adders in electronic circuits. They formalized prefix adders in terms of first-order recursive equations used in standard computer arithmetic community. Their work provides a foundation for formal proofs of computer arithmetic algorithms.

With the extensive application of network in modern information systems, the trustworthiness especially security requirements for the platform and the data become higher and higher, particularly in open network environment. Zhang et al. [10] proposed the first trusted network connect (TNC) model in the universally composable framework to analyze the security of extensible authentication protocol in the network authorization transport interface. Their work presented a whole new approach of addressing TNC model in the universally composable framework and can be applied to analyze more protocols in the TNC architecture. To ensure the security of information content on the internet, Fang et al. [11] proposed a control model together with the corresponding evaluation frame. The control model is based on the three core-elements of communication, namely "Who communicates with whom", "How do they communicate" and "What is the content of communication". The reference monitor of the model is placed in the transmission channel and its effectiveness in controlling information transmission on the Internet can be quantitatively evaluated through the evaluation frame. Based on the vision that the physical layer security mechanisms are promising to achieve fast authentication with a low overhead in the future communication networks, Wen et al. [12] introduced a physical layer assisted authentication security scheme under public key infrastructure in vehicular communication networks, which has an advantage that the fast and lightweight message authentication process does not need synchronization among a group of vehicles but which is often required in other schemes. To address the concern of constructing information-theoretic secure network coding in the presence of eavesdroppers, Luo et al. [13] constructed information-theoretic secure network coding without additional encryptions and without giving up any capacity, which gives better results than the traditional ones. Wang et al. [14] presented a novel approach to improve the search efficiency and scalability of mobile ad hoc networks by clustering nodes based on cognitive trust mechanism, inspired from the brain informatics. Liu et al. [15] addressed the k-fault tolerant power assignments problem in heterogeneous wireless sensor networks, with the objective of providing k-vertex disjoint paths between any pair of sensor nodes while minimizing the total energy consumption. And three algorithms were proposed for this problem.

Virtualization plays an important role in building secure computing platforms, especially in cloud computing. To make trusted computing base (TCB) as small as possible, Chen et al. [16] proposed a light-weight architecture for TCB by designing a trusted virtual execution environment. By leveraging hardware isolation features such as system management mode provided by CPU, only security-sensitive code of applications is executed in the virtual environment such that the TCB only includes security-sensitive code and some management code of the virtual environment. To address the concern that the current distributed hash table (DHT) overlay in internet-based virtual computing environments (iVCE) cannot satisfy the "trust" requirements of Internet applications, Zhang et al. [17] proposed a trusted DHT overlay in iVCE, which supports upper-layer applications to form trusted subgroup and realize trusted DHT routing.

The security and dependability of data storage are critical for the future data accessibility in trusted computing, especially in presence of network. Ren et al. [18] proposed a secure and dependable data distributed storage scheme for in-networking stored sensing data in unattended wireless sensor networks. The scheme takes advantages of secret sharing and Reed-Solomon code, with low communication and storage overhead, and without the need of holding original data. To address the issue that an ordinary user without control permission over the whole system cannot secure data storage or data sharing of his own files in shared distributed storage systems, Xue et al. [19] proposed a new system architecture for secure file systems that enables ordinary users to secure file storage and sharing efficiently under untrusted multi-party shared storage and network environments which are out of their control. Based on this architecture, they implemented a stackable secure storage system called Corslet, which could provide end-to-end confidentiality and integrity as well as efficient access control for user data.

2 Trustworthy software

As the soul of information infrastructure, software has a direct impact on the trustworthiness of the whole information system. Trustworthy software has become one of the research focuses over the world recently. In 2007, the National Natural Science Foundation of China (NSFC) launched a grand research program on the fundamental research on trustworthy software [20], placing great importance on the aspects like metrics and models for software trustworthiness, software construction and verification, software evolution and control, and evaluation of environ-

ment trustworthiness. The program has obtained a lot of advances in recent years.

Eliciting and specifying requirements is always regarded as a very important and yet difficult work in software development. Jin et al. [21,22] proposed some principles for identifying trustworthiness requirements from software environment ontology, and constructed a requirement knowledge base. They identified two general situations that were usually related to different requirements, and introduced a set of constraint-patterns based on the different compositions of the two general situations. A requirement-oriented approach is further provided to reflect constraints in feature models, which supports to identify, specify and explain constraints between features.

Formal verification and analysis of software are always attached much importance. Li et al. [23] presented a method of computing the abstraction state of successive assignments and control statements. It narrows down the abstract state, reduces the time of employing a theorem prover, and uses a novel abstraction-searching strategy based on weight graph to find the shortest counterexample as early as possible, thus reducing the time for verification. Yang et al. [24] proposed a so-called slicing execution that is a lightweight symbolic execution, to extract abstract models from C programs by considering only part of the program variables. On this basis, they presented a conservative variant of weakest precondition to specify the over-approximated weakest precondition via variable abstraction. Chen et al. [25] proposed linear absolute value relation analysis to discover linear relations among values and absolute values of program variables in the framework of abstract interpretation. They proposed a new numerical abstract domain, namely the abstract domain of linear absolute value inequalities, which is able to infer non-convex invariants and can be used to analyze programs involving piecewise linear behaviors. Heap bounds are important to the correctness of software with dynamic memory allocation schemes but with limited memory. In this regard, Li et al. [26] presented an approach to statically find symbolic heap bounds for list-manipulating programs in cyber-physical systems, by combining shape analysis and numeric reasoning. Modern satisfiability modulo theories (SMT) techniques and solvers provide powerful backend engine support for software verification. Ma et al. [27] proposed a framework which integrates classical optimization procedures into the DPLL(T) architecture for solving SMT problems and presented two techniques for improving the solving efficiency with respect to linear arithmetic theory. The ways of improving the expressiveness of model and resolving the state explosion problem are always concerned in model checking. In system design, hybrid automata are well-studied formal models for dynamical systems, but the reachability problem is undecidable. Bu et al. [28] presented a path-oriented reachability analysis procedure for a class of nonlinear hybrid automata called convex hybrid automata. The approach encodes the reachability problem along a path of a convex hybrid automaton as a convex feasibility problem, which can be efficiently solved by off-the-shelf convex solvers, such as CVX. Then the verification can be applied in the frameworks of bounded model checking and counterexample-guided abstraction refinement. On the research frontier of quantum programming, Ying et al. [29] reviewed several verification methods for quantum programs and pointed out the potential applications of programming techniques and related formal methods in quantum computing.

Testing and debugging continue to be important means for improving software trustworthiness. To build a semantic framework for automated debugging, Li et al. [30] proposed a structural operational semantics for program debugging. The debugging process is divided into three sub-processes: tracing, locating and fixing. The tracing process reproduces the execution of the failed test case, which is then utilized to locate ill-designed statements and to generate a system of fix-equations whose solutions will be used to fix the bugs. The functions of both tracing and locating are formally specified by the rules of structural operational semantics.

Since verification and testing always face the challenges like state explosion and uncertain running environment, it is normally impossible to exhaustively verify and test the software. Therefore, runtime monitoring has become an indispensable means to find latent software faults. Zhang et al. [31] combined static analysis with runtime verification so that the possible fault can be predicted in advance. The defined predictive semantics is capable of predicting monitored property's satisfaction/violation even when the observed execution does not convince it.

Improving the security and reliability is a key issue for developing trustworthy software. Zhang et al. [32] developed a malware detection model based on a negative selection algorithm with a penalty factor, which overcomes the drawback of the traditional negative selection algorithms in defining harmfulness of "self" and "nonself" by introducing the penalty factor. By adjusting the penalty factor, the model can achieve a tradeoff between true positive and false positive rates to satisfy the different requirements of users. Experimental results demonstrated that the proposed model achieves better true positive rate on unknown malware and better generalization ability while keeping a low false positive rate. To explore fault propagation behaviors, Liu et al. [33] designed a software cascading faults model based on call relations between software functions. They introduced the concepts of function fault-tolerant capability and software fault intensity, and proposed an allocation rule on fault-tolerant capability. Simulations on practical software networks showed that a weak fault intensity, a small number of initial faults, and a strong fault-tolerant capability can slow down the cascading fault propagation and improve the stability of software systems.

Service-oriented computing is a hot topic nowadays in computer science, and how to obtain trusted service compo-

sition is a key issue. Li et al. [34] studied the reliability-aware synthesis problem for composing available services automatically and guaranteeing that the composed result satisfies the specifications, such as temporal constraints of functionality. The approach focuses on handling attributes and state relations, and permitting users and services to operate over them. A heuristic synthesis algorithm is also proposed with the complexity of EXPTIME. Due to the ever increasing number of services, it then becomes a challenging issue to enable the users to rapidly select and compose the proper services. Liu et al. [35] studied how to utilize service communities for automated service composition. They proposed the service community architecture and identified two key components to facilitate service discovery and composition. Two composition types are provided to help users explore the space of potential composition opportunities without having to understand too many details of individual candidate services.

Providing the proper tools and environment for developing trustworthy software is important in practice. For this purpose, the Ministry of Science and Technology of China supported a key project in National High-Tech Research and Development Program, named Trustie (Trustworthy software tools and integration environment) [36]. The project has built a large-scale software production environment for trustworthy resource sharing and cooperative development. Trustie includes software tools, software resource repositories, technique-oriented software production lines, collaborative platform for software development, and trust assurance mechanisms for developing trustworthy software. It has been used in some large software vendors, such as Digital China, Careland.

This work was supported by the National Natural Science Foundation of China (*61120106006, 60970035, 61202120*) *and National High-Tech Research and Development Program of China* (*2011AA010106*).

1 Shen C X, Zhang H G, Wang H M, et al. Research on trusted computing and its development. Sci China Inf Sci, 2010, 53: 405–433
2 Zhang H G, Li C L, Tang M. Capability of evolutionary cryptosystems against differential cryptanalysis. Sci China Inf Sci, 2011, 54: 1991–2000
3 Zhang H G, Li C L, Tang M. Evolutionary cryptography against multidimensional linear cryptanalysis. Sci China Inf Sci, 2011, 54: 2565–2577
4 Feng D G, Chen W D. Security model and modular design of fair authentication key exchange protocols. Sci China Inf Sci, 2010, 53: 278–287
5 Yan T, Yan F L. Quantum key distribution using four-level particles. Chin Sci Bull, 2011, 56: 24–28
6 State Cryptography Administration Bureau. Functionality and Interface Specification of Cryptographic Support Platform for Trusted Computing, December 2007. http://www.oscca.gov.cn
7 Feng D G, Qin Y. A property-based attestation protocol for TCM. Sci China Inf Sci, 2010, 53: 454–464
8 Zhang H G, Yan F, Fu J M, et al. Research on theory and key technology of trusted computing platform security testing and evaluation. Sci China Inf Sci, 2010, 53: 434–453
9 Liu F, Tan Q P, Mohamed O A. Formal proof of integer adders using all-prefix-sums operation. Sci China Inf Sci, 2012, 55: 1949–1960
10 Zhang J W, Ma J F, Moon S J. Universally composable secure TNC model and EAP-TNC protocol in IF-T. Sci China Inf Sci, 2010, 53: 465–482
11 Fang B X, Guo Y C, Zhou Y. Information content security on the Internet: The control model and its evaluation. Sci China Inf Sci, 2010, 53: 30–49
12 Wen H, Ho P H, Gong G. A framework of physical layer technique assisted authentication for vehicular communication networks. Sci China Inf Sci, 2010, 53: 1996–2004
13 Luo M X, Yang Y X, Wang L C, et al. Secure network coding in the presence of eavesdroppers. Sci China Inf Sci, 2010, 53: 648–658
14 Wang W, Zeng G S. Bayesian cognitive trust model based self-clustering algorithm for MANETs. Sci China Inf Sci, 2010, 53: 494–505
15 Liu L, Li L, Hu B. Algorithms for k-fault tolerant power assignments in wireless sensor networks. Sci China Inf Sci, 2010, 53: 2527–2537
16 Chen H, Sun J H, Liu C, et al. A light-weight, secure and trusted virtual execution environment (in Chinese). Sci Sin Inform, 2012, 42: 617–633
17 Zhang Y M, Lu X C, Li D S. Embedded DHT overlays in virtual computing environments. Sci China Inf Sci, 2010, 53: 483–493
18 Ren W, Ren Y, Zhang H. Secure, dependable and publicly verifiable distributed data storage in unattended wireless sensor networks. Sci China Inf Sci, 2010, 53: 964–979
19 Xue W, Shu J W, Liu Y, et al. Corslet: A shared storage system keeping your data private. Sci China Inf Sci, 2011, 54: 1119–1128
20 Liu K, Shan Z G, Wang J, et al. Overview on major research plan of trustworthy software (in Chinese). Bull Natl Nat Sci Found China, 2008, 3: 145–151
21 Wang P W, Jin Z, Liu H Y. Capability description and discovery of Internetware entity. Sci China Inf Sci, 2010, 53: 685–703
22 Zhang W, Zhao H, Jin Z, et al. Towards a more fundamental explanation of constraints in feature models: A requirement-oriented approach. Lect Note Comput Sci, 2011, 6727: 36–51
23 Li L, Song X Y, Gu M, et al. Competent predicate abstraction in model checking. Sci China Inf Sci, 2011, 54: 258–267
24 Yang X, Wang J, Yi X. Slicing execution with partial weakest precondition for model abstraction of C programs. Comput J, 2010, 53: 37–49
25 Chen L, Miné A, Wang J, et al. Linear absolute value relation analysis. Lect Note Comput Sci, 2011, 6602: 156–175
26 Li R, Wang J, Chen L, et al. Quantitative analysis for symbolic heap bounds of CPS software. Comput Sci Inf Syst, 2011, 8: 1251–1276
27 Ma F, Yan J, Zhang J. Solving generalized optimization problems subject to SMT constraints. Lect Note Comput Sci, 2012, 7285: 247–258
28 Bu L, Zhao J, Li X. Path-oriented reachability verification of a class of nonlinear hybrid automata using convex programming. Lect Note Comput Sci, 2010, 5944: 78–94
29 Ying M S, Feng Y, Duan R Y, et al. Quantum programming: From theories to implementations. Chin Sci Bull, 2012, 57: 1903–1909
30 Li W, Li N. A formal semantics for program debugging. Sci China Inf Sci, 2012, 55: 133–148
31 Zhang X, Leucker M, Dong W. Runtime verification with predictive semantics. Lect Note Comput Sci, 2012, 7226: 418–432
32 Zhang P T, Wang W, Tan Y. A malware detection model based on a negative selection algorithm with penalty factor. Sci China Inf Sci, 2010, 53: 2461–2471
33 Liu Y H, Liu X L, Wang J. A software cascading faults model. Sci China Inf Sci, 2011, 54: 2454–2458
34 Li M, Li B, Huai J P. Reliability-aware automatic composition approach for web services. Sci China Inf Sci, 2012, 55: 921–937
35 Liu X Z, Huang G, Mei H. A community-centric approach to automated service composition. Sci China Inf Sci, 2010, 53: 50–63
36 Trustie: Trustworthy software tools and integration environment. http://www.trustie.com/