I.J. Wireless and Microwave Technologies, **2012, 3, 41-47**
Published Online June 2012 in MECS (http://www.mecs-press.net)
DOI: 10.5815//ijwmt.2012.03.07

Available online at http://www.mecs-press.net/ijwmt

Research on Trustworthy Distributed System

LUO Chen[a], HE Ming[b], LIU Xiao-Ming[c], LI Yuan[d]

[a,b,c]Institute Command Automation PLAUST, Nanjing, China
[d]NO.73685 Troop, PLA, Nanjing, China

Abstract

To arrive at the goal of intensifying the trustworthiness and controllability of distributed systems, the core function of secure algorithms and chips should be fully exerted. Through building the trustworthy model between distributed system and user behaviors, constructing the architecture of trustworthiness distributed systems, intensifying the survivability of services, and strengthening the manageability of distributed systems, the secure problem of distributed systems is to be radically solved. By setting up the trustworthy computing circumstance and supplying the trustworthy validation and the active protection based on identity and behavior for trustworthy distributed system, we will reach the goal of defending the unaware viruses and inbreak. This research insists that the security, controllability, manageability, and survivability should be basic properties of a trustworthy distributed system. The key ideas and techniques involved in these properties are studied, and recent developments and progresses are surveyed. At the same time, the technical trends and challenges are briefly discussed.

Index Terms: Trustworthiness; trustworthy distributed system; controllability; survivability

1. Introduction

At present, the techniques of distributed system are excessive, miscellaneous, and the cost of implementation is great. The influence on the performance of distributed system is increasingly complex. The overstaffed abuse is gradually revealed. For example:

1) distributed system is built on the insecure terminal system

The most prominent secure problem of terminal system is prone to suffer from the erosion by the worm virus and Trojan horse. Because the bulk of terminal systems do not adopt enough safety precautions, some important programs and files will be destroyed. Moreover, other goal systems will be attacked by the worm virus and Trojan horse. Therefore, these will lead to the drop of performance of the whole distributed system. Distributed system is confronted with the serious crisis of trust[1].

* Corresponding author.
E-mail address: [a]lc0810@126.com; [d]lulu1979714@163.com

2) Distributed system is scare of the trusted safeguard measures

Practices indicate that the worm virus and Trojan horse could not be kept out with firewall, IDS, and antivirus software. On the one hand, these products make high requirement for administrators. A few users are able to fall short of this kind of demand. On the other hand, as far as the architecture is concerned, these products are extra add-ons. They ascribe the passive defensive forms and can not cope with the secure menace which is increasingly variational. The secure problems of distributed system need be solved and provide more reliably and simply controllable means to construct the trustworthy environment [2].

3) Distributed system is devoid of controllability and manageability; most remote-behavior is unpredictable

At the present time, capability of distributed systems is insufficient in mangy conditions such as user behaviors, run-states, controllability and manageability of system resource. At the same time, those capabilities are absolutely necessary not only for the security of distributed systems but also for health and continuance of development.

Therefore, new ideas are needed to resolve the problems such as security and function of distributed systems. To arrive at the goal of intensifying the trustworthiness and controllability of distributed systems, through building the trustworthy model between the distributed system and user behaviors, constructing the architecture of trustworthiness distributed systems, intensifying the survivability of services, and strengthening the manageability of distributed systems, the core function of secure algorithms and chips should be fully exerted. The secure problem of distributed systems including protection, creditability and manageability is to be radically solved. The security of service of distributed systems is improved effectively and development of Electronic Commerce and Electronic Government is promoted healthily and fleetly.

In this paper, we present a new scheme for constructing a trustworthy distributed system and make research on secure key techniques. In section1, we analyse the situation of security in distributed systems and points out the necessity to build trustworthy distributed systems. In section 2， we introduce the notion of trustworthy distributed system. Through building the trustworthy model between the distributed system and user behaviors, constructing the architecture of trustworthiness distributed systems, intensifying the survivability of services, and strengthening the manageability of distributed systems, the security problem of distributed systems is radically resolved in section 3. The significance of this paper is present in section 4.

2. Notion of Trustworthy Distributed Systems

At the present time, there are different cognitions to the trustworthy distributed systems: based on dependable authentication, based on conformity of exiting security technologies, based on trustworthiness of distributed system, based on trustworthiness of service supported by distributed system. The divergence to opinion may result in illegibility of definition on trustworthy distributed system and aggrandize difficulty of estimation for maneuverability of resolvent, as well as difference between requirement and development is magnified.

In this paper, distributed system, user behavior and its result is divinable and controllable in the trustworthy distributed system. Status of behavior can be supervised and unconventional action can be managed, while aftereffect of action can be estimated. In another word, the trustworthiness of distributed system has a set of attributes that security and survivability must be ensured in user's view and the manageability of distributed system must be supported in designer's view. Around maintenance of trustworthiness and manageability of behavior between components those three attributes of trustworthy distributed system can be amalgamated to arrive at the goal of trustworthiness of distributed system, while the conceptions of security, survivability, controllability and manageability are decentralized and isolating in traditional sense.

Unlike conventional researches on security, survivability and controllability, which are isolated and separated, the three properties are closely related in trustworthy distributed system, and are formed an organic whole around trustworthiness maintenance and behavior control, which are divided into three parties, input, process and output, as depicted in Fig. 1.

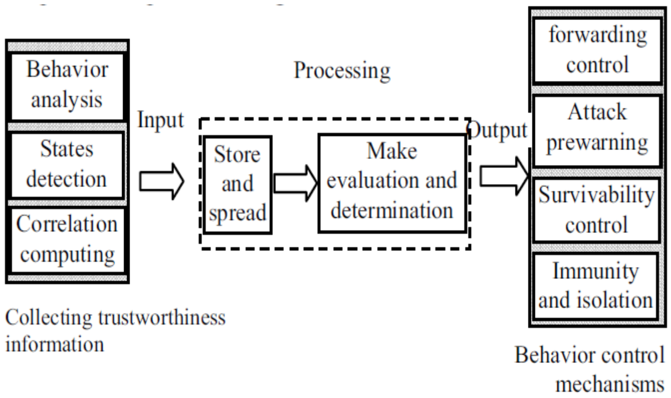

Fig 1. Trustworthiness maintenance and behavior control

The role of security is to reduce vulnerabilities on the chain of trustworthiness gathering, spreading and processing. Survivability can be thought of as a special control mechanism, i.e. resources management and schedule under the circumstance of existing misbehaviors. Controllability provides detailed mechanisms to monitor systems states and control misbehaviors. Trustworthiness information is collected by several methods, such as behaviors analysis, states detection and correlation computing. Then, trustworthiness information is stored on efficient format for quickly querying and updating, and spread to corresponding components for correlation computing.

To complete trustworthiness of distributed system, there are four problems: 1) Trustworthiness of remote user: trustworthiness of user is the precondition of security in distributed system and needs identity authentication terminal system so that termination and user can be controlled separately by distributed system. 2) Trustworthiness of remote platform: trustworthiness of remote platform contains trustworthiness of identity and computing environment. Distributed application is secure only when the platform is credible, otherwise, the remote node may be counterfeit or controlled by Trojan horse. 3) Trustworthiness of remote task: when the distributed application id executed, it must be partitioned to several independent physical modules which need to verify identity and trustworthiness of behavior each other. In that way, initiator of task can affirm that the task has been done inerrably. 4) Trustworthiness of remote action: comparing with trustworthiness of task, trustworthiness of action requires to forbid some actions and to restrict activity of remote user. Controllability of remote action refers to distribution and controllability of authority. To achieve the security strategy of whole system, authority of termination must be restricted. The last two problems are more difficult.

3. Research on Key Technology of Security

Around algorithm, technology and production of the distributed system, this research has four steps: (1) a trustworthy model of distributed system and user behavior is present based on exiting security technology through analyzing requirement of trustworthy distributed system. (2) a core chip of security is designed and completed. (3) an archetype is built to intensify security of trustworthy distributed system. (4) an estimation theory of trustiness is present to verify the archetype. The first is the main step in the research that the effect to security of distributed system is studied according to the characteristic of user behavior. The study on security chip is the foundation of substrate hardware. All the study is based on the second step. The perfect archetype is built through amalgamating pivotal security technologies such as security arithmetic, security protocol and intrusion prevention. The third step is the difficulty in the whole study. The last step is the soul of all the study in which the archetype is verified using trustworthiness estimation to prefect mechanism of trustworthiness of distributed system.

3.1. Trustworthy model

Trustworthy model is the pivotal process in development of system. In the TCSEC of Us Department of Defense formal description, verification and covert channel analysis is needed form Standard B. How to build trustworthy model which analyzes distributed system and user behavior availably is the precondition to study the trustworthy distributed system. From identity, behavior, content and computing environment, the foundational method which verifies system trustworthiness is studied through amalgamating method of verifying trustworthiness and traditional Take-Grand model, introducing trusted subject, restricting acquirement and authorization used only by trusted subjects and adding regulation to verify trustworthiness in model, as a result trustworthy model of distributed system and user behavior is built. There are two primary advantages in that model. Firstly security vulnerability of system can be analyzed by mathematics model because the requirement of trustworthiness of system is described abstractly and exactly without implementation details; secondly security trustworthiness of system is improved by the use of formal description and verification.

The elements in analysis of trustworthiness are present in fig.2. Estimation of trustworthiness of behavior contains trustworthiness of behavior and identity, while the latter is based on trustworthiness of content such as capability of protection and service, recommendation of trust and record of behavior.

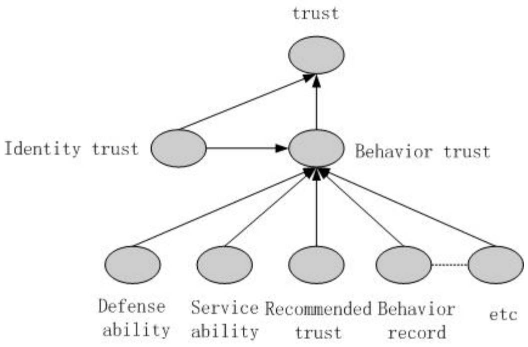

Fig 2. a kind of analysis model of trustworthy model

The evaluation of user's behavior is comprehensive evaluation for user's behavior, which is reflected by user's past behaviors. In order to get evaluation result effectively, we first subdivide user's behavior into behavior attributes, such as security behavior attribute and performance behavior attribute. Then we subdivided behavior attributes once again into more small data unit, namely behavior evidences. We use the layered, subdivided and quantitative idea to convert the complicated and comprehensive evaluation of user's behavior into the measurable and computable evaluation of behavior evidences. Thus the evaluation of user's behavior in the trustworthy distributed system can be solved effectively. So this method is feasible in engineering.

3.2. Secure Kernel chip

It is the foundation to trustworthy distributed system on hardware that SOC technology is adopted to design secure kernel chip, also security algorithm and key storage are completed inside chip. A security chip which can be applied to different cryptographic algorithms is needed imminently because of different applications with dissimilar cryptographic algorithms. In this paper, a secure kernel chip SOC which is constituted with kernel of RISC and multi-processor is designed, also that chip measures up to the standard of TPM. The chip can be applied to different cryptographic algorithms while the cost and efficiency of cryptographic algorithm are affected lightly.

3.3. Enhanced security architecture

Consulting exiting architectures of security operation system this paper puts forward the architecture of trustworthy model through secure kernel chip plays an important role in the controllability of security system, then enhanced security architecture is built in trustworthy distributed system. That architecture, which realizes trustworthy access controllability and supports flexible security strategy, can ensure the security of mechanism.

(1) Enhanced security architecture based on P2P

There is not a central manager in the architecture of P2P to manage nodes and users. Therefore, their trustworthiness of identity must be authenticated by the trusted third part (usually it is the center authentication, CA) and every node can authenticate destination node through proof supported by trusted third part (usually it is the signature for certificate of platform and user identity by CA).

Furthermore, secure kernel chip (SKC) supports authentication for trusted proxy in own node and verifies its trustworthiness when the computer system starts. Every node can verify trustworthiness of trusted proxy on the platform of destination through EK after destination is verified through authentication with signature of CA, since authentication of platform contains its authenticated key.

(2) Enhanced security architecture based on C/S

In distributed system based on topology of P2P authentication to destination is needed to verify particularly in the light of trusted model due to the lack of uniform view of authentication. The latter behavior is safe in the view of the owner of authority but unsafe in the view of other node, because other node may be controlled through the authorization once it is accredited to destination node.

This problem is avoided easily in distributed system based on C/S for database management of user and authority is centralized and the view of authorization is consistent for all nodes. If authorization is distributed only by server and client must request authority from server, this problem is solved easily.

In the architecture based on C/S, user's information including authorization and identity is managed by a trusted centralized management platform exiting in the server, while a trusted proxy is disposed on the client. The server verifies identity of client through authorization with its signature. Authorization of client encapsulated in SKC with encryption is requested from server which supports the key of decryption. All the authorization of client must be distributed by server and client has no prerogative to authorize any authorization to other client. Therefore, server can know which authorization the client has at any moment and grant or retract some authorization to client.

A simple architecture of trustworthy distributed system which avoids disadvantage like traditional affixed security mechanism is present in fig.3. To research architecture of trustworthy distributed system, there is one point to be realized: physical positions of nodes in distributed system are dispersed, so that security service is consistent in the view of system.

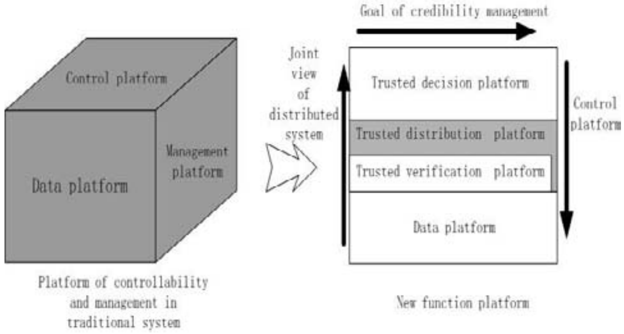
Control platform
Management platform
Data platform
Platform of controllability and management in traditional system
Joint view of distributed system
Goal of credibility management
Trusted decision platform
Trusted distribution platform
Trusted verification platform
Data platform
Control platform
New function platform

Fig 3. a simple architecture sketch map of trustworthy distributed system

Compared with traditional security architecture, security controllability is applied in enhanced architecture of trustworthy distributed system in four aspects: 1) security of password: using secure kernel chip of terminal system, hardware-encrypted platform like TCP is completed. Security algorism of key is ensured while encryption or decryption of data and digital signature authentication are completed, profiting from flexible ability of chip to support security algorism, perfect machination of key management and security defense. 2) security of identity authentication: it is no possibility that counterfeit user can operate system illegally because security level is heightened and certification has three steps “USB Key + password + biology keystroke characteristic” , also the computer is used exclusively. Based on the certification technology PKI, the identity of platform is safe and the risk of defense that counterfeit system intrudes distributed system is reduced, since the identity of platform is the unique sequence code of secure kernel chip with 64-bit in enhanced security system. 3) security of permission assignment: in enhanced security system inner process scheduling and outer process access is verified strictly under the instruction of trustworthy model so that permission of system is insured to be safe. 4) security of access control: by the trusted monitor in enhanced terminal system, trustworthiness of any access is verified to insure the trustworthiness of identity, behavior and computing environment in the access from subject to object. 5) security of system audit: all kinds of behavior or event logged in enhanced security system support history of events and supervise afterwards. Based on the enhanced terminal system, taking advantage of C/S architecture and simplifying strategy of authority controllability, the whole view of authority controllability is built on the server. Monitoring of client behavior is completed using trusted proxy of client. After those measures, security management in the whole distributed system is put into effect to every host and user.

3.4. Evaluation theory of trustworthiness

It is not possible to build a perfect trustworthy distributed system, so the quantitatively trustworthiness estimation of distributed system is valuable. Quantitative research on trustworthiness could find the weakness and risk in the distributed system and improve them. Quantifying of trustworthiness is also at exploring stage.

Trustworthiness evaluation is performed based on some preconfigured models, with logic instructions generated to drive particular control actions, such as forwarding control, attack prewarning, survivability control, and immunity [4]. Therefore, evaluation theory of trustworthiness which contains estimation of security, survivability and manageability is the precondition to monitor and revises system. It is also insurance of performance of the whole trusted distributed system. Though there is no absolute safe system, the ultimate goal of estimation trustworthiness of distributed system is not to remove weakness completely but support a scheme to balance service and security for administrator and a measure to defense attack actively such as that through building mechanism to describe behavior of attack, aggressive behavior is taken out from plentiful normal behaviors and access controllability of terminal system is completed. Emphasizing architecture and quantitative analysis on survivability of distributed system based on the transform between problem and space, estimation of trustworthiness is transformed to a method frame of classic problem.

4. Conclusions

Trustworthiness is an important aspect to the study on distributed system. In that paper, trusted computing technology and trustworthiness management technology of networks are integrated to resolve the conjuncture with distributed system and enhance the ability to dispose states dynamically so that enhanced trustworthy security system is built. That system supports a basal strategy to intelligent self-adaptive controllability of system security and service quality.

References

[1]Cyber Trust [EB/OL]. http://www.nap.edu/catalog/6161.html,2006.

[2]LIN Chuang, REN Fengyuan. New network with trustworthiness and controllability as well as expansibility[J]. Software Journal, 2004, 15(12): 1815-1821. (in Chinese)

[3]LIN Chuang, PENG Xuehai. Research on network architecture with trustworthiness and controllability[J]. Journal of Computer Science and Technology, 2006, 21(5): 732-739.

[4]LIN Chuang, PENG Xuehai. Research on trustworthiness of network[J]. Computer Journal, 2005, 28(5): 751-758. (in Chinese)

[5]LIN Chuang, WANG Yang, LI Linquan. Random model method and evaluation technology of network security[J]. Computer Journal, 2005, 28(12): 1943-1956. (in Chinese)

[6]TIAN Junfeng, XIAO Bing, MA Xiaoxue, et.al. Trustworthy model and analysis in TDDSS[J]. Computer research and development. 2007, 44(4): 598-605. (in Chinese)

[7]SHEN Changxiang, ZHANG Huanguo, FENG Dengguo, et.al, Summarazation of information security[J]. China Science: E(Information Science), 2007, 37(2): 129-150.